Website Vulnerability Analysis of AB and XY Office in East Java

Muchammad Zaidan [1], Febyola Noeraini [2], Zamah Sari [3], Denar Regata Akbi [4]
Universitas Muhammadiyah Malang, Jl. Raya Tlogomas No. 246, Malang 65144, Indonesia

ARTICLE INFO

Article history:

Received May 07, 2023
Revised June 10, 2023
Published June 30, 2023

Keywords:

Analysis;
Vulnerabilities;
Website;
Scanning;
Brute Force

ABSTRACT

Study this aim for analyze and identify vulnerability existing security on AB and XY Service Websites in East Java. Contribution study this is give more understanding deep about type vulnerability specific security and its impact to field website security. Method research used involve data scanning, analysis vulnerabilities, and Brute Force experiments. A total of 2 samples of AB and XY Service Websites were analyzed For identify existing vulnerabilities the data. However so, necessary noted that method study this own a number of limitations. First, size sample used possible limited to AB and XY Service Websites in East Java only, so generalization results study against other websites needs done with be careful. Second, analysis statistics used only covers analysis descriptive, so study this not yet investigate linkages between existing variables. Although thus, results study show exists necessary weaknesses and vulnerabilities corrected on AB and XY Service Websites. A number of findings covers problem website configuration and handling vulnerability that is not adequate. With highlight specific susceptibility, research this give more understanding deep about threat security faced by AB and XY Service Websites. In context field website security, research this own implication important. With understand existing vulnerabilities on AB and XY Service Websites, steps repair proper security can take for protect sensitive data and improve protection security in a manner whole. Kindly whole, research this identify and analyze vulnerability security on AB and XY Service Websites, as well give more understanding Specific about type existing vulnerabilities. Although there are limitations in method study this is the result still give valuable insight in field website security and can become base for repair more security effective and more data protection on both the AB and XY Service Websites.

Corresponding Author:

Muchammad Zaidan, Muhammadiyah University, Malang and 65144, Indonesia
Email: muchammadzaidan@webmail.umm.ac.id

1. INTRODUCTION

System information and the digital world has become integral in this modern era, where technology the more become need main. However, existence vulnerability in design system information can bring risk to data security and progress technology. Website security is very important in facilitate user in look for their information and data need, as well protect personal data user. System information and the digital world has become one unity in this modern era, where many people depend on existing technology. We live in an age where website security is very important in facilitate user in look for news, announcements, and desired data as well as protect personal data user. However, there is conditions particular where capacity design system information still not yet perfect, so resulted data leak through various point get in raises risk to continuity progress technology [1].

Vulnerabilities on a website can own serious consequences, such as damage reputation and credibility A company or organization. Security information saved user in the website database can threatened by attacks that are not responsible answer. This becomes significant problem. because that's important for apply steps proper security to use prevent data leakage and potential loss big. Data protection is task to be priority tall in work that can detect vulnerability security systems and web applications. The goal is for look for method for identify gap in infrastructure network so that can anticipate attacks by hackers on the web application [2]. Existence web analytics and methodologies assessment used for collecting data is very important in identify and mitigate threat cyber. Test analysis vulnerability can be rated from level maturity with similarity system device soft. There are several form implementations that includes data confidentiality, data integrity, and contingency availability application in form error. Do test analysis vulnerability no only analysis basic, but also involves the authentication process moment identify it with give access to track certain. because it, this process must be implemented with well that the system is their function. Administrators must depend on three factors, is methods, packages, and dependencies so that possibility hacked through the server to be smaller [3].

System information and the digital world has experience development rapidly in this modern era, where technology become no inseparable from life daily many people. However, progress technology also brings significant risk, especially in matter website security. Existence vulnerability on the website can impact serious about the company or organization, threatening reputation and trust user. Data leaks resulting from attacks cyber can resulted loss financial and loss hard trust for restored. Statistics and examples real from data breaches can give more understanding in about importance website security. Various companies and organizations have fall victim to an attack cyber, with stolen user data or abused. For example, some case famous involve personal data theft like information card credit or information resulting identity loss finance and pollution name good for affected company impact [4].

Besides that, is, attack cyber on government websites also have serious consequences. Attack on government websites can bother service public, hinder access important information, and even can damage security national. because that's important for understand vulnerability and implement steps proper security for protect websites and user data [5]. Services AB and XY are institution government located in East Java, which aims for realize service quality and effective public. Second institution this own role important in fulfil all need public in effort develop administration and documents needed by the community. Condition this capable give linkages with pattern life society and some company. For example, society will be facilitated in prepare all needs, especially those that are online, because matter this too is form effort for apply service the community carried out by the AB and XY Offices.

Based on analysis performed there is a number of problems like lack of understanding about causative factors attack security on the system AB and XY service website information. Research gaps can lie in identification and analysis root reason attack specific security, e.g., weakness design system or disobedient to practice security best. Furthermore, lack of research that focuses on analysis most likely vulnerability occurred on the AB and XY service websites. Research gaps can lie in in -depth research about type possible attack happen, like attack hacking, phishing attacks, or malware attack, and how vulnerability the can identified and corrected. No exists comprehensive evaluation to steps security that has implemented on AB and XY service websites. Research gaps can lie in research that tests and analyzes effectiveness steps existing security, as well explore crevices security potential yet overcome, and lack understanding about practice security that is applied to AB and XY service websites. Research gaps can lie in the research that analyzes policy existing security, monitoring security carried out, as well procedure update implemented system, with objective increase awareness will practice correct security and prevent possible attack happened. As well as lack solution -focused research effective mitigation to vulnerabilities found on the AB and XY Service websites. Research gaps can lie in the development and implementation specific solution for overcome vulnerabilities that have identified, like use technology more encryption strong or application mechanism more authentication safe.

Based on problem above study this focuses on assessment vulnerabilities on the AB and XY websites of service, an institution government in East Java. Study this aim for identify and evaluate vulnerability specific, incl attack like XSS (Cross-site Scripting) [6]. In context this, research this aim for do comprehensive analysis against AB and XY Service websites, an institution government in East Java. Study this will focus on assessment vulnerability and trial attack for identify and evaluate vulnerability specific, incl attack like XSS (Cross-site Scripting). Study this will use various tool security such as OWASP ZAP, Burp Suite, Skipfish, Wapiti, Rapidscan, and Nikto For support analysis vulnerability and trial attack [7]. Focus study this will aimed at identification and evaluation vulnerability specific, incl attack like XSS (Cross-site Scripting) and usage tools security such as OWASP ZAP, Burp Suite, Skipfish, Wapiti, Rapidscan, and Nikto. Through study this is expected can found possible solutions and recommendations increase AB and XY Service web site security, so give contribution significant in increase quality and effectiveness service the public they are provide.

Study this aim for do comprehensive analysis to the AB and XY Service websites with focus on assessment vulnerability and trial attack. Study this aim for identify and evaluate vulnerability specific, like XSS (Cross-site Scripting) attacks, as well for evaluate performance tools security such as OWASP ZAP, Burp Suite, Skipfish, Wapiti, Rapidscan, and Nikto in the context of the website. With do study this is expected can found possible solutions and recommendations increase AB and XY Service website security. This will contribute in a manner significant in increase quality and effectiveness service the public they are provide with protect personal data user with better and build trust user to institution the. Study this will produce repair significant in design experiment and get proof strong empirical. In study this, will identify a number of indicator specific security based on type different attacks, mainly phishing attacks on websites. Repair this will produce A more structure effective and special, which delivers strong influence in increase security. Besides that, analysis on website links will be done with extract a number of relevant features, and will do evaluation use detector XSS (Cross-site Scripting) vulnerabilities.

Because it, author will do study with analysis evaluation vulnerability and trial attack that includes use a number of circuit violence on AB and XY service websites use a number of tools (OWASP ZAP, Burp Suite, Skipfish, Wapiti, Rapidscan, and Nikto). The hope is research this will give analysis comprehensive on the AB and XY Service websites as well give contribution significant in increase quality and effectiveness service public. This will achieve with notice structure security from the agency's website the study this own implication significant practical in increase quality and effectiveness service provided by AB and XY Offices. With do AB and XY Office web site analysis using method evaluation vulnerability and trial attack, research this will produce deep understanding about vulnerabilities and weaknesses that exist on the website. Findings study this will give real benefits in a number of aspects. First, with identify and fix vulnerability If security is found, AB and XY offices will can increase security of their website and protect personal data user with more ok. This will build trust user to institute and improve reputation as well as credibility them. Second, with evaluate performance tools detection vulnerability such as OWASP ZAP, Burp Suite, Skipfish, Wapiti, Rapidscan, and Nikto in AB and XY Office website context, research this will give valuable guide in choose and use effective tools in mitigate threat security.

Besides that, the analysis was carried out in study this will help identify need improvement and development more on the AB and XY Office websites. With know existing vulnerabilities, institutions this can take action preventive and proactive for increase safety and quality their service give to society. With thus, research this will give significant contribution in increase quality and effectiveness service publicly provided by the AB and XY Offices through more understanding Good about their website vulnerabilities, more data protection well, and use effective tools in face threat security. Study this will use method evaluation vulnerability and trial involving attacks use a number of tools and techniques specific. Following is more detail carry on about methodology to be used, like Evaluation Vulnerability, Method evaluation vulnerability will used for identify and evaluate vulnerability security on AB and XY Office websites. A number of tools to be used in evaluation this includes OWASP ZAP, Burp Suite, Skipfish, Wapiti, Rapidscan, and Nikto. Tools this will used for scan and analyze websites with objective identify existing vulnerabilities, such as XSS (Cross-site Scripting) attacks, SQL injection, and vulnerabilities other [8]. Test Attack, After identification vulnerability done, research this will involve test attack For test vulnerabilities found. technique that will used including test XSS attacks, SQL injection, and attacks other relevant with AB and XY Office websites. Through test Attack this, research will test extent of vulnerability the can exploited and evaluated level resilience system to attack the. Besides that, research this will involve analysis features on the website link [9]. In analysis this, a few features on the website link will be extracted and evaluated for identify indicator potential from phishing attacks or effort attack others. Methodology this will give comprehensive approach in identify, evaluate, and test vulnerability security on AB and XY Office websites. With use tools that have proven effective and relevant techniques, research this will give deep understanding about circumstances the security of the website and provide valuable insight for development and improvement future security.

Study this will bring contribution new in field security system information and websites with focus on the context of Dinas AB and XY. This will give outlook new about vulnerabilities and solutions specific security for organization kind. Study this own objective main forgive contribution new in field security system information and websites, with focus on the context of Dinas AB and XY. In context this, research this expected can give outlook new about possible vulnerabilities There is in system information and websites used by the organization kind. With analyze and identify specific vulnerability for AB and XY Services, research this will help understand threat relevant security and deliver suitable solution. In a world that is increasingly connected digitally, security information become very important aspect for organization. In context this, research this will investigate various possible vulnerabilities there is in system information and websites for AB and XY Services, such as vulnerability configurations, brute force attacks, and flaws mechanism security certain. With identify vulnerability this, research this will give more understanding good about risk security faced by the organization and provide base for develop effective solution.

Through study this is expected that will There is effort for increase security system information and website in organization kind. With notice findings and recommendations from study this, Service AB and XY can take steps proactive in repair weakness existing security and apply practice best for protect system they from existing threats. Following this is a number of examples review available literature become reference in study in study kind like [10], Understanding Security Vulnerability Awareness, Firm Incentives, and ICT Development in Pan-Asia, Research this do review to frequent vulnerabilities and threats found in web applications. The result can give outlook about vulnerability that may also be relevant with AB and XY Service websites. Next A Large-Scale Analysis of Android — Web Hybridization [11], Research this see practice best in securing government websites. Overview literature this can give available guidelines and recommendations adapted for increase AB and XY Service website security which is part from agency government. Furthermore, study on A Survey of Exploitation and Detection Methods of XSS Vulnerabilities [12], Overview literature This identify and describe various threat security general cyber faced in environment organization. Information this can help in understand various attacks that may also apply to AB and XY Service websites. Next A survey on vulnerability assessment tools and databases for cloud-based web applications [13], Research this do review comprehensive literature about analysis vulnerability in the system information. This can give outlook about methods and approaches used in identify and address possible vulnerabilities available on the AB and XY Service websites.

Contribution research that can done based on background back above is about Enhancement Security System Information on AB and XY Service Websites study this is the focus is do analysis vulnerability (vulnerability assessment) and efforts involving attacks various type attack, like brute force attack, using a number of tools (OWASP ZAP, Burp Suite, Skipfish, Wapiti, Rapidscan, and Nikto). Objective mainly is for identify and address vulnerability the existing security on the AB and XY Service websites. In study this, can developed strategies and measures more security strong for protect data and information stored sensitive in the website's database system.

Contribution furthermore is about Application Methodology Analysis Vulnerabilities on Government Websites study this will focus on deployment method analysis effective and efficient vulnerability on government websites, especially on AB and XY Service websites. methods they can involve use tools analysis vulnerabilities, such as web analytics, to collect data and identify vulnerability security. Objective mainly is for give right recommendation in overcome vulnerabilities found, so can increase security and integrity government website system the. Study this can give guides and guidelines practical for organization government in face threat security cyber and protect user data. Second contribution above can give significant contribution to understanding and improvement security system information, particularly on government websites such as AB and XY Services. With increase data security and protection, reputation and trust public to institution government can maintained and improved.

2. METHODS

2.1. Licensing Research and Legality

Study this involves the process of website analysis carried out by researchers after obtain permission from the owner of the website under study, namely the AB & XY Service. Permission the obtained through letter that has approved by the website owner. Licensing before do website analysis is step important in study this for ensure obedience to ethics research and related data privacy with the website under study. In study this, researcher honor right privacy and interest’s website owner. Application letter permission has filed to the AB & XY Service for do analysis on their website. the letter explains goals, methods, and space scope research to be done. Besides that, the letter also includes information about data security and privacy to be guarded during the analysis process. Licensing process this is very important for guard trust between researchers and website owners. Researcher explain with clear objective study this is for identify potency vulnerability security on the AB & XY Service website. Besides that, the researcher also explained that all data obtained during analysis will guard confidentiality and use only for objective research.

Owner, in matter this AB & XY Service, consider letter application permission with careful. They evaluate interest research, the method will used, and the steps taken for protect their data security. After mature consideration, the website owner provides agreement written through letter that has Approved as sign agreement for continue the analysis process. In context study this permission before do website analysis has great significance this show that researcher committed for guard integrity research and engage the website owner is in the process. With get permission before do analysis, researcher show attitude professionalism and ethics high research. Besides that’s permission before do Website analysis also involves aspect law and compliance to applicable regulations. Researcher must obey Constitution data privacy and rules valid use of the website. In matter here, letter permission that has been be approved by the website owner proof that study this done with notice applicable laws and regulations.

Kindly Overall, licensing before carry out the process of analyzing the AB & XY Service website through letter that has approved by the owner of the website has important significance in guard trust, integrity, and compliance to applicable rules in study this. This step also shows attitude professionalism and ethics high research from researcher. With exists licensing this, research this can done with notice aspect data privacy, security, and interests the owner of the website under study. Following Fig. 1 is stages research used in research this, as following:

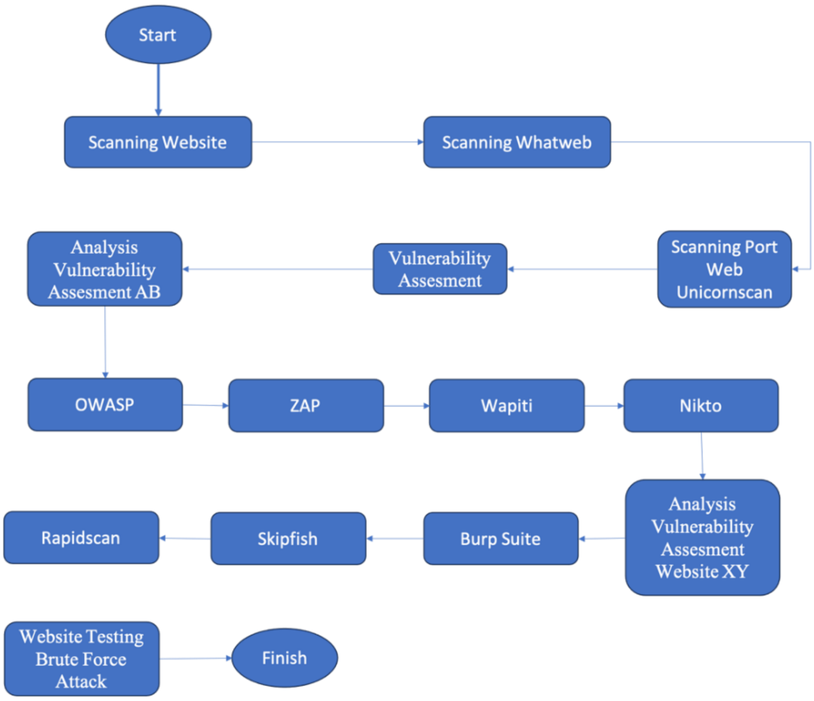
Start
Scanning Website
Scanning Whatweb
Scanning Port Web Unicornscan
Vulnerability Assessment
Analysis Vulnerability Assesment AB
OWASP
ZAP
Wapiti
Nikto
Analysis Vulnerability Assessment Website XY
Burp Suite
Skipfish
Rapidscan
Website Testing Brute Force Attack
Finish

Fig. 1. Research Flowchart

Fig. 1. Show a several methods are needed in meeting research starting from the website scanning process, targeting analyzing website vulnerability assessments and also penetrating in attempted brute force attacks on websites using several Linux-based tools such as OWASP ZAP, Burp Suite, Skipfish, Wapiti, Rapidscan, and Nikto.

2.2. Website Scanning

This stage is the first step in conducting research, because it takes some basic information from some website data related to website identity such as IP addresses, ports and other components used in the website structure. Further scanning is needed to later identify the security holes of the target website using the Whatweb and Unicornscan tools.

Scanning through the tool can be done in 2 different ways, namely internally and externally. This method can overcome the types of application components with the use of static and dynamic methods, it will make the scanning accuracy increase. However, there are some impacts that can cause the performance of an application because it will experience theft within the same host [13]. Vulnerability scanning tools aim to find parts of the system that cause vulnerability to security threat attacks in the form of failures, misconfigurations [13]. In external mode, an application will try to depend on a different component endpoint. Thus, these scans may not achieve the desired level of accuracy, as they can exploit and increase the overheating of the application system [13].

Function from deep website scanning study this is for identify vulnerability security on the websites under study. The website scanning process involves use tool specifically that automatic analyze various aspect from a website, like server configuration, code source, vulnerability web application, and settings security other. With scanning websites, researchers can gather information about possible vulnerabilities available on the AB and XY Office websites. This involves search gap security, like vulnerability to SQL injection attacks, cross-site scripting (XSS), server vulnerabilities, and others. The results of scanning the website will be give description about existing vulnerabilities and help researcher in identify areas that need repaired or strengthened the security. Objective from deep website scanning study this is for assist AB and XY Office in increase their website security with identify and fix vulnerabilities found. With evaluate existing vulnerabilities, steps proper safeguards can take for reduce risk attack by an unauthorized party authorized and protect sensitive data stored on that website.

2.2.1. Website Data Scanning using Whatweb

Whatweb is able to identify the information contained on websites targeted by researchers. The steps of this method can also scan the response on HTTP received by the target website, in this process it will be known the process of identifying the type of website server and managing what website content structure is contained in the application.

Function from scanning website data using Whatweb is for analyze various aspect from AB and XY Office websites, e.g., technology used, possible vulnerabilities there, and information other relevant with security. Website data scanning uses Whatweb is A tool or device software used for do analysis automatic against the website. Objective from use Whatweb in study this is for:

1. Identification Technology Used: Whatweb can help in identify technology used in website development such as CMS (Content Management System), web servers, languages programming, databases, and more. Information this important because can help researcher understand website architecture and understanding possible vulnerabilities related with technology the.
2. Scanning Vulnerability: Whatweb also got identify possible vulnerabilities There is on the AB and XY Office websites. This including search gap security general like vulnerability to SQL injection attacks, cross-site scripting (XSS), file disclosure, directories open, and others. With find vulnerability this, researcher can highlight vulnerable areas and prioritize action the necessary safeguards.
3. Collection Information: Whatweb can gather information important about websites like structure page, directory open, exposed email address, and version device software used. Information this can give outlook about website configuration and maybe give instruction about vulnerability possible potential exploited by attackers.

With use Whatweb for scanning website data, research this can give more picture comprehensive about vulnerability existing security on AB and XY Office websites in East Java. The results of this scan can assist AB and XY Office in identify and fix vulnerabilities found, as well increase their website security in a manner whole.

Whatweb contribute in identify hole security with gather information about configuration and features used by the website. Following is a number of information specific can collected by Whatweb:

1. Webserver: Whatweb can identify the type of web server used by the website, such as Apache, Nginx, or Microsoft IIS. Information this important because each web server has different characteristics and vulnerabilities.
2. Platform and Technology: Whatweb can gather information about the platforms and technologies used in website development, such as the CMS (Content Management System) used (eg WordPress, Joomla, Drupal), language programming (eg PHP, Python, Ruby), or use framework work (Laravel, Django, Ruby on Rails).
3. Plugins and Extensions: Whatweb can identify the plugins and extensions used by the website. Information this can give instruction about functionality extras that are on the website and can be influence possible vulnerabilities there.
4. Files and Directories: Whatweb can find visible files and directories or can accessed in a manner public on the website. This including configuration files, log files, or possible directory containing information sensitive.
5. vulnerability Related: Whatweb can also give information about related vulnerabilities with technology used on the website. For example, if Whatweb detect use version device existing software obsolete and vulnerable to known attack, that is will give warning about potency vulnerability the.

With gather Information this, Whatweb give contribution in identify hole website security. Information about the web servers, platforms, plugins and extensions used can help in identify specific vulnerability related with technology. If anything known vulnerabilities related with version device soft or configuration used, Whatweb can give warning about potency vulnerability. Information about visible files and directories or can accessible to help in identify gap possible security possible access no legitimate or data theft. With so, Whatweb role in gather relevant information for analysis vulnerability and help in identify hole security on the website with give outlook about technology and configuration used.

2.2.2. Scanning Website Ports using Unicornscan

Unicornscan is a network scanning tool designed to perform the scanning process with efficiency and speed that is considered quite high because it can scan large networks in a short time. This tool can process port scans as well as website protocols simultaneously, which will allow in identifying services running on a particular port. Not only that, unicornscan is capable of processing Ping, SYN and UDP scan types. Unicornscan is capable of performing scans unexpectedly, this can make it possible to check network security without triggering firewall detection.

Port scanning involves sending packets to open ports and checking for a response to SYN requests, which can be viewed as suspicious activity. The possibility of an attacker attack will also be considered in this scanning process, because the attacker can send data by varying the port on which the script is used to run the script [14].

In other studies, also stated that Unicornscan is one of the tools used in paper to perform port scanning attacks. It is a fast and lightweight network scanner that sends packets to the target host and analyzes the responses to determine open ports and services. The paper mentions that the most recent version of Unicornscan available in the Kali Linux repositories was used for generating attack datasets.

Function of the website port scanning using Unicornscan is for analyze open ports or can accessed on the AB and XY Office websites.

Website port scanning using Unicornscan is A tool or device software used for scan for open ports on a system or network. Objective from use Unicornscan in study this is for:

1. Identification: Through port scanning using Unicornscan, researcher can identify open ports on the AB and XY Office websites. Information about open ports this important because can give instruction about service or application running behind the port. Ports that do not should open or open without clear need can show exists configuration that does safe or possible vulnerabilities can exploited by attackers.
2. Scanning vulnerability Related Port: After identify open ports, researcher can continue with do scan vulnerability related to that port. This involves use tool or another method for test security service or application running on that port. For example, if found HTTP port (Port 80) open, researcher can continue with use tool like Nikto or OWASP ZAP for look for vulnerability Specific against a web server running on that port.
3. Understanding Infrastructure Network: Through port scanning, researchers can also obtain outlook about infrastructure network used by the AB and XY Office websites. Information about open ports and services running behind them can give description about architecture networks and systems used. this can help researcher understand potency attack that can done to infrastructure it and give recommendation appropriate security.

With use Unicornscan for do website port scanning, research this can complete analysis vulnerability with check for open ports on the AB and XY Office websites. The results of port scanning can be help in identify potency vulnerability, test security services running on that port, and delivers more understanding Good about infrastructure network used. All this will contribute to the effort increase website security and protect the data stored on it. This tool contributes in identify hole security with gather information Specific about open ports and services running on them. Following is a number of information specific can collected by Unicornscan:

1. Open Ports: Unicornscan can identify open ports on a system or network. Information this help in know service or possible protocol running on that port, such as HTTP port (80), HTTPS port (443), or SSH port (22).
2. Banners and Versions Service: Unicornscan also available gather information about banners and versions services running on open ports. Information this can give instruction about type running service and version device software used. Version device existing software worn or prone to can disclose potency possible vulnerabilities exploited by attackers.
3. Protocol Network: Unicornscan can identify protocol network that is used on an open port, such as TCP (Transmission Control Protocol) or UDP (User Datagram Protocol). This help in determine type running service and proper method for continue analysis more continue.
4. Response Service: Unicornscan can analyze response or the response given by the service on an open port. Response this can give information addition about running services, structure the protocol used, or possibility gap related security.

With gather Information this is, Unicornscan contribute in identify hole security with explore open ports and services running on them. Information about open ports, banners and versions service, as well protocol network help in identify type possible service prone to or need checked more continue. If version device existing software worn or prone to detected, this can give instruction about possible vulnerabilities exists and is necessary repaired. Besides that, information response service can give more understanding in about protocol used and help in do analysis more carry on to services running on that port. With so, Unicornscan role in gather information about open ports, running services, and responses service for identify hole security and deliver outlook about possible vulnerabilities is on the system or medium network analyzed.

2.3. Vulnerability Assessment Analysis Website

At the analysis stage, this website vulnerability assessment is part of the process of identifying and classifying security holes based on the maturity level of implementing controls on a website [8]. The need to consider a risk in conducting vulnerability assessment in a design of threat modeling that allows one to find problems in application testing [14].

The investigation process involves obtaining information and identifying the website being assessed based on the analysis. This can be used as a score in updating its website security improvements for both destinations. This method is intended to determine the level of site vulnerability. There are various tools for scanning for vulnerabilities through sniffing attempts aimed at The activities that fall under this category include collecting information, The activities involved in this context include attempting to breach wireless networks, cracking passwords, using forensic tools to investigate security incidents, spoofing to manipulate information, and compromising electronic devices [14]. This process involves the use of special tools namely OWASP ZAP, Burp Suite, Skipfish, Wapiti, Rapidscan, and Nikto.

The website vulnerability assessment's analysis phase covers the website's creation, which involves various vulnerabilities such as SQL injection. During the analysis phase of website vulnerability assessment, vulnerabilities such as insecure authentication and session management, cross-site scripting (XSS), misconfigured security settings, insecure direct object references, and exposure of sensitive data are identified. Basic scanning techniques are also used in this phase [15].

SQL injection is a technique that combines code injection by adding several viruses that can break the database structure contained on the website. Not only that, this technique will attack the firewall layer wall on a network that does not have attack defense [16]. Attackers will circumvent authentication and authorization to retrieve vital information. In some cases, SQL injection techniques often cause various perceptions that excessive data leakage will be a concern for administrators to be more able to handle these conditions seriously, SQL injection uses the POST method in order to store data [17], [18]. Script coding injection in this technique has several queries to retrieve data performed by the attacker, namely by writing" SELECT Column1, Column2 FROM Table1 WHERE Column3=4", by adding some other queries such as "UNION" or ">=12" [19].

Broken authentication is a common vulnerability related to the implementation and technicalities of authentication in applications, this can make attackers run an impersonation permanently or temporarily. Misconfigured session management causes authentication failures. Once the authentication process is completed, data communication for a specific user becomes possible [20].

The need for efforts to store confidential data and the need for protection of sensitive data exposure components [17]. Broken access control is a technique performed by some attackers in manipulating unauthorized paths, so as to access data functionality that has been protected. Security misconfiguration is a vulnerability that OWASP tools have, which refers to the use of attack system configurations.

Cross-Site Scripting (XSS) attacks are categorized as vulnerabilities that are exploitable through cross-web scripting, which involves injecting insecure data into web pages with the intention of executing malicious code [17], [21], [22], [24]. So that there is a technological relationship in creating website content by getting the code executed in the browser [25]. XSS will work when the website provides invalid input, because it can allow attackers to commit piracy [15], [18], [26]. XSS will give some warnings using a "string" code of the form " alert(1)" to be sent to HTTP, so XSS can provide an observation in the penetration testing process to use payloads "<script> alert(1);< /script> or on error ="alert(1);" [23]. The payload will identify if a keyword is found that is classified as vulnerable to the threat of an attacker, so there will be a URL action inserted with the code that was previously injected [24]. There is a parameter located on the HTML page, where the parameter will run a code at the time of the attack.

Insecure deserialization is often used to transmit a dataset over a network, this is done to protect the data. It requires a code deserialization to be implemented so that the attacker cannot perform a malicious transmission process with exploit attempts [19].

CSP is a component of vulnerability analysis that is capable of processing a script for website exploitation. The need to use rendering engines such as Firefox or other web browsers to be able to call the onload function, the purpose is to collect a hash value on the generated script after accessing the page and sending it to a third party. This element is responsible for creating a Content Security Policy (CSP) header that can gather multiple reports from a website, in cases where the website does not already have a CSP header it will be adjusted to the existing CSP database. There are some uses of CSPs that are based on JS code with the process of removing scripts contained in the CSP database. If a website does not use JS code, then the website is not secure [12].

CSRF is a component of the top 10 vulnerability analysis, which is useful in performing fraudulent requests that allow attackers to modify databases so that website owners cannot distinguish servers based on legitimate or invalid requests [28], [29]. Objective from use method this in study the is as following:

1. Identify Vulnerability: Method this aim for identify possible vulnerabilities There is on the AB and XY Office websites. Through analysis vulnerability, researcher can find gap security, vulnerable configuration, or Disobedient to practice good security that can be exploited by attackers. With identify vulnerability here are the steps proper safeguards can take for repair and protect the website.
2. Measure Risk: Vulnerability Assessment Analysis Website helps in evaluate possible risk related with vulnerabilities found. Researcher can categorize vulnerability based on level severity, probability exploitation, and impact potential. With so, researchers can prioritize action security based on risks posed by each vulnerability.
3. Give Recommendation Security: After identify vulnerability and measure risk, goal from the Vulnerability Assessment Analysis Website is give recommendation appropriate safeguards. Recommendation this can cover steps for repair vulnerability, apply practice more security well, configure repeat system or application, or use solution security addition. Recommendation this assist AB and XY Office in increase the security of their website and protect the data stored on it.
4. Provide Results Report: The results of the Vulnerability Assessment Analysis Website are disclosed in form report. Report this containing summary findings vulnerability, level risks, and recommendations security. Report this can used as base for communicate findings and recommendations to interested parties, e.g., website manager, team security, or management organization.

With use Vulnerability Assessment Analysis Website method, research this aim for give comprehensive understanding about vulnerabilities exist on AB and XY Office websites. This allows AB and XY Office to take necessary action to use repair vulnerability, increase website security, and protect sensitive data from potency attack or exploitation by unauthorized parties authorized. In the Vulnerability Assessment Analysis process on the website, several tools and techniques scan used for gather information specific and contributing in identify hole security. A number of information that can collected through analysis this among others:

1. Scanning Vulnerability Scanning: Scan tool vulnerability such as OWASP ZAP, Wapiti, and Nikto used for identify vulnerabilities that exist on the website. Tools this in a manner automatic scan the website and search common vulnerabilities related with bad configuration, vulnerability device known software, loopholes security on the code, and frequent attacks done.
2. Identification vulnerability Related Configuration: Scan tool vulnerability can gather information about configuration used on the website. For example, if web server configuration does adequate or There is settings that do not safe tool the can identify and report related vulnerabilities with configuration the. Information this can help in identify possible vulnerabilities repaired with change more configuration safe.
3. Invention vulnerability Related Device Software: Scan tool vulnerability can look for version device software used on the website and compare them with known vulnerabilities. If version device vulnerable software detected, tool will give report about related vulnerabilities with version the. Information this important Because device existing software worn or no updated can become target attack.
4. Invention Vulnerability in Code: Apart scan vulnerability general, tools scan vulnerabilities too analyze code web resources for look for gap security. the tool can find vulnerability related with bad input validation, execution code that doesn't safe, or gap security others contained in the code application.

In other similar research tool this used Because diverse utility [13], vulnerability assessment databases can help improve the security of cloud-based web applications by providing developers with a comprehensive list of known vulnerabilities and their associated risks. This information can be used to identify potential security threats and prioritize remediation efforts. Additionally, vulnerability assessment databases can be used to track the status of vulnerabilities over time and ensure that they are properly addressed as new patches and updates become available.

2.4. Analysis of Vulnerability Assessment Website AB using OWASP ZAP, Wapiti, Nikto

In this method, researchers need to collect information related to the system or website that is used as a target to be tested. The test was carried out using OWASP, Wapiti and Nikto techniques to find several security holes or a vulnerability on the target website.

2.4.1. OWASP

OWASP has information security risk assessment parameters and This tool has two functions. That is, website vulnerability analysis and risk identification, as well as technical recommendations for components that need improvement [19], [30], [31]. OWASP ZAP can carry out a plan in analyzing the results of the analysis by taking an action, stages of implementation, and actions that have been prepared [26]. This relates to methods based on the analysis of key risk factors, vulnerability factors, threat agents as well as technical and business impact factors [32]. OWASP also has a feature in conducting website penetration tests, so that several types of threats will be found with various levels to prevent these attacks, OWASP strives to optimize the target based on the level of vulnerability resulting from exploitation [27], [28]. As for Functions from OWASP is as following :

1. OWASP ZAP is tool testing security source open used for perform automatic scanning against the website.
2. This tool used for identify possible vulnerabilities There is in the AB website with do series test security like search SQL injection vulnerabilities, cross-site scripting (XSS), and common attacks to web application.
3. OWASP ZAP does to help in do analysis configuration security and test reliability system authentication and authorization.

As for Purpose from OWASP is as following:

1. identify vulnerability possible security it's on AB's website using automatic scanning technique.
2. Do series test security for find gap possible potential exploited by attackers.
3. Give report detailed results about vulnerabilities found as well as recommendation appropriate safeguards.

OWASP ZAP (Zed Attack Proxy) is tool scan security designed web application for identify and test vulnerability web application security. This tool developed by the Open Web Application Security Project (OWASP), a security - focused global community web application. OWASP ZAP contributed in identify hole security with do various type testing and analysis web application security. Following is a number of information specific can collected by OWASP ZAP:

1. Scanning Vulnerability: OWASP ZAP got do scan vulnerability in a manner automatically on web applications. This tool try find various type vulnerability, incl gap general security related with poor input processing, weakness configuration, attack injection (SQL, XSS), and still Lots again.
2. Search vulnerability Related Configuration: OWASP ZAP can detect configuration that does secure on web applications, e.g., bad server settings, drawbacks cryptography, or policy weak security. Information this help in identify possible vulnerabilities repaired with change more configuration safe.
3. Exploitation Vulnerabilities: Besides scan vulnerabilities, OWASP ZAP can also do exploitation to successful vulnerability found. This tool can operate attack simulation and show possible impact happen if vulnerability no repaired. This help developers and researchers' security for understand potency attacks and their consequences.
4. Data and Traffic Analysis Network: OWASP ZAP got analyze the data and then cross sent network between web applications and clients. This including identifies attack or activity suspicious, check existence information sensitive which is not should revealed, and confirmed obedience to practice recommended security.

With gather information, OWASP ZAP contributed in identify hole security with method following:

1. Identify Possible Vulnerabilities Exploited: OWASP ZAP helps in identify possible vulnerabilities exploited by attackers in web applications. With do comprehensive scanning and analysis, Tools this can find possible vulnerabilities utilized for access or manipulate sensitive data, damage function application, or do attack other.
2. Give Reports and Recommendations Repair: After scan done, OWASP ZAP generates a report that lists the vulnerabilities found along details. Report this help team developer or security for prioritize and improve detected vulnerabilities. This tool also delivers recommendation security Specific For overcome vulnerabilities found.
3. Support Testing Continuous Security: OWASP ZAP got used as part from the testing process sustainable security. This tool possible user for do scan in a manner periodically or automatic for identify vulnerability new possible appear after changes to the web application or infrastructure.

With so, OWASP ZAP is important tool in identify hole web application security. With do scan vulnerability, looking for vulnerability related configuration, and do analysis to data and past cross network, Tools this help in identify existing vulnerabilities and deliver recommendation proper fix. Study the former also shows that OWASP tools, OWASP stands for Open Web Application Security Project. It is a non-profit organization that aims to improve the security of software and web applications. OWASP provides resources, tools, and guidelines for developers, security professionals, and organizations to build secure applications and protect against common web application vulnerabilities such as SQL injection, cross-site scripting (XSS), and others.

2.4.2. Wapiti

Wapiti is an official and open-source vulnerability scanning tool that runs on the Linux OS. Wapiti can carry out the testing process based on component adjustments to website creation. Other research is also becoming reason Why tool This used [29], Wapiti is an open-source web vulnerability scanner that was evaluated in the paper. It is implemented with a command-line interface (CLI) and requires more technical knowledge from the users. The comparative evaluation study conducted in the paper did not show significant differences among the evaluated scanners, including Wapiti, in terms of their capabilities in detecting common web vulnerabilities. Function from Wapiti tool is as following:

1. Wapiti is tool testing security used for detect vulnerabilities in web applications with use technique known attack.
2. This tool does inspection to the input parameters sent to the website and try find gap such as SQL injection, cross-site scripting (XSS), and vulnerabilities against disclosure files.
3. Wapiti can too test security web page with identify vulnerability like directory open or related weaknesses with arrangement HTTP security.

Objective dare use Wapiti tool is as following:

1. Testing the AB website using known attacks for detect gap existing security.
2. Do input parameter checking and testing security web page for identify possible vulnerabilities exploited by attackers.
3. Give report results that include vulnerabilities found and recommendations the necessary safeguards.

Wapiti is tool scan designed security special for identify vulnerability web application security. The goal is for test web application against various type attacks, such as SQL injection, XSS (Cross-Site Scripting), and LFI (Local File Inclusion) attacks. Following is explanation about Wapiti, information collected, and their contributions in identify hole security:

1. Scanning Vulnerabilities: Wapiti do scan vulnerability in a manner automatically on web applications. This tool sends series request to the web server for inspect existence gap security common, like vulnerability injection, gap security configuration, weakness encryption, and vulnerabilities others generally exploited by attackers.
2. Identification XSS and SQL Injection Attacks: Wapiti special focus on identification XSS and SQL injection attacks are common happens in web applications. This tool try insert script malicious and bogus SQL queries to in the submitted input to the web server for see is application prone to attacks the.
3. Analysis Website Structure: Wapiti also analyzes website structure for look for vulnerability related configuration or construction that is not safe. This tool try identify files or directory that can accessed in a manner no valid, URLs that are not protected, or other possible features can be exploited by attackers.
4. Build Report: After scan done, Wapiti generates a report that lists the vulnerabilities found along details. Report this covers information about type successful attack done, the associated URL with vulnerability, and some information helpful addition in understand characteristic vulnerability.

Through the information collected, Wapiti contributed in identify hole security with method following:

1. Detect vulnerability General: Wapiti helps in identify vulnerability common frequently happens in web applications. With test application to XSS attacks, SQL injection, and vulnerabilities general other, Tools this help reveal possible vulnerabilities exploited by attackers.
2. Providing Evidence and Detailed Information: Reports generated by Wapiti provide proof concrete about vulnerabilities found. This help team developer or security in understand vulnerability with more ok and fix it.
3. Increase Awareness will Security: With using Wapiti, awareness will importance security web application can improve. This tool help educate developer and owner application about gap possible security is in the application them and pushed steps more security ok.

With thus, Wapiti constitutes tool important in identify hole web application security. With do scan vulnerabilities, focus on XSS and SQL injection attacks, as well analysis website structure, Wapiti helps find and uncover vulnerability necessary security fixed in web application.

2.4.3. Nikto

Nikto is a testing tool that has tested as many as 6700 programs classified as malicious files, while 1250 versions of applications that do not get updates. Nikto can check multiple file indexes through HTTP servers [30]. HTTP is a combination of HTTP and SSL which is classified as a website marked with a green display in the browser search field. Reason use Nikto as tool analysis is [31] Nikto is a free software command-line network security analysis automated scanner that is used to scan web sites and servers for known misconfigurations and security vulnerabilities. It is a tool that helps in identifying vulnerabilities in web applications. To use Nikto, one can enter the syntax "Nikto -h hostname" in the command-line. The assessment of the Nikto tool in the paper found that only the top websites from a few domains exploited the header while the remaining domains did not use header files and informational alerts were found. Function from Nikto in study this is as following:

1. Nikto is tool testing security used for perform a vulnerability scan on the web server.
2. This tool analyzes AB's website for look for gap security like directory open, the file can be downloaded, and vulnerabilities to known web server attacks.
3. Nikto can to inspect version device software used on web servers and delivers information about related vulnerabilities with version already worn or vulnerable.

Objective from Nikto in study this is as following:

1. Identify vulnerability in the web server used by the AB website with perform automatic scanning.
2. Do inspection to directory open, the file can be downloaded, and common attacks against web servers.
3. Give report results that include findings vulnerability, information version device vulnerable software, and recommendations for overcome vulnerabilities found.

Nikto is one tool scan security used for identify vulnerabilities in web applications. This tool designed special for detect gap general security happens on a web server, like weakness configuration, files that are not should can accessible, and vulnerabilities related with device software used. Following is explanation about Nico, information collected, and their contributions in identify hole security:

1. Scanning Weakness General: Nikto in a manner automatic do scan against the web server for look for weakness common frequently happens in web applications. This tool try find related vulnerabilities with configuration that does safe, loophole security related with directories and files, as well vulnerability to attack famous such as SQL injection, XSS, and so on.
2. Analysis Device Software Used: Nikto also analyzes information device software used on web servers, incl version device software, patch levels, and associated vulnerabilities with version the. Information this help in identify known vulnerabilities on version device software used, so can take right action for overcome vulnerability the.
3. Identification Weakness Configuration: Nikto try identify weakness in web server configuration that can give access no legitimate or open gap security. For example, Tools this will look for settings that do not safe like directory that can accessed public, used vulnerable protocol, or featured that are not need to get exploited by attackers.
4. Build Report: After scan Done, Nico produce a report that lists the vulnerabilities found and related details. Report this give information about type vulnerabilities, associated URLs, and possible action suggestions taken for repair vulnerability the.

Contribution Nikto in identify hole security is as following:

1. Detect Known Vulnerabilities: Nikto help in detect known vulnerabilities on web servers and devices software used. This tool identifies common vulnerabilities happened and gave important information for owner system for take steps appropriate repair.
2. Give Information Vulnerable Configuration: Nikto help in identify weakness in web server configuration that can show gap security. With give information about settings that do not safe tool this possible owner system for overcome problem possible configuration exploited by attackers.
3. Increase Awareness will Security: With use Nikto, awareness will vulnerability security on the web server can be improved. This tool help educate owner system about gap possible security there on their server and shove steps more security ok.

Kindly Overall, Nikto is useful tool in identify hole web application security do scan vulnerability, analysis device software and configuration, as well provide helpful report owner system take necessary action for repair vulnerability the. With use tools such as OWASP ZAP, Wapiti, and Nikto, research this aim for do analysis comprehensive vulnerability on the AB website. Tools the used for identify and document vulnerability security is there, so allows AB Office to take right action to use repair vulnerability it and improve their website security in East Java. OWASP ZAP, Wapiti, and Nikto is the tools used in study for do evaluation website security. Following is comparison and evaluation to third tool these:

1. OWASP ZAP:
   a. Pros: OWASP ZAP is comprehensive and powerful tool for identify vulnerability web application security. He provides various features that include scan automation, manual testing, and integration with tool testing other. OWASP ZAP also has an active and sustainable community that ensures constant updates and improvements.
   b. Limitations: Although OWASP ZAP has Lots features, use Possible need deep understanding about web security. This tool tends complex for users who haven't experienced in testing security.

2. Wapiti:
    a. Pros: Wapiti is test - focused tool web vulnerabilities and have simple and easy interface used. This tool support scan automatic and manual, as well can detect various vulnerability general such as SQL injection and cross-site scripting (XSS). Wapiti also supports testing for HTTP GET and POST methods.
    b. Limitations: Wapiti possible no comprehensive like OWASP ZAP and some tool other. He Possible no own level the same comprehensiveness and flexibility in matter features and settings possible testing done.
3. Nikto:
    a. Pros: Nico is powerful tool for identify vulnerability common on web servers and web applications. This tool fast, easy use, and provide scan vulnerability - focused automation general like directory open, forgotten files, and vulnerable scripts. Nikto also provides structured report for results scan.
    b. Limitations: Nikto possible no give level depth same scan like OWASP ZAP or more tools sophisticated. Hetends focus on vulnerability common and possible no detect more vulnerability Specific or new.

Comparison this depending on needs testing specific security and level skill user. Every tool owns its advantages and limitations himself, and election the right tool depending on context and purpose testing.

2.5. Vulnerability Assessment Analysis using Burp Suite, Skipfish, Rapidscan

2.5.1. Burp Suite

Burp Suite was invented and founded in 2004 as a security testing tool for web applications. Web application protection testing programs have become an option for the use of a growing method of detecting bugs in APIs as well as mobile applications. To test the security of an application effectively, one must understand the various vulnerabilities in the application [38]. Study kind also explained about Burp Suite is a web proxy tool that is mentioned in the paper. It is used for intercepting and modifying HTTP traffic between a web browser and a web server. It can be used for security testing and vulnerability scanning of web applications [32]. The Burp suite was also selected Because reason [33] Burp Suite is an open-source security tool used for performing and testing security features of web applications. It is used in this study to capture the flow of data by setting it as a proxy listener which acts as a local HTTP proxy server. The proxy listener intercepts all the requests on port 8080 of the loopback interface. By configuring the web browser in the attacker's system as a proxy server, packets are routed through the Burp Suite. In Burp Suite of attacker system, intercept parameter is set to on and interface gains access to all data values flow from client to ThinkSpeak server for the fixed period of time.

Burp Suite is one tool important in testing penetration and analysis security web application. This tool own various useful features for identify hole security and test strength security web application. Following explanation about Burp Suite Functions:

1. Scanning Vulnerability: Burp Suite allows scan vulnerability automatically on web applications with send series attack against the specified target. This tool tries various type attack like SQL injection, XSS, CSRF and more For identify existing vulnerabilities.
2. Intercepting Proxy: Burp Suite works as a possible proxy user for monitor and modify requests and responses sent between the browser and the web server. This possible detection and manipulation attack like injection, buffer redundancy, and parameter manipulation.
3. Website Spidering and Mapping: Burp Suite can do web site indexing (spidering) and mapping automatic for identify all parts and functions web application. This help in ensure no there is a forgotten area or vulnerable hidden to attack.
4. Analysis Manual Vulnerability: Aside feature automatically, Burp Suite also provides tool for do analysis manual vulnerability. This possible analysis deep to complex vulnerabilities or no can detected in a manner automatic.

The Information Collected by Burp Suite is as following:

1. Request and Response: Burp Suite records every request and response sent between the browser and the web server. Information this including URLs, parameters, headers, cookies, as well content and code source web page. This help in analyze interaction between web applications and users as well as identify potency vulnerability.
2. Vulnerability Related Version Device Software: Burp Suite can identify version device software and related vulnerabilities with version the. Information this help in estimate level vulnerability based on version device software used on the web server.

Burp Suite contribution in identify Hole Security is as following:

1. Scanning vulnerability Automatic: Burp Suite helps identify vulnerability common on web applications with do scan automatic. This tool sends series attack against the target and analyze response for look for indication vulnerability like gap injection, XSS vulnerabilities and so on.
2. Intercepting Proxy: Burp Suite's proxy feature makes it possible user for monitor and modify requests and responses sent between the browser and the web server. This help identify possible vulnerabilities missed in scan automatic, as well possible testing more attacks deep.
3. Analysis Manual Vulnerability: Burp Suite provides powerful tool for do analysis vulnerability manually. This possible user for exploring and auditing web application for deep, seek complex vulnerabilities or no detected in a manner automatic.

Kindly overall, Burp Suite is very useful tool in identify hole web application security. With feature scan vulnerability automatic, proxy intercepting, and capabilities manual analysis, Burp Suite helps in identify existing vulnerabilities, monitor interaction between web applications and users, as well give required information for repair hole detected security.

2.5.2. Skipfish

Skipfish is an open-source web application scanning tool with a C programming structure, the purpose of This tool is similar to the use of nmap and nessus, but skipfish allows web development to be able to do reconnaissance. Skipfish is designed to find vulnerabilities before hackers perform the exploitation process. This tool can define code within websites against XSS, SQL and XML injection attacks [41]. Study earlier in use skipfish tools shows that Skipfish is an open-source web application scanner tool that is used to find vulnerabilities in web applications before a hacker can exploit them. It is similar to other web security hole scanners like Nmap and Nessus. Skipfish can be used to scan web applications or sites for possible security problems that might exist. It can operate on various operating systems like Linux, BSD, MAC, and Windows. Skipfish can be used to determine whether the codes on a web site are vulnerable to common attacks such as cross-site scripting (XSS), SQL, and XML injection attacks. The final report produced by This tool is intended to function as a basis for security assessment of web applications [34].

Skipfish is tool scan testing - focused security structure and content web application. This tool used for evaluate security and identification related vulnerabilities with configuration, settings, and structure web application. Objective use Skipfish in study this is for do scan on the AB Office and XY Office websites. This tool used for analyze structure web application, search vulnerability related configuration that does secure, and identify gap possible security there. Objective Finally is for give recommendation necessary repairs For increase security the web application. Skipfish is tool scan security used for test security web application and identify hole security. Following is explanation about Function Skipfish that is Scanning Structure and Content: Skipfish do scan structure and content web application for thorough For identify vulnerabilities and gaps security. This tool try map whole structure web page, including URL, parameters, and features other, for look for potency vulnerability. Then Information Collected by Skipfish are:

1. Structure Web Application: Skipfish gather information about structure medium web application analyzed. This includes URLs, parameters, and hierarchy’s page. Information this useful for mapping and understanding more carry on about medium web application analyzed.
2. Vulnerability Related Configuration: Skipfish try identify related vulnerabilities with configuration that does safe. For example, Tools this can detect If arrangement file access or server configuration is not sufficient and acceptable cause vulnerability security.

Contribution Skipfish in identify Hole Security:

1. Scanning vulnerability Structured: Skipfish do scan structured on web application for identify gap possible security there. With map structure web application for thorough, Tools this can find related vulnerabilities with configuration, settings, or implementation that doesn't safe.
2. Detection vulnerability Configuration: Skipfish can identify related vulnerabilities with configuration that does safe. This tool can disclose server settings are not secure, file permissions are not right, or configuration others can show vulnerability in web application.

With focus on scanning structure and content web application, Skipfish contribute in identify hole security with look for related vulnerabilities with configuration, settings, and implementations are not safe. This tool helps complete scan vulnerability in a manner thorough in effort increase security web application.

2.5.3. Rapidscan

Rapidscan is a multiscanner testing tool that features a combined scan from several website scanning tools. Rapidscan is tool scan security automatically used for identify vulnerabilities in web applications. This tool can do scan to web application and search vulnerability common frequently happened. Objective use

Rapidscan in study this is for do scan vulnerabilities on AB Office and XY Office websites. This tool used for look for vulnerability general such as SQL injection, XSS, LFI, and others. Objective Finally is for identify vulnerability and deliver recommendation necessary repairs for increase security web application. kindly overall, function of the respective tools (Burp Suite, Skipfish, and Rapidscan) in study this is for do scan vulnerability, identify gap existing security, and deliver recommendation necessary repairs for increase security AB Office and XY Office web applications in East Java. Rapidscan is tool scan security automatically used for identify hole web application security. Following is explanation about Function Rapidscan:

1. Scanning vulnerability Auto: Rapidscan do scan automatic to web application with try various type common attacks and scenarios used by attackers. This tool looks for common vulnerabilities happen like SQL injection, XSS vulnerabilities, LFI (Local File Inclusion), RFI (Remote File Inclusion), and so on.
2. Analysis Configuration Security: Rapidscan also analyzes configuration security on the web server for look for possible gap exploited by attackers. This tool try detect vulnerable configuration like file permissions are not right, server settings are not safe, or parameters that are not protected.

Following is Information Collected by Rapidscan:

1. Vulnerability Regarding User Input: Rapidscan identify related vulnerabilities with user input like SQL injection, XSS, and the like. This tool try utilize gap possible security happen when user input No processed with right by the web application.
2. Configuration Security: Rapidscan also tried identify vulnerability related configuration security on web servers. Information collected covers version device vulnerable software, server settings are not safe, or other possible configurations show vulnerability in web application.

Contribution Rapidscan in identify Hole Security is as following:

1. Scanning Auto: Rapidscan help identify hole web application security do scan automatic. This tool try scenarios and attacks usual general exploited by attackers. With do scan auto, Rapidscan can reveal possible vulnerabilities missed or no detected with manual testing.
2. Identifier User Input Vulnerability: Rapidscan focus on related vulnerabilities with user input. With test method web applications respond to and process user input, Tools this help identify gap possible security exploited by attackers.

Kindly whole, Rapidscan role in identify hole web application security do scan automate and analyze configuration security. This tool help increase security web application with disclose possible vulnerabilities exists and is possible action proper fix done.

Burp Suite, Skipfish, and Rapidscan is the tools used in study For evaluate website security. Following is comparison and evaluation to third tool these:

1. Burp Suite:
   a. Pros: Burp Suite is very powerful and comprehensive tool for testing security web application. He provides various features that include scan automated, manual testing, recording and playback HTTP reset, analysis vulnerability, and manipulation request. Burp Suite is also supported integration with other tools and have active community.
   b. Limitations: Although Burp Suite has Lots features, use Possible need deep understanding about web security. This tool tends complex for users who haven't experienced in testing security. Besides it, version complete Burp Suite is product paid, though there is also a free version available with limited features.
2. Skipfish:
   a. Pros: Skipfish is light and fast tool for testing web security. He owns ability for identify vulnerabilitygeneral such as SQL injection, cross-site scripting (XSS), and directories open. Skipfish can run with easy and give structured report about vulnerabilities found.
   b. Limitations: Skipfish Possible No comprehensive like Burp Suite inside matter features and levels completeness testing. This tool tend focus on vulnerability common and possible No detect more vulnerability Specific or new. Neither does Skipfish Again active developed by the developer, so Possible No get update latest.
3. Rapidscan:
   a. Pros: Rapidscan is the tools it consists of from several sub- tools such as Fierce Bruter Subdomain, SSLyze, NMAP, and Wafw00f, which are used for test website security from various aspect. This tool covers subdomain scanning, SSL analysis, port scanning and web firewall detection. Rapidscan give comprehensive results in One Suite tool.

b. Limitations: Rapidscan Possible No own level depth testing and completeness the same features like Burp Suite. Besides that's ability testing Rapidscan Possible limited to vulnerabilities and components already known, and possible No effective in detect more vulnerability Specific or new.

2.6. Website Testing Brute Force Attack

In this step, it is necessary to conduct practical experiments as a form and effort of researchers in providing real results. Researchers will conduct experimental attempts with brute force attacks on the AB and XY Service websites. Later it will be known which website between the two is classified as having a website security creation structure with higher integrity.

There are several ways or possibilities that can be done in carrying out attacks, namely in 2 ways such as active and passive attacks. Attempted active attacks can be carried out by testing tools by tampering with information, falsifying messages and denying service. Likewise with passive attacks, where this attack is carried out in the form of manipulating information from the object being targeted without the consent of the administrator [4].

Brute force attacks fall into the category of phishing with penetration testing that allows attackers to manipulate emails, but some studies have shown that such attacks do not provide true accuracy, so this has little effect in real life [35]. Brute force attacks can be prevented using a series of algorithms with vendor redirects and frequently changed password attempts. Another solution is that it is recommended to lock the account with time constraints.

Penetration testing also needs to have an understanding that there needs to be detailed information collection, the test will map information from IP addresses and open the website port network. This penetration testing is carried out in various experiments in analyzing the gaps connected in a system into the network.

Study earlier is [36] with results The paper proposes a deep learning-based intrusion detection system for detecting brute force attacks on MQTT-IoT networks. The proposed system uses a recent dataset, MQTT-IoT-IDS2020 dataset, to train the deep learning model with a high number of instances and using flow-based features. The classification model is very accurate in detecting such attacks with more than 99% accuracy in discriminating between normal and brute force attacks. The proposed system can be used by IoT network administrators to detect and prevent brute force attacks on their networks, which can lead to severe damage on IoT networks. The paper also provides two feature sets, Bi-flow features and Uni-flow features, which can be used by researchers and practitioners in the field of IoT security for developing intrusion detection systems for other types of attacks.

Brute force attack is attacks carried out with try all possibility password combination in a manner over and over again until find the correct password. Objective main from use method this in study the is as following:

1. **Test Password Strength**: Methods this aim for test password strength used on the AB and XY Office websites. With do brute force attack, researcher can inspect what is the password used own enough complexity tall or easy guessed. If the password is weak found, p this can show exists weakness necessary security repaired.
2. **Identification Potency Attack**: With perform a brute force attack, researcher can identify potency attacks on websites. If the brute force attack is successful, p this signify that the website does own adequate mechanism for protect account user from attack repeated password attempts. Researcher can use results this for give recommendation appropriate safeguards, e.g., apply more password policies strong or enable feature protection to brute force attack.
3. **Realize Risk Security**: With see how much websites vulnerable to brute force attack, researcher can increase awareness about risk possible security faced by AB and XY Office websites. Brute force attack can used by attackers for get access No legitimate to account user or restricted area other on the website. With know potency risk here are the steps appropriate safeguards can taken For protect the website and the data contained in it.

In context study this, usage Website Testing Brute Force Attack method aims for identify vulnerability security related with the passwords used on the AB and XY Office websites. Result of testing this can help in identify weakness security, deliver recommendation for increase password complexity and implement steps security addition for protect websites from brute force attack. Testing Brute Force Attack is one method testing security used for test password strength (password) on a system or application. Brute Force Attack is involving techniques test repeated with try all combination Possible from password until find the right. Following is explanation about Functions of Testing Brute Force Attack:

1. Test Password Weaknesses: Methods this used for test weakness system security password related with try various password combination in a manner repeated. The goal is for look for know how much easy or difficult system or application the can accessed use technique Brute Force attack.

2. Evaluate Password Strength: With try various password combination, Testing Brute Force Attack can help evaluate password strength used in system. If system easy penetrated with Brute Force attack, hence the password Possible vulnerable and must strengthened.

Information Collected by Testing Brute Force Attack is as following:

1. Password Test: Testing Brute Force Attack try various password combination for look for now the correct password. Tool or script used will repeat series password test until find valid.
2. Time Required: Information collected is time required for try every password combination. This can give indication how much easy or difficult for guess the correct password.

Contribution of Testing Brute Force Attack in identify Hole Security is as following:

1. Identifying Weak Passwords: With do Brute Force attack, method this can identify weak passwords or vulnerable. If system or application allow easy passwords guessed or no strong, Brute Force attacks can with easy it worked. This gives instruction that system need strengthen password policy or apply mechanism protection addition.
2. Increase Awareness Security: Through Testing Brute Force Attack, organization or developer can realize importance use of strong passwords and policies proper security. Brute Force attacks often become the simplest and most effective method for attacker for get access no valid. With test password strength, they are can increase policy security and awareness importance strong password protection.

3. RESULTS AND DISCUSSION

In this section, some information related to security holes found on the target website will be presented during testing by determining the results in the form of a table of improvement recommendations in several sequences of website structure components.

Due to the author's commitment to abide by the code of ethics on information dissemination agreed upon by both AB and XY service agencies, there are certain aspects that cannot be elaborated on in detail. Nonetheless, the following results, steps, and methods were obtained:

In this part, we provide the outcomes of scanning the data services of websites AB and XY using the what web tool test. Some results can be found in the form of network structure information starting at the IP Address Development Framework website.

Table 1 shows the results, starting in the "information" column there is the type of information obtained while in the " whatweb tools" column there is the name of the tool used in the scanning process. In addition, there is identity information from each official website. The column presents the results of the IP address, HTTP server, OpenSSL version, HTTP headers, email address, operating system, website development toolkit, and also the PHP framework used.

Table 1. Information Identity of AB and XY Service Website

Information	Whatweb tools	
	AB Service	XY Service
IP Addresses	103.135.14.1**	36.66.194**.
HTTP Servers	Apache Ver 2.4.46	Apache Version 2.4.29
OpenSSL	1.1.1h	-
HTTP Headers	PHP/7.3.24	-
E-mail	@DinasAB.go.id	@DinasXY.go.id
Operating System	Win64	UbuntuLinux
Website Development Toolkit	-	Bootstrap
PHP Framework	-	Codeigniter

Table 1 in the AB service column displays the IP address with the result 103.135.14.1**, AB service uses an Apache-based HTTP server version 2.4.46 with OpenSSL version 1.1h, the framework used in the AB agency's website structure, PHP Codeigniter, and the Win64 operating system. Table 1 presents the results for Service XY, the IP address of the website is 36.66.194** with Apache HTTP server version 2.4.29 using the Bootstrap website development toolkit, as well as using an Ubuntu Linux-based operating system. Method this used in research earlier [37] with results research The paper discusses the problem of source address validation implementation (SAVI) in a Software-Defined Network (SDN) environment. A common strategy for SAVI is to create bindings between the IP address of a node and a property of the host's network attachment. The proposed D-SAVI framework is designed to filter out packets that do not match existing binding relationships with better packet forwarding efficiency. Therefore, the IP address function is an essential part of the proposed framework.

3.1. Results of Scanning Port Website AB and XY Services using Unicornscan

In this section, the outcomes of the port scanning activity performed on the AB and XY Service website layers using the Unicornscan tool will be presented. Table 2 shows the results of an experimental website port scanning process using unicorn scan on the AB Agency website. The results indicate that the website has three open ports, namely port 80 for the HTTP protocol, port 443 for HTTPS, and port 1723 which utilizes the PPTP protocol. Table 3 shows the results of an experimental unicorn scan website port scanning process running on the XY service website. In this case, the website employs three different ports to facilitate communication with clients over the network. Port 80 is used for the HTTP protocol, which is the foundation for the World Wide Web and enables the exchange of data and information across the internet. Port 443 is used for the HTTPS protocol, which is a secure version of HTTP that encrypts data exchanged between the client and server to prevent unauthorized access or interception. Finally, port 2048 is used for the DLS MONITOR protocol, which is a network protocol that enables remote monitoring and management of devices in a network.

Table 2. Scanning the AB Service website port using Unicornscan

Port Open	Protocol Layers	Results
TCP ports	HTTP Protocol	80
TCP ports	HTTPS protocol	443
TCP ports	PPTP protocol	1723

Table 3. Scanning the port of the XY Service website using Unicornscan

Port Open	Protocol Layers	Results
TCP ports	HTTP Protocol	80
TCP ports	HTTPS protocol	443
TCP ports	DLS-MONITOR protocol	2048

3.2. Results of Analysis Vulnerability Assessment Web Service AB

A result of the vulnerability analysis process of the AB service website will be presented with several testing experiments using different tools including OWASP ZAP, Wapiti, and Nikto. This analysis process is carried out with the aim of providing information about what security holes are detected in the structure of the AB service website.

3.2.1. OWASP Result Testing

Table 4 presents the outcomes of the vulnerability assessment conducted on the AB Dinas website using OWASP tools., there are several components generated in the table such as the Lack of Anti-CSRF Tokens, there are vulnerable JavaScript library components, in addition to the presence of cookie components that do not have HttpOnly, Cookies lacking SameSite attributes. There are several results that are classified as lacking perfect security, namely Leaking Server Details via X-Powered-By HTTP Response Header and also X-Content-Type-Options header not defined components, both of which cannot be defined. In addition, there are some relatively minor vulnerabilities such as the Disclosure of Unix Timestamps.

Table 4. Analysis of the Vulnerability Assessment of the XY Service Website using the OWASP ZAP Tools

Components	OWASP Tools	
	Results	Risk
Lack of Anti-CSRF Tokens	3 detected	Medium
Vulnerable JavaScript Libraries	5 detected	Medium
Lack of HttpOnly flag on cookie	16 detected	Medium
Insecure Cookies	17 detected	Low
Cookies lacking SameSite attribute	19 detected	Low
Leaking Server Details via X-Powered-By HTTP Response Header	16 detected	Low
Disclosure of Unix Timestamps	5 detected	Low
X-Content-Type-Options header not defined	23 detected	Low

The results in Table 4 detected the Lack of Anti-CSRF Tokens component with the discovery that 3 components have been detected with the "Medium" vulnerability category, this allows CSRF attacks that can compromise the integrity and confidentiality of user data. The existence of Vulnerable JavaScript Library components detected as many as 5 components in the same risk level / medium category. This component is considered to be used to perform an attack in the form of XSS. There are some components that do not have HttpOnly Flag, Secure Flag, and SameSite attributes, where these three components are detected as many as

16-19 low-level risks. However, even though the risk is relatively low, there is a possibility that there are still many drawbacks in attributes that cause attacks such as hijacking attempts and cookie theft.

In addition, Table 4 detected several results such as a small vulnerability in the Leaking Server Details via X-Powered-By HTTP Response Header Response Header which gave results of 16 components detected. This provides information that there is technology used on the server. Furthermore, 3 Disclosures of Unix Timestamps components were detected that allow attackers to know sensitive information. There are 23 components generated in the header not defined component. This component allows attackers to manipulate or spoof MIME Types and provide results based on XSS attacks.

Table 4 presents results from evaluation vulnerabilities carried out on the AB Dinas website using OWASP tools. There is a number of the resulting components in table such, like Lack of Anti-CSRF Tokens, vulnerable JavaScript library components, as well exists the cookie component doesn't own attribute Less HttpOnly and Cookies attribute SameSite. There is a number of classified results as lack perfect security, i.e. Overload Server Details through the X-Powered-By HTTP Response Header and also the missing X-Content-Type-Options header components undefined, both No can defined. Besides that, there is a number of relative vulnerability small like Unix Timestamp disclosure. Impact and consequence potential from every identified vulnerability is as following:

1. Lack of Anti-CSRF Tokens: Vulnerability this can possible Cross-Site Request Forgery (CSRF) attacks that can compromise integrity and confidentiality of user data. Attack this can utilise fact that the website does validate incoming requests, so attack can carry out by parties who do not authorize.
2. Vulnerable JavaScript library components: Vulnerability this possible Cross-Site Scripting (XSS) attacks that can cause execution code dangerous on the side client. XSS attacks can used For steal information user, change content page, or do detrimental action user other.
3. Cookie component without attribute HttpOnly, Secure, and SameSite : Lacks attribute this can increase risk attack such as session hijacking and cookie theft. Attack this can result use account that doesn't legitimate, access personal data user, or do action dangerous use identity authenticated user.
4. Overload Server Details via X-Powered-By HTTP Response Header: Vulnerability this disclose information about the technology used by the server. this can give instruction to attacker about version device soft or related vulnerabilities with technology used.
5. Unix Timestamp Disclosure: Vulnerability this possible attacker for obtain information sensitive about time related with system. Although this possible looked as relative vulnerability small, information revealed time can used by attackers for do more attacks complex.

Following is guide about method repair identified vulnerabilities:

1. Lack of Anti-CSRF Tokens:
   - Add Anti-CSRF token on all vulnerable components.
   - Be sure every request that modify important data requires a valid Anti-CSRF token.
   - Verify Anti-CSRF token on server side before process requests that modify data.
2. Vulnerable JavaScript Library components:
   - Update or change vulnerable JavaScript library with more version safe.
   - Apply practice good development in integrate and use JavaScript libraries, such as renew.
   References in a manner order and follow guide security provided by the developer library.
3. Component cookies without attribute HttpOnly, Secure Flag and SameSite :
   - Add attribute HttpOnly on the containing cookie information sensitive. Attribute this prevent JavaScript access to the cookie.
   - Activate the Secure Flag attribute on the cookie that was sent via HTTPS. This ensure that cookies only sent through secure connection.
   - Set attribute SameSite on cookies with appropriate value (for example, " Strict" or "Lax"). This help prevent CSRF and XSS attacks.

Besides that’s important for ensure that all implemented improvements tested in a manner thorough for ensure its effectiveness. Always update and do monitoring security in a manner regularly on the website for identify and fix vulnerability new possible appears. Repair Vulnerability this important for guard integrity, confidentiality, and availability of user data. With apply steps this is a risk attack like CSRF and XSS can be minus, as well protect user from potency losses caused by exploitation vulnerability the.

3.2.1.1. Comparison with another research within OWASP

Other studies have use framework OWASP's inner workings various analysis and complex cases. As example, there is discussing research mapping listed vulnerabilities in version latest OWASP Top Ten list to in blockchain technology. OWASP is A foundation non- profit providing information and sources power for help educate developer about problem security potential in code them. The OWASP Top Ten list is tool that is wide acknowledged for identify vulnerability in web application. Research results this is identification vulnerability potential in blockchain system with inspect integration external common, like exploration block web and device based soft wallet, for the same vulnerabilities that are described in the OWASP Top Ten List. Study this find that nine from ten OWASP vulnerabilities also apply for blockchain system, except XML External Entities (XXE) which are not apply Because less use of XML in blockchains. Mapping framework already work there, like OWASP, to in blockchain technology can help in identify vulnerability potential in blockchain system.

OWASP in various study has used into the diverse enough analysis and cases complex, other studies also show that [38] The research paper discusses the mapping of the vulnerabilities listed in the latest version of the OWASP Top Ten List to blockchain technology. OWASP is a non-profit foundation that provides information and resources to help educate developers about potential security issues in their code. The OWASP Top Ten List is a widely recognized tool for identifying vulnerabilities in web applications. The result of this research is the identification of potential vulnerabilities in blockchain systems by examining common external integrations, such as web-based block explorers and wallet software, for the same vulnerabilities outlined within the OWASP Top Ten List. The study found that nine out of ten of the OWASP vulnerabilities also apply to blockchain systems, with the exception of XML External Entities (XXE), which is not applicable due to the lack of use of XML in blockchain. This mapping of existing frameworks, such as OWASP, to the blockchain can help in the identification of potential vulnerabilities in blockchain systems.

3.2.1.2. Implications and explanations OWASP findings

The results of the analysis in Table 4 show a number of findings vulnerabilities on the AB Dinas website analyzed use OWASP tools. A number of findings the includes:

1. Lack of Anti-CSRF Tokens: Findings this show that There is components in websites that do not have Anti-CSRF tokens with category vulnerability "Medium". This possible CSRF attacks that can compromise integrity and confidentiality of user data.
2. Vulnerable JavaScript Library components: Findings this show that there is a number of component vulnerable JavaScript library with category the same risk, namely " Medium". Component this can used for do XSS attack.
3. Cookie component without attribute HttpOnly, Secure Flag, and SameSite: Some component No own attribute HttpOnly Flag, Secure Flag, and SameSite. Third Component this detected as risk low 16-19 times. Although the risk relatively low, still There is possibility exists lack possible attributes cause attack like attempted hijacking and cookie theft.

Besides it, Table 4 also detects a number of findings else, like vulnerability small on Leaking Server Details via X-Powered-By HTTP Response Header resulting in 16 components detected. This give information that There is the technology used on the server. Furthermore, there are 3 detected Disclosure of Unix Timestamps components, which are possible attacker for now information sensitive. There are also 23 detected components in header component which is not defined. Component this possible attacker For manipulate or falsify MIME type and delivers results based on XSS attack.

3.2.1.3. Strengths and limitations of AB 's website results findings

Strength from the AB Dinas website exists effort for do evaluation vulnerability use OWASP tools. this show awareness to security system. Findings the give outlook about potency existing vulnerabilities on the website and allows steps mitigation for applied. However, there is a number of necessary limitations noticed. The findings are presented in Table 4 only covers possible vulnerabilities detected use OWASP tools. There is a possibility that Still There is other vulnerabilities that do not detected by the tool the. Besides it, analysis this no give detailed information about context website usage and configuration system that can influence vulnerability. because it is necessary done evaluation comprehensive security with combine analysis automatic and manual as well involve expert security for identify and address vulnerability in a manner thorough.

3.2.2. Result of Tools Wapiti

Table 5 presents results from evaluation information AB website identification using Wapiti tools. Analysis this succeed covers four components, which consists from One Configuration Policy Security Content (Content Security Policy/CSP), four HTTP Secure Security Headers, one cookie with attribute HttpOnly Flag, and two cookies with the Secure Flag attribute.

Table 5. Analysis of Vulnerability Assessment of the AB Service Website using Wapiti Tools

Components	Wapiti Tools
	Results
Content Security Policy Configuration	1 detected
HTTP Secure Headers	4 detected
HttpOnly Flag cookie	1 detected
Secure Flag cookies	2 detected

Impact and consequence potential from every identified vulnerability is as following:

1. Content Security Policy Configuration (CSP): Vulnerability in configuration policy security content can possible attack such as cross-site scripting (XSS). CSP aims for limit source power that can loaded by the web page, so protect to injection code dangerous. If the CSP is not configured with right, XSS attacks can be utilize gap this for insert code dangerous to in web pages and access user data or damage integrity page.
2. HTTP Secure Headers: Vulnerabilities in HTTP Secure headers can be resulted decline security in a manner whole. Headers such as Strict-Transport-Security (HSTS), X-Frame-Options, X-XSS-Protection, and others, aim for protect web applications from various attack. If these headers No configured with Correct or No there, attack like Man-in-the-Middle attacks, clickjacking, or XSS can become more maybe.
3. HttpOnly Flag cookie: Lack attribute HttpOnly Flag on cookies can be possible attack like Cross-Site Scripting (XSS) or session hijacking attacks. Attribute HttpOnly instructs the browser to just send cookies to the server, so reduce risk XSS attacks that take advantage of cookies.
4. Secure Flag cookie: A vulnerability in a cookie that doesn't own the Secure Flag attribute can be possible attack to no connection secure (non-HTTPS). The Secure attribute instructs the browser to only send cookies through secure connection, such as HTTPS. If cookies are sent through no connection safe, attacker can steal those cookies and did no access legitimate to account user.

Following is guide about method repair identified vulnerabilities:

1. Configure Content Security Policy (CSP):
   - Define and apply appropriate Content Security Policy for control source power that can loaded by web page.
   - limit source Power allowed external order only load from trusted source.
   - Set policy for prevent cross-site scripting (XSS) attacks with block or remove potency cause of XSS, like use 'script- src ' directive for limit source external can load script.
2. HTTP Secure Headers:
   - Implement secure HTTP headers like HTTP Strict Transport Security (HSTS) for ensure communication through secure HTTPS connection.
   - Use the X-Frame-Options header for prevent clickjacking attacks with control How web page can load in frames or iframes.
   - Enable the X-XSS-Protection header for strengthen protection to cross-site scripting (XSS) attacks on multiple browsers.
3. Cookies with attribute HttpOnly Flag and Secure Flag:
   - Set attribute HttpOnly on the containing cookie information sensitive. This will prevent JavaScript access to those cookies and protect from XSS attack.
   - Activate the Secure Flag attribute on the cookie that was sent via HTTPS. This ensure that cookies only sent through secure connection.
   - Check and make sure all cookies are sensitive has be marked with Correct with attribute HttpOnly Flag and Secure Flag.

Besides that's important for do monitoring security in a manner regular, follow practice secure development, and updating device soft with version the latest that has been repair known vulnerabilities. With apply steps this, vulnerability on the website can minus, and security and integrity web application can improve.

3.2.2.1. Comparison with another research:

Research results this use Wapiti tool for do analysis vulnerabilities on the AB website. Other studies using method similar is [39]. Study the explain that Wapiti is a vulnerability scanner source web application open. This tool designed for scan web application and find vulnerability security such as SQL injection, cross-site scripting (XSS), file inclusion, and vulnerabilities execution command. Wapiti can used for test HTTP

GET and POST requests, and can also detect possible errors leads to vulnerability. This tool written in Python language and can run on the system Linux, Windows, and macOS operations.

3.2.2.2. Implications and explanations findings

The results of the existing analysis in Table 5 shows findings from evaluation use the Wapiti tool on the AB website. Successful components is known includes:

1. Configuration of Content Security Policy (CSP): Findings this show exists One component Content Security Policy configuration. Content Security Policy is used for control source power that can loaded by web page and help protect from cross-site scripting (XSS) attacks and attacks type other.
2. HTTP Secure Headers: Available four successful Secure Headers component identified. Secure Headers included settings on HTTP headers that contribute to security web application with control behavior and policies security such as HSTS (HTTP Strict Transport Security), X-Frame-Options, X-XSS-Protection, and others.
3. Cookies with attribute HttpOnly Flag and Secure Flag: Found One cookie component with attribute HttpOnly Flag and two cookie components with the Secure Flag attribute. Use attribute HttpOnly Flag on cookies can be protect cookies from XSS attacks and usage the Secure Flag attribute can be prevent man-in-the-middle attack and make sure that cookies only shipped through secure HTTPS connection.

3.2.2.3. Strengths and limitations of AB 's website results findings

Strength from the AB based website results findings is implementation a number of step positive security. Found it Content Security Policy configuration, HTTP Secure Headers settings, as well use attribute HttpOnly Flag and Secure Flag on cookies show effort for increase security and protect user from attack like XSS and man-in-the-middle attacks. However, it is necessary noticed that the findings presented in Table 5 maybe only covers part from possible vulnerabilities it's on AB's website. Use Wapiti tools only is one method for find vulnerability, and maybe Still There is other vulnerabilities that do not detected by the tool this. because that's important for carry out evaluation comprehensive security with combine method different and involving analysis expert security for identify and address vulnerability in a manner thorough.

3.2.3. Result of Nikto

Table 6 is a form of the analysis results in the vulnerability assessment analysis column of the AB Office website using Nikto tools. Table 6 explains that the detection of several website components that have been analyzed, such as Secure Flag Cookies and HttpOnly Flag Cookies, detected results that both do not create tokens and display -win perfectly, this can cause open security holes starting from hijacking and CSS attacks, as well as no results detected in the component The anti-clickjacking X-Frame-Options so that it is vulnerable to clickjacking attacks.

Table 6. Analysis of Vulnerability Assessment of the AB Service Website using Nikto Tools

Components	Tools Nikto
	Results & Solutions
Secure Flag Cookies	DinasAB token & Disp -win not created
Httponly Flag Cookies	DinasAB token not created
The anti-clickjacking X-Frame-Options	Undetected
SSL and HSTS Headers	Undetected
Transport Layer Security (TLS) with Certificate Transparency (CT) headers	Undetected
The X-Content-Type-Options header	Undetected (This may allow the user agent to present the content of the website in a manner that is not consistent with its MIME type.)
Script injection protection headers	Undetected (This header can provide a hint to the user agent on how to protect against certain forms of XSS attacks.)

The analysis results indicate that several security components on the website are not well-defined. The SSL and HSTS Header components are undetected, causing the website to not run HTTPS perfectly and leaving it vulnerable to MITM (Man in The Middle) attacks. Additionally, the Transport Layer Security (TLS) with Certificate Transparency (CT) header components are undetected, causing the website to not be able to validate the TLS certificates contained in the browser. The X-Content-Type-Options header component settings are also not well-defined, providing opportunities for attackers to conduct sniffing attacks. Furthermore, the analysis detected that the Script injection protection header component is not well-defined.

Table 6 represents results column analysis analysis evaluation AB Office website vulnerabilities use tool Nikto. Table 6 explains that there is a number of website components that have analyzed, such as Secure Flag

Cookies and HttpOnly Flag Cookies. Detection results show that both of them No creates a token and disp - win automatically perfect, which can be cause gap security start from hijacking and CSS attacks, as well No There is results detection of the X-Frame-Options Anti-clickjacking component so prone to clickjacking attack. Impact and consequence potential from every identified vulnerability is as following:

1. Secure Flag Cookies and HttpOnly Flag Cookies: Lack arrangement the Secure Flag and HttpOnly Flag attributes on cookies can possibly attack like Cross-Site Scripting (XSS) or session hijacking attacks. The Secure Flag attribute instructs the browser to only send cookies through secure connection (HTTPS), temporarily attribute The HttpOnly flag instructs the browser to only send cookies to the server, so reduce risk XSS attacks that take advantage of cookies.
2. Component: Lack arrangement X-Frame-Options Anti-clickjacking component can make websites vulnerable to clickjacking attack. Clickjacking attacks involve fraud user for clicking link or actual button hidden inside other elements on the web page. With no exists protection from component here, attacker can hide element dangerous and deceptive user for do action that is not wanted.
3. SSL and HSTS Headers: Lack detection on SSL component and HSTS Header shows that the website does operate HTTPS protocol by perfect and vulnerable to man-in-the-middle (MITM) attacks. Use of HTTPS and the correct settings for HSTS (HTTP Strict Transport Security) can protect communication between users and servers from MITM attack with ensure that connection always done through safe channel.
4. Transport Layer Security (TLS) with Certificate Transparency (CT) header: Lack detection on the Transport Layer Security (TLS) header component with Certificate Transparency (CT) shows that the website does can validate contained TLS certificates in browsers. this can increase risk attack certificate false or manipulation certificate by an unauthorized party authorized.
5. X-Content-Type-Options header: Settings that are not right on the X-Content-Type-Options header component gives opportunity for attacker for do sniffing attack. With No arrange with correct this header, attacker can try manipulate type content sent by the server and exploit gap possible security related with type content certain.
6. Script injection protection header: Undefined component protection to injection script can increase risk attack injection script like Cross-Site Scripting (XSS) attacks. When the server is not arrange with correct this header, the web page becomes more prone to to XSS attacks that can cause execution code dangerous on the side client.

In conclusion, results analysis show that there is a number of component security on the website that is not defined with ok. Vulnerability this can possibly attacks like XSS, hijacking, clickjacking, Man-in-the-Middle attacks, attacks certificate fake, manipulation type content, and injection script. because that's important for overcome Vulnerability this with configure and set component security with correct to use increase level website security. Following is guide about method repair identified vulnerabilities:

1. Secure Flag Cookies and HttpOnly Flag Cookies:
   1. Be sure all cookies (cookies) that contain information sensitive has been marked with the Secure Flag and HttpOnly Flag attributes.
   2. Set the Secure Flag attribute on the cookies that are sent through secure connection (HTTPS) to prevent hijacking attack.
   3. Activate attribute HttpOnly Flag on the containing cookie information sensitive for protect it from cross-site scripting (XSS) attacks.
2. X-Frame-Options anti-clickjacking components:
   1. Apply setting X-Frame-Options on the HTTP response header for control method web page can loaded in frames or iframes.
   2. Set value X-Frame-Options as "DENY" or "SAMEORIGIN" for prevent clickjacking attack.
3. SSL and HSTS Header Components:
   1. Make sure SSL (Secure Sockets Layer) is enabled configured with right and certificate has installed with appropriate validity.
   2. Enable and set the HTTP Strict Transport Security (HSTS) header for ensure website only walk through secure HTTPS connection.
4. Components of Transport Layer Security (TLS) with Certificate Transparency (CT) Header:
   1. Update arrangement for make sure the website can validate the TLS certificate that is in the browser.
   2. Activate supervision certificate with using Certificate Transparency (CT) for inspect validity certificate used.

5. Settings X-Content-Type-Options header component:
   Set setting X-Content-Type-Options header as " nosniff " for prevent attacker change type content that the browser interprets and protects from sniffing attack.
6. Script injection protection header components:
   1. Apply appropriate settings for protect websites from attack injection script.
   2. Use a header such as "Content-Security-Policy" or "X-XSS-Protection" for prevent attack injection script.

With apply steps this, identified vulnerabilities can repaired, and website security can be improved. Besides that's important for do monitoring security in a manner periodically, following practice safe development, and ensure update device soft with version the latest that has been repair known vulnerabilities.

3.2.3.1. Comparison with another research:

No There is comparison direct with other studies mentioned in findings the. However, research previously used tool Nikto, like research A or B, got give understanding more carry on about a similar vulnerability or method a similar analysis that has been done on another website.

3.2.3.2. Implications and explanations findings

Analysis results in Table 6 indicates a number of findings in evaluation vulnerabilities on the website AB uses tool Nikto. Components following succeed identified:

1. Secure Flag Cookies and HttpOnly Flag Cookies: Findings this show that cookies (cookies) with the Secure Flag and HttpOnly Flag attributes are not arranged with ok. Lack arrangement this can cause gap security like hijacking attacks and CSS attacks.
2. X-Frame-Options anti-clickjacking component: No There is results detected on the component this. Absence good X-Frame-Options settings on the website can make it prone to clickjacking attack.
3. Components and HSTS Header: No detected, shows that no SSL settings and HSTS headers implemented with ok. This causes the website doesn't walk with perfect use HTTPS and leave it prone to to Man-in-The-Middle (MITM) attack.
4. Transport Layer Security (TLS) component with Certificate Transparency (CT) Header: No detected, shows that the website does can validate contained TLS certificates in browsers. Lack this can cause vulnerability to attack forgery certificate.
5. Arrangement component X-Content-Type-Options header: No arranged with well, give opportunity for attacker for do sniffing attack.
6. Script injection protection header component: No arranged with well, show vulnerability to attack injection script.

3.2.3.3. Strengths and limitations of AB's website results findings

Power that can identified from the AB based website results findings is use of the Secure Flag and HttpOnly Flag on cookies (cookies), indicating effort for increase security and protect user data. However, there is a number of weaknesses in arrangement detected AB website security in analysis. This covers absence or settings that do not good on components such as X-Frame-Options, SSL, HSTS Header, Transport Layer Security (TLS) with Certificate Transparency (CT) Header, X-Content-Type-Options header, and Script injection protection header.

Drawbacks this can give gap for attacker for do attack such as clickjacking, Man-in-The-Middle (MITM), and injection script. because therefore, the AB website is necessary increase arrangement security for overcome vulnerability and protect user data in a manner more ok. It's also important for record that visible finding in Table 6 maybe only covers part from possible vulnerabilities exist on AB's website, and are required analysis more security comprehensive for identify and address vulnerability in a manner thorough.

3.3. Results of Analysis Vulnerability Assessment Website XY Service

Several explanations will be presented from the results of a vulnerability analysis conducted on the XY Agency website using testing tools such as Burp Suite, Skipfish and Rapidscan. The output of the analysis scan in this section will present information that corresponds to several components of available tools.

3.3.1. Result of Burp Suite

Table 7 describes the results of the Analysis Vulnerability Assessment Website of Dinas XY using Tools Burp Suite. The analysis has identified several components, including the presence of 5 TLS cookies without secure flag sets, indicating a potential security vulnerability. Another finding was the detection of a TLS certificate with a "medium" level, which suggested possible issues with the validity of the certificate usage.

Table 7. Analysis of the Vulnerability Assessment of the XY Service Website using the Burp Suite Tools

Components	Tools Burp Suite	
	Results	**Risk**
TLS cookies without secure flag set	5 detected	Medium
TLS certificates	1 detected	Medium
Vulnerable JavaScript dependencies	2 detected	Medium
Password field with autocomplete enabled	3 detected	Low
Strict transport security not enforced	1 detected	Low

The Vulnerable JavaScript dependency component had two results related to dependencies. The Password field with autocomplete enabled on the login form had three components. Additionally, one website was found not to apply the Strict Transport Security components, which can lead to decreased effectiveness when transmitting data over a network.

Research also supports this that the burp suite tools have produce results analysis form [40] The Burp Suite Pen Tester is a tool used for scanning activities. It provides necessary and essential tools needed for scanning activities. The free version of the tool is capable of automatically crawling web-based applications. The tool is designed to identify vulnerabilities in web applications and can be used to test the security of web applications. The results of the scan can be used to identify vulnerabilities that can be exploited by attackers. The proposed method was evaluated by exploiting the Metaesploitable Linux distro, and it was found to be able to automatically mitigate vulnerabilities afflicting six widespread services. The paper concludes by drawing future research lines.

Table 7 explains results from Analysis Evaluation XY Service Website Vulnerabilities using Burp Suite Tools. Analysis this has identified a number of components, incl presence of 5 TLS cookies without secure flag setting, which indicates exists vulnerability security potential. Findings other is detection One TLS certificate with level of "medium", which shows possibility problem with validity use certificate. Component Vulnerable JavaScript dependencies own two results related dependencies. Password field with autocomplete setting enabled on login form has three components. Besides it, one website found No apply component of Strict Transport Security, which can result reduced effectiveness moment transmit data through network. Impact and consequence potential from every identified vulnerability is as following:

1. TLS cookies without secure flag: Insufficient setting the secure flag on the TLS cookie can cause vulnerability in security session. The secure flag instructs the browser to only send cookies through secure connection (HTTPS). If a TLS cookie is sent through no connection safe, attacker can steal those cookies and get no access legitimate to account user.
2. TLS certificate with "medium" level: Detect TLS certificate with the "medium" level indicates exists problem potential related validity use certificate. Invalid TLS certificate or has expired can open gap for attacker for do man-in-the-middle (MITM) attack or attack other to no connection safe.
3. Vulnerable JavaScript dependencies: Detect vulnerable JavaScript dependencies show exists vulnerability in components used by web applications. Vulnerabilities in JavaScript dependencies can be exploited by attackers for do attack like attack injection script (XSS) or attack others who take advantage gap component safety the.
4. Autocomplete enabled on Password field: When autocomplete enabled on password field on login form, p This can increase risk leakage information user. If the use of autocomplete is saved by the browser or tool another, attacker can take advantage of it for get access to account user.
5. non-applicability Strict Transport Security component: Non-applicability the Strict Transport Security (STS) component means the website doesn't in a manner consistent use HTTPS protocol. This can increase risk MITM attacks and current data interceptions transmit data through network that doesn't safe.

Following is guide about method repair identified vulnerabilities:

1. TLS cookies without secure flag sets:
   - Be sure all marked TLS cookies with the secure flag.
   - Every containing cookie information sensitive must ship through secure HTTPS connection.
   - Update arrangement cookies that don't has the secure flag to match with standard security.
2. TLS certificate with a "medium" level:
   - Update TLS certificate that has level security "medium" to more level high.
   - Be sure the certificate used on the website is valid and reliable.
   - Review reset and update arrangement certificate for ensure optimal security.
3. Vulnerable JavaScript dependency components:

- Review vulnerable JavaScript dependencies and make sure for renew the version that has the security patch.
- Update or change vulnerable dependencies with more alternatives safe.
- Do monitoring security continously to JavaScript dependencies for identify and address possible vulnerabilities appears.

4. Password field with autocomplete enabled on the login form:
   - Deactivate autocomplete feature in the password column on the login form.
   - Use attribute `autocomplete="off"` on the password input element for prevents the browser from remembering and filling in automatic user password.
   - Give guide to user for No allow storage automatically passwords on their browsers.
5. Non-application of Strict Transport Security (HSTS) components:
   - Apply Strict Transport Security (HSTS) settings on the website for ensure that all connection done through secure HTTPS protocol.
   - Set HSTS header with appropriate value, such as ` Strict-Transport-Security: max-age=31536000; includeSubDomains; preload`.
   - Review server configuration and confirm that HSTS is enabled and working with right.

With follow guide this, identified vulnerabilities can repaired and website security can be improved. Important for always updating and monitoring new vulnerability appears, as well follow practice security best in website development and management.

3.3.1.1. Comparison with another research

No There is comparison direct with other studies mentioned in findings the. However, research previously used Burp Suite tools, such as research mentioned [41], got give understanding more carry on about a similar vulnerability or method a similar analysis that has been done on another website.

3.3.1.2. Implications and explanations findings

Analysis results in Table 7 shows a number of findings in evaluation vulnerability on the website Service XY uses Burp Suite tool. Components following succeed identified:

1. TLS cookies without secure flag sets: Findings this show that there are 5 TLS cookies that are not own secure flag setting, which indicates potency vulnerability security. The secure flag is used for ensure that cookies only shipped through secure HTTPS connection.
2. TLS certificate with a "medium" level: Findings this show exists One TLS certificate with level security "medium", which indicates possibility problem in use certificate. This Can show problem in validity certificate used on the website.
3. Vulnerable JavaScript dependency component: Available two results related with vulnerable JavaScript dependencies. This indicate exists dependencies that have vulnerability necessary security overcome.
4. Password field with autocomplete enabled on the login form: Yes, three related components with autocomplete settings in the password column in the login form. Arrangement this can increase risk security Because can possible theft login information.
5. Non-application of Strict Transport Security (HSTS) components: Found that one website does apply the Strict Transport Security component. Absence arrangement this can reduce effectiveness moment transmit data through network, increase risk attack to no connection safe.

3.3.1.3. Strengths and limitations of the XY website results findings

Power that can identified from the XY based website results findings is exists identification related vulnerabilities with TLS cookies, TLS certificates, vulnerable JavaScript dependencies, and autocomplete settings in the password field. This show effort for identify and fix problem existing security. However, the weaknesses detected on the XY website include settings that do not according to TLS cookies, invalidity TLS certificates, drawbacks in JavaScript dependencies, and vulnerable autocomplete settings. Besides that, is, absence Strict Transport Security (HSTS) settings are also a possible weakness increase risk attack. With Thus, the XY website is necessary fix and improve arrangement security, like enable secure flag on TLS cookie, validate TLS certificate used, address vulnerability in JavaScript dependencies, and set autocomplete automatically safe. Besides it is also important for apply Strict Transport Security (HSTS) component for increase security data transmission via network.

3.3.2. Skipfish Tools Results

Table 8 displays findings from the Vulnerability Assessment of Dinas XY' website using the skipfish tool. The analysis covered several components, including Resource fetch, which encountered failure while attempting to retrieve 25 resources. In the Numerical filename component, 22 filename numbers were identified, which need to be rechecked. The four results under the Server component were classified as error results. The Resource not directly accessible component yielded six findings of resources that cannot be accessed directly. One resource was identified under the New 404 signature component. The New 'Server' header value seen component had two results. Additionally, seven new HTTP cookie components were successfully added, and one component was detected in the SSL certificate issuer information component.

Table 8 displays results from Evaluation Service XY website vulnerability using tool skipfish. Analysis This covers a number of components, including Resource fetch, are subjected to failure moment try take 25 sources power. In the numerical filename component, 22 numbers are identified in necessary file name checked repeat. Four results below server components are classified as results error.

The resource not directly accessible component returns six findings source no power can accessed in a manner direct. One source power identified in New 404 signature components. The New 'Server' header value seen component generates two results. Besides it, seven new HTTP cookie component succeed added, and one component detected in component information publisher SSL certificate.

Table 8. Analysis of Vulnerability Assessment of the XY Service Website using Skipfish Tools

Components	**Skipfish tools**
	Results
Resource fetch failed	25 detected
Numerical filename – consider enumerating	22 detected
Incorrect or missing charset	35 detected
Incorrect or missing MIME type	5 detected
Password entry form – consider brute-force	2 detected
Hidden files / directories	21 detected
Generation of server errors	4 detected
Restricted resources	6 detected
Original 404 identifiers	1 detected
Recently identified 'Server' header value	2 detected
Added HTTP cookie detected	7 detected
SSL certificate authority information	1 detected

Impact and consequence potential from every identified vulnerability is as following:

1. Resource fetch failure: Failure in take source Power can resulted access limited or No availability content required by users. This can bother experience users and raises inconvenience.
2. Numerical filename: Presence number in filename can raises vulnerability If file processing is not taken into account with Correct case use number or appropriate file memory. This can be exploited by attackers for manipulate access to the file it should be No can accessed or resulted system error.
3. Server error results: The error results on the server component show exists problem in server operation. This can bother website functionality and availability as well disclose information sensitive about server infrastructure to attacker.
4. Resource not directly accessible: Resource no power can accessed in a manner direct can hinder access user to expected content. this can bother functionality and experience user.
5. New 404 signature: Findings this indicate that there is source no power found (404) with sign hand new. this can indicate that There is change or addition in possible website content affect existing links and navigation.
6. New 'Server' header value seen: Detect new 'Server' header value show exists change in server configuration. this can disclose information about technology used and enabled attacker for do study more carry on to related vulnerabilities with technology the.
7. HTTP cookie components: Added new HTTP cookie component can cause vulnerability to attack such as cookie hijacking or session hijacking. This can result access No legitimate to account user or leakage information sensitive.
8. SSL certificate issuer information: Findings in Component this show that There is problem or discrepancy with publisher SSL certificate. This can raise vulnerability to Man-in-the-Middle (MITM) attacks and reduce security communication protected by SSL.

In all case here are the steps repair must take for repair vulnerabilities identified and confirmed more security and functionality Good from that website. Following is guide about method repair identified vulnerabilities:

1. Resource fetch:
   - Review return source failed power take and check the cause.
   - Check network and server connection to ensure Stable accessibility.
   - Be sure that source power required available and available accessed with right.
2. Numerical filename:
   - Review repeat use numeric filename and check is There is weakness or related problems.
   - Consider for implement policy use more file names descriptive and easy understood.
3. Servers:
   - Check server configuration for identify and fix the problem it causes results server component error.
   - Make sure the server is running with secure configuration and not prone to attack that can exploited.
4. Resources are not directly accessible:
   - Review return arrangement right access to sources no power can accessed in a manner direct.
   - Be sure right proper access given to the source power required.
5. New 404 signature:
   - Check URL structure and server settings for identify and fix the problem it causes response 404.
   - Be sure proper diversion for source no power found.
6. New 'Server' header value seen:
   - Check change in header settings 'Server' and make sure that change it is valid and safe.
   - Review server configuration whole and sure server security and stability is maintained.
7. New HTTP cookie components:
   - Review addition or change in new HTTP cookie setting.
   - Be sure appropriate cookie settings with policy necessary security and privacy.
8. SSL certificate issuer information:
   - Review information publisher SSL certificate and make sure the certificate used is valid and issued by a trusted authority.
   - Update SSL certificate if needed and confirmed authenticity and integrity awake.

With follow guide this, identified vulnerabilities can repaired and website security can be improved. Important for do monitoring security in a manner regular and updating arrangement as well as configuration in accordance with practice security best.

3.3.2.1. Comparison with another research

No There is comparison direct with other studies mentioned in findings the. However, tools skipfish used in analysis own wide usage in study web security. Study previously used skipfish or tool similar can give outlook more carry on about a similar vulnerability or method a similar analysis that has been done on another website.

3.3.2.2. Implications and explanations findings

Analysis results in Table 8 shows a number of findings in evaluation vulnerability on the website Service XY uses tool skipfish. Components following succeed identified:

1. Resource fetch: Findings this show that there are 25 sources failed power taken moment effort recovery. This can indicate problem in access or load source resources required by the website.
2. Numerical filename: There are 22 identified numeric filenames. Findings this show necessity do inspection repeat to use possible numeric file names indicate problem or weakness in the system.
3. Servers: Yes, four classified results as results error in the Server component. This indicate exists problem in configuration or response from a possible server can exploited by attackers.
4. Resource not directly accessible: Findings this show There is six source no power can accessed in a manner direct. This can indicate exists problem in accessibility or configuration arrangement right access to sources power.
5. New 404 signature: One source Power identified in component this. Findings this indicate that There is One source generating power response 404, which means No found. This can show problem in URL structure or server settings.
6. New 'Server' header value seen: Two results identified on the component this. Findings this show that There is different header settings 'Server' from the previous one seen. Change This can indicate change in configuration or possible server versions need checked more continue.
7. New HTTP cookie components: Seven new HTTP cookie component succeed added. Findings this can indicate exists addition or change in cookie settings on the website.

8. SSL certificate issuer information: One component detected in component this. This show information publisher SSL certificate used on the website. Information this important for verify authenticity certificate.

3.3.2.3. The strengths and limitations of the XY website from results findings

Power that can identified from the XY based website results findings is exists identification related vulnerabilities with taking source power, usage numeric filename, server configuration, accessibility source power, 'Server' header settings, HTTP cookie settings, and information publisher SSL certificate. With know vulnerability this, action repairs and improvements security can take for overcome identified problem. However, Findings this also indicates exists limitations in XY website security. Detected vulnerabilities in taking source power, server configuration, accessibility source power, and setting HTTP cookies can exploited by attackers for access information sensitive, destructive website integrity, or do XSS (Cross-Site Scripting) and CSRF (Cross-Site Request Forgery) attacks. Limitations this show necessity do action repair and strengthening the necessary security for protect the XY website from potency attacks and violations more security seriously.

3.3.3. Result Tools Rapidscan

There are several scanning tools in the Rapidscan tool, the results found based on Table 9 are detected 2 tools that are able to provide multiscanner scan results namely Subdomain Fierce Bruter, SSLyze, NMAP and Wafw00f. These results show that there are several components, each of which has a risk of a level of security holes, namely the risk of medium level in subdomains and Secure Client Initiated Renegotiation, and WAF. Although the results of the WAF component are classified as medium level, if not repaired properly, there will be sources of vulnerability such as the FREAK vulnerability component with a high level. In study this, is used a number of tool scanner in Rapidscan tool, and the results found based on Table 9 that There are 2 tools that can give results scan multiscanner, namely Subdomain Fierce Bruter, SSLyze, NMAP, and Wafw00f. This result show exists a number of components, each has risk level different vulnerabilities. Risk level vulnerability medium located on subdomains, Secure Client Initiated Renegotiation, and WAF. Although results WAF components are classified as risk level medium, if no repaired with fine, got become source vulnerability, like component FREAK vulnerability with risk level high. Impact and consequence potential from every Vulnerability this can vary greatly. Vulnerabilities on subdomains can be possible attack transfer identity or no access legitimate to system. Vulnerable Secure Client Initiated Renegotiation can cause renegotiation attacks and resulting no communication safe between client and server. Vulnerabilities in WAF components can be possible bypass attack against WAF protection and express gap security on protected web applications.

Table 9. Analysis of the Vulnerability Assessment of the XY Service Website using the Rapidscan tool

Components	**Rapidscan tools**	
	Multiscanner Tools	**Risk**
Subdomains with Fierce	Bruter subdomain	Medium
Secure Client Initiated Renegotiation is supported	SSLlyze	Medium
FREAK Vulnerability Detected	NMAP	high
No Web Application Firewall	Wafw00f	Medium

In case FREAK vulnerability, which has risk level high impact can be very serious. Vulnerability this can possibly attack to SSL/TLS encryption used for protect web communications, so possible attack sensitive data being transmitted through network. For avoid adverse impacts and consequences, important for quick identify and fix existing vulnerabilities. Corrective action can covers renew version device software, configure repeat system, or implement steps protection addition like a firewall or filter then cross. With do proper action, organization can reduce risk attack and protect data and systems they from existing threats. guide general about method repairs a number of identified vulnerabilities:

1. Vulnerability Subdomains:
   - Check and validate existing subdomains.
   - Be sure only valid subdomains are allowed for operate.
   - Protect sensitive subdomains with steps security extra, like authentication two factor.
2. Secure Client Initiated Renegotiation Vulnerability:
   - Update your server with version the latest that has been repair vulnerability this.

   - Set repeat your SSL/TLS configuration for disable renegotiation or follow guide security provided by your vendor.
3. Web Application Firewall (WAF) Vulnerabilities:
   - Update and configure your WAF with the most recent rules.
   - Ensure WAF recognizes and protects to attack latest.
   - Review and fix WAF configuration for minimize possibility bypass attack.
4. FREAK vulnerabilities:
   - Update OpenSSL version or device soft encryption others affected impact vulnerability this.
   - Set reset and configuration reset your SSL/TLS for repair FREAK vulnerability.
   - Be sure vulnerable protocol disabled and only use more version safe.
5. Besides it is recommended for:
6. Routine check and update device software, system operations, and applications to version latest to have repair security.
   - Use strong web security, such as enabling HTTPS, using valid SSL certificate, and implement control adequate access.
   - Own policy Strong and encouraging password management user for using unique and complex passwords.
   - Perform security audits routines and scans vulnerability for detect and address vulnerability new possible appears.

3.3.3.1. Comparison with another research

No There is comparison direct with other studies mentioned in findings the. However, Findings this show use a number of tool scan in Rapidscan tool for get results scan multiscanner. Scanning multiscanner has used in Lots study web security before for get more picture comprehensive about vulnerabilities and weaknesses in something system. Other studies using the same tools or similar can give outlook more carry on about similar findings or method a similar analysis that has been done on another website.

3.3.3.2. Implications and explanations findings

Analysis results in Table 9 shows findings from scan use a number of tools in Rapidscan tool. A number of identified findings includes:

1. Bruter subdomains: Findings this indicate exists risk vulnerability level medium in subdomains. Subdomains are not protected with Good can give chance for attacker for do targeted attack.
2. SSLyze: Findings this indicate exists risk vulnerability level medium in Secure Client Initiated Renegotiation. Problems at initiation negotiation repeat can influence security and integrity communication through SSL/TLS protocol.
3. NMAPs: No There is explanation related findings with NMAP inside given text.
4. Wafw00f: Findings this show exists risk weakness in WAF (Web Application Firewall) component. Although Findings this classified as level risk medium, if no repaired with fine, got become source more vulnerability seriously, like categorized FREAK vulnerabilities as level risk high.

Implications from Findings this is exists potency vulnerability in a subdomain, initialize negotiation repeat no safe, and settings weakness in WAF component. For guard XY website security, action repairs and improvements security need taken for overcome Findings this. this important for vulnerability the No can exploited by attackers and for guard integrity, confidentiality, and availability system.

3.3.3.3. Strengths and limitations of the XY website results findings

Based on Findings this, a few power that can identified from the XY website is exists use tool scan multiscanner that can identify vulnerability in a subdomain, initialize negotiation reset SSL/TLS, and WAF settings. With know vulnerability here are the steps repairs and improvements proper security can taken. However, Findings this is also revealing a number of limitations on the security of the XY website. There is risk vulnerability level detected medium in a subdomain, initialize negotiation reset SSL/TLS, and WAF components. otherwise, quick fixed, vulnerabilities this can give opportunity for attacker for take profit and cause more losses seriously. because it is necessary taken action for strengthen XY website security with repair identified vulnerabilities.

3.4. Results of Testing Websites using Brute Force Attack

A presentation of the results of the process of attempted brute force attacks on both websites, but not all results that appear in this experiment will succeed perfectly. Because some results cannot be explained completely in this method, due to the relationship between the rules of the code of ethics between the author and also the agency that is used as the target of the research object in this case study.

SQL injection experiments were carried out to facilitate brute force experiments carried out on the XY Service website, which included the following results and explanations:

```
id= txtEmail - Request.POST [' xyzname ']

id = txtPassword - Request. POST [' passwordxyz ']

Query = SELECT id FROM users WHERE txtEmail - ' userxyz ' AND txtPassword - '
passwordxyz '
```

The collection of queries above is an injection code attempted by the author in trying to access into the system, where the code is used to retrieve input values on the "email" and also the "password" filled in the login page. The code is entered into a website database to be checked on existing query combinations.

```
id= txtEmail - Request.POST [' xyzname ']
```

The 'id' variable contained in the query 'id= txtEmail ' will hold a user input value in the email form. Query on ' Request.POST [' namaxyz ']' which indicates that ' Request.POST ' function to retrieve the copy from the form with the 'POST' method on the login page. Then on [' namaxyz '] Used as an input attribute on the email login page.

```
id = txtPassword - Request. POST [' passwordxyz ']
```

The variable 'id' contained in the query 'id= txtPassword ' will hold a user input value in the password form. ' Request. POST [' passwordxyz ']' which indicates that there is an attribute value with password input in the login form.

```
Query = SELECT id FROM users WHERE txtEmail - ' userxyz ' AND txtPassword - ' passwordxyz
'
```

Variable 'Query' will receive a code from the SQL query to check if there is a match between the email and the password that was previously input. 'SELECT id' will select a value from ID user from the Users table. 'FROM users' is a query used to search the user table. Then there is the query 'WHERE txtEmail – ' userxyz ' AND txtPassword – ' passwordxyz ' which describes the query process in checking the match of email and password data based on the user database of the form.

The investigators were unable to retrieve any outcome of the Brute Force attack carried out on the XY website, indicating that the attack did not breach the targeted website system. This suggests that the XY website is structured with a robust security system that effectively deters attackers from gaining unauthorized access and perpetrating malicious activities that can potentially compromise the security of the website.

3.4.1. Comparison with another research

Other similar research is [42] The practical implication of this paper is that it proposes a new hash-based RFID mutual authentication protocol to address the privacy and forgery problems associated with RFID systems. This protocol enables the constant creation of distinct response messages without interference from intended or meaningless requests generated by an adversary, while the secret value is not directly transmitted. The proposed protocol makes it difficult for an attacker to launch successful brute-force attacks against the approach. This protocol can be implemented in RFID systems to enhance their security and prevent unauthorized access to tag information.

3.4.1.1. Implications and explanations findings

Findings this describes the query process in SQL usage for inspect compatibility between the email and password entered previously in XY website system. Use of this query is part of the authentication process common user in system web authentication. In Findings this, no There is successful result obtained from Brute Force attack performed on the XY website. this indicate that system XY website security has Sturdy and effective structure in prevent attacker for get no access legal and do activity evil can endanger the website's security. Implications from Findings this is that system XY website security is proven effective in protect user data and prevent Brute Force attack. This show exists serious endeavor in apply security on the XY website, which can give trust to user that their data safe and protected.

3.4.1.2. Strengths and limitations of the XY website results findings

Based on Findings this, the strength of the XY website is system robust and effective security in prevent Brute Force attack. This show that serious endeavour has done for protect user data and prevent no access legitimate to system. However, findings it also has limitations in give information more carry on about the strengths and limitations of the XY website whole. Findings only related with Brute Force attacks and not give description thorough about vulnerability security other possible There is on the XY website. because it, for evaluate the strengths and limitations of the XY website thorough, necessary done evaluation more security comprehensive.

4. CONCLUSION

Based on conclusion from analysis AB and XY Services website vulnerabilities as well results verification identity, got concluded that both websites own a number of necessary weaknesses and vulnerabilities repaired for guard safety and quality both websites. Need done improvements to website configuration such as cookie settings, SSL, HTTP headers, and more. Besides that, it is also necessary for repair such other vulnerabilities a vulnerable JavaScript dependency, no exists Anti-CSRF. Based on results analysis vulnerability and verification identity from the AB and XY Services websites, found vulnerability necessary specifics repaired to use guard safety and quality the two websites, such as AB Dinas Website:

- Lack of Anti-CSRF Tokens Vulnerability: Shortage use of Anti-CSRF tokens can possible threatening CSRF attacks integrity and confidentiality of user data.
- Vulnerable JavaScript Library Components: Vulnerable JavaScript components to XSS attacks can exploited by attackers.
- Cookie Components without HttpOnly and SameSite Attributes Vulnerabilities: Multiple the cookie component doesn't own arrangement HttpOnly and SameSite, improve risk cookie theft and hijacking attacks.

XY Services Website:

- Vulnerability Leaking Server Details via X-Powered-By HTTP Response Header: Server information leaked via X-Powered-By HTTP response header could give instruction technology used and become source information for attacker.
- Vulnerability: Setting a password field with autocompletion feature can possibly attack theft credentials user.
- Absence of Strict Transport Security (HSTS) Vulnerability Header: Absence Strict Transport Security (HSTS) settings can be reducing effectiveness sending data through network and upgrade risk MITM attack.
- Vulnerability SSL Certificate Issuer Information: Information publisher an SSL certificate that doesn't detected can raises inability for validate TLS certificate in the browser.

In framework increase security these two websites, are very important for quick overcome vulnerabilities the. Ignore necessary repairs can resulted risk serious and adverse consequences, such as access No legitimate to information sensitive, data breach, website contamination, and loss reputation. However, it's important for overcome Vulnerability this with immediately and effectively. Failure for do it can result serious risks and consequences for websites and their users. Vulnerability this can exploited by actors wicked for endanger integrity, confidentiality, and availability of user data, as well as launch attack such as cross-site scripting (XSS), SQL injection, and brute force attacks. Potency risks and consequences from Vulnerability this including access no legitimate to information sensitive, data breach, website tampering, and crash reputation. Besides that, information personal and financial user Possible risk, cause loss finance, theft identity, and offence privacy. Besides that, the website can experience downtime or disturbance service, which resulted loss finances and losses trust user.

Because that's very important for take action quick for overcome identified weaknesses and vulnerabilities. This including applies practice secure coding, patching and updating device software and components in a manner regularly, and use a web application firewall. It's also important for configure cookies with safe, sure proper SSL implementation, and manage JavaScript dependencies effective. With thus, the web site can reduce potency risk, increase posture security, and guarding confidentiality and integrity of user data. As conclusion, prioritize settlement Vulnerability this is very important for protect website, guard trust user, and prevent potency loss financial and reputation. Recommended for allocate source power, involve professional security If necessary, and establish maintenance processes strong security for keep going monitor and manage emerging threats and vulnerabilities. Based on results analysis vulnerability and verification identity from the AB and XY Services website, find vulnerability necessary specifics repaired to use guard safety and quality both websites. Important for determine impact potential from Vulnerability this to website security and quality as well explain How weakness this can exploited by the attacker and the consequences potential for users and organizations. Following is impact potential from vulnerability mentioned on AB Dinas Website:

- Lack of Anti-CSRF Tokens Vulnerability: Vulnerability this can possible Cross-Site Request Forgery (CSRF) attack, in which the attacker can manipulate actions performed by users who have authenticated. Impact the potential is compromise to data integrity of its and potential users for do action No legitimate on Name user.
- Vulnerability: Cross-Site Scripting (XSS) attacks can be exploited through vulnerable JavaScript components. Attacker can insert code dangerous to in the website and access user data or manipulate site content. Impact including theft credentials, replacement content, or attack other to website users.
- Cookie Components without HttpOnly and SameSite Attributes Vulnerability: Flaw this increase risk cookie theft and hijacking attacks. Attacker can steal session cookies user and access account user without authorization. Impact is accessing No legitimate to information private, offence privacy, and misuse account.

XY Services Website:

- Vulnerability Leaking Server Details via X-Powered-By HTTP Response Header: Information about the technology used in the server can be help attacker in designing more attacks specific. Impact including enhancement risk attack to infrastructure and applications, as well violation possible security resulted data theft or leakage information sensitive.
- Password Field with Autocomplete Enabled Vulnerability: Flaw this possible attacker for steal credentials user with use autocompletion feature on the password field. Impact is accessing No legitimate to account user, theft identity and potential for do action harm on Name user.
- Absence of Strict Transport Security (HSTS) Vulnerability Header: None proper HSTS settings, vulnerable website to Man-in-The-Middle (MITM) attack, in which the attacker can intercept communications and steal user data. Impact covers theft information sensitive, data manipulation, or another harmful attack.
- SSL Certificate Issuer Information Vulnerability: Attacker can utilize information publisher an SSL certificate that doesn't detected for do phishing attacks or forgery identity. Impact including fraud user, lose trust of the website, and its potential sensitive data theft.

In framework increase security these two websites, are very important for quick overcome vulnerabilities the. Ignore necessary repairs can resulted risk serious and adverse consequences, such as access no legitimate to information sensitive, data breach, website contamination, and loss reputation. because it is recommended for implement practice secure coding, commit update routine and patching, as well using a web application firewall. Besides it, secure cookie configuration, proper SSL implementation, and management effective JavaScript dependencies are also a must noticed. In framework guard continuous security, is recommended for allocate source power, involve professional security If needed, and establish maintenance processes tough security to use Keep going monitor and manage threats and vulnerabilities new one that appeared. With take action soon, these two websites can reduce risk, increase level security and guarding secrecy as well as user data integrity. In part test brute force attack on XY website, several actions No succeed when try access website login page. This show that attacker will difficulty in do outside action authority. Based on results findings from the data presented, follows is analysis conclusion study with approach quantitative as following:

1. Vulnerability Assessment with OWASP Tools:
   - Component "Lack of Anti-CSRF Tokens" detected with level vulnerability "Medium" as many as 3 components. This possible CSRF attacks that can endanger integrity and confidentiality of user data.
   - There are 5 "Vulnerable JavaScript Library" components detected at tier equal /medium risk. Component this prone to to XSS attack.
   - There is a number of components that don't own the " HttpOnly Flag", "Secure Flag", and " SameSite " attributes. There are 16-19 components with risk low. Although the risk relatively low, still There is possibility exists lack in attribute this can trigger attack like test hacking and cookie theft.
   - There is a number of vulnerability small such as "Disclosure of Unix Timestamps", "Leaking Server Details via X-Powered-By HTTP Response Header", and "X-Content-Type-Options header not defined". Although vulnerability relatively small, still need noticed and repaired.
2. Wapiti Tool:
   - In results analysis with Wapiti, there is CSP components, HTTP Secure Headers, HttpOnly Flag cookies, and Secure Flag cookies have been checked.

- Information more carry on about results analysis this No given, so analysis conclusion quantitative No can do.

3. Nikto Tools:
    - There is a number of identified vulnerabilities, such as Secure Flag Cookies and HttpOnly Flag Cookies that are not arranged with perfect. This can cause gap security open like hijacking and CSS attacks.
    - A number of component other such as SSL and HSTS Headers, Transport Layer Security (TLS) with Certificate Transparency (CT) headers, and X-Content-Type-Options headers are not arranged with well, give opportunity for attacker for do attack such as sniffing and manipulation of MIME Types.
4. Burp Suite Tools:
    - Analysis results with Burp Suite express a number of components that don't defined with ok. For example, the SSL component and HSTS Headers are not detected, so the website is not walk with perfect use HTTPS protocol and vulnerable to MITM attack.
    - Neither does the X-Content-Type-Options header component arranged with well, give opportunity for attacker for do sniffing attack.
    - Information more carry on about results analysis this No given, so analysis conclusion quantitative no can do.
5. Skipfish Tool:
    - Analysis results with Skipfish show a number of necessary components checked reset, such as a Failed Resource fetch take 25 sources power.
    - There are also several component others who produce results error or no can accessed in a manner direct.
    - Information more carry on about results analysis this No given, so analysis conclusion quantitative no can do.

Kindly overall, important for remembered that Website security is an ongoing process. Handle identified weaknesses and vulnerabilities is step an important start, however monitoring sustainability and action security must be proactive too done. In the digital age that continues growing, threat security also continues change and develop. because that is, assessment routine to website vulnerability, deployment practice security best, and updates device regular software be very important. Continuous monitoring help detect attack new, prevent vulnerabilities that have not known and confirmed that action proper security taken immediately. Besides it, adopt approach proactive to security, like involve team trained security and use tool monitoring security, can help prevent attack before they raise significant damage. Based on matter the necessity for apply standard industry on the second website repair service such, then following recommendations for website management advice with standard industry as following:

1. OWASP (Open Web Application Security Project). (2020). OWASP Top Ten Projects. Retrieved from https://owasp.org/www-project-top-ten/
2. NIST (National Institute of Standards and Technology). (2017). NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
3. ISO/IEC (International Organization for Standardization/International Electrotechnical Commission). (2017). ISO/IEC 27001:2017 Information technology - Security techniques - Information security management systems - Requirements. Retrieved from https://www.iso.org/standard/54534.html
4. SANS Institute. (2021). SANS Critical Security Controls. Retrieved from https://www.sans.org/critical-security-controls/
5. CERT (Computer Emergency Response Team) Division of the Software Engineering Institute, Carnegie Mellon University. (2021). Common Weakness Enumeration (CWE). Retrieved from https://cwe.mitre.org/index.html
6. IETF (Internet Engineering Task Force). (2014). RFC 6797: HTTP Strict Transport Security (HSTS). Retrieved from https://tools.ietf.org/html/rfc6797

With follow approach this, organization can look after secure online environment and protect sensitive data user. Do evaluation security in a manner regular, apply action necessary security, and update system in a manner periodically is crucial steps in guard website security. In a world that continues change and more connect, invest in cyber security to be the more important. With high awareness to continual risk and security, organization can ensure that their website still safe, guard trust user, and protect information important from potential attack harm. Based on above, following is limitations Study from study this:

1. Scope Research: Research that has done Possible only focus on one aspect or tool testing certain. Limitations this can influence whole understanding about XY website security. more research broad and deep can give more insight comprehensive.

2. Limited Data: Research Possible only based on one limited data sources or datasets. More data usage broad and representative can increase validity and reliability findings.
3. No take into account Other Aspects: Research conducted Possible No take into account other possible aspects affect XY website security, eg policy security organization, infrastructure network, or factors social can influence action user.

In in conclusion, findings from analysis whole show exists vulnerability security in the analyzed website. Component such as Lack of Anti-CSRF Tokens, Vulnerable JavaScript Library, and inequality cookie attributes (HttpOnly Flag, Secure Flag, and SameSite) are required noticed and repaired. Besides that, some vulnerability small such as Disclosure of Unix Timestamps and Leaking Server Details were also found. Important for website owner for repair Vulnerability this for increase security and protect user data. Based on results research that has delivered following is some suggestions for study in the future that can done related with findings these:

1. Analysis Weakness Others: Do analysis weakness more security comprehensive on the XY website. Besides Brute Force attacks, it is also necessary to consider other attacks such as SQL injection, cross-site scripting (XSS), and attacks other common happens in web applications.
2. Study Comparison: Do study comparison with similar websites for evaluate strengths and weaknesses XY website security. This can give more understanding Good about how XY websites perform compared to with its competitors in matter security.
3. Penetration Test: Perform a penetration test in a manner thorough for identify potency vulnerability security yet detected on the XY website. Penetration test can involve series technique attack and test more security carry on for test as far as the XY website can be endure to various attacks.
4. Evaluation System Security: Evaluate system security used by the XY website, incl mechanism authentication, use of SQL queries, and layers security other. Objective from evaluation this is for identify gap possible security there and recommend necessary repairs.
5. Monitoring Security: Do monitoring security in a manner periodically on the XY website for detect attack or activity suspicious. This can help in detect and respond in a manner fast to threat new security or moderate growing.
6. Training Security: Do training security to XY website developer and administrator for increase awareness they about practice security best. This can help in reduce risk attack security caused by errors configuration or lack knowledge security.

With do studies it is expected can give more understanding comprehensive about strengths and weaknesses XY website security as well give guide for increase security in a manner whole. Based on matter we also describe it about Prospects Future Research as following:

1. Study About Security Application Mobile: Do study about security application cellular related with the XY website. Development mobile technology has resulted enhancement use application mobile, and security application cellular become crucial thing.
2. Study about IoT (Internet of Things) Security: Doing study about XY website security in Internet of Things (IoT) context, because the more many devices connected that can interact with the website.
3. Study About Intelligence Build and Security: Researching use intelligence artificial intelligence and technology related in increase XY website security, eg system detection clever intrusion or introduction pattern automatic attack.
4. Study About Privacy and Compliance Regulation: Do study about XY website compliance with regulation applicable privacy policies, such as the General Data Protection Regulation (GDPR) in the European Union. This involve understanding about personal data protection and implementation mechanism appropriate privacy.
5. Study About Detection Techniques Attack New: Develop techniques and methods new for detect attack security yet identified in a manner effective. This can involve approach-based intelligence artificial or more data analysis continues.
6. Study About Recovery After Attack: Explore method recovery and response emergency after happen attack security. This involves development of effective recovery strategies and plans possible emergency reduce impact attack and recover website operations with fast.

Prospects future research this will help in increase understanding about XY website security and involve aspects latest in security system information. Research conclusion this also indicates that although has identified a number of vulnerability related website configuration, brute force attacks, and Anti-CSRF flaws, likely Still There is other vulnerabilities that do not tested or identified. This important for noted Because vulnerabilities that have not detected can become threat potential for website security. because it is necessary done steps extra, like more research deep or more testing comprehensive, for identify and address vulnerability potential other possible there. With so, attempt website security a must sustainable and continuous improved for protect data and reduce risk attack that can endanger the security of the website. There is a number of example other possible vulnerabilities No tested or identified in study this, however need noticed that examples This characteristic common and can varies depending on environment and context specific website being evaluated. A number of example vulnerability possible potential not yet detected or tested in study this includes:

1. Cross-Site Scripting (XSS): An enabling XSS vulnerability attacker insert code script dangerous to in web page to be executed by the viewing user page the. This can used for steal information sensitive user or launch attack other.
2. SQL Injection: A SQL injection vulnerability occurred when user input No verified with true and possible attacker for insert malicious SQL commands. This can possible attacker for manipulate database or get access no legitimate to system.
3. Server Misconfiguration: Incorrect server configuration or not enough appropriate can cause vulnerability significant security. For example, including arrangement file permissions are not right, use version device vulnerable software, or firewall settings are not adequate.
4. Insecure Direct Object References: Vulnerabilities this happen when web application permit access direct to object (for example, file or database) without adequate verification. This can possible attacker for access or modifying data that is not should.
5. Server-Side Request Forgery (SSRF): An enabling SSRF vulnerability attacker for force the server to make request to source another power inside or outside network that doesn't should accessed. This can used for access internal system, exploit vulnerability else, or do phishing attacks.

Important for realize that this list only covers a number of example general, and every website can own vulnerability unique need more evaluation deep. For identify more vulnerability wide, recommended for use framework work evaluation comprehensive security and follow practice best determined by the organization security, such as OWASP (Open Web Application Security Project).

Acknowledgments

The writers express their gratitude to the University of Muhammadiyah Malang for providing them with the opportunity to conduct this research, which has resulted in its successful completion.

REFERENCES

[1] A. Jamil, K. Asif, R. Ashraf, S. Mehmood, and G. Mustafa, “A comprehensive study of cyber-attacks & counter measures for web systems,” in *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*, pp. 1–7, 2018, https://doi.org/10.1145/3231053.3231116.

[2] A. A. Ali and M. Zamri Murah, “Security Assessment of Libyan Government Websites,” *Proceedings of the 2018 Cyber Resilience Conference, CRC 2018*, pp. 1–4, 2019, https://doi.org/10.1109/CR.2018.8626862.

[3] A. F. Maskur and Y. Dwi Wardhana Asnar, “Static Code Analysis Tools with the Taint Analysis Method for Detecting Web Application Vulnerability,” *Proceedings of 2019 International Conference on Data and Software Engineering, ICoDSE 2019*, pp. 1-6, 2019, https://doi.org/10.1109/ICoDSE48700.2019.9092614.

[4] G. Dong, F. Liu, and G. Wu, “A Website’s Network Attack Analysis and Security Countermeasures,” *Procedia Comput Sci*, vol. 208, pp. 577–582, 2022, https://doi.org/10.1016/j.procs.2022.10.080.

[5] D. Arnaldy and A. R. Perdana, “Implementation and Analysis of Penetration Techniques Using the Man-In-The-Middle Attack,” *Proceedings - 2019 2nd International Conference of Computer and Informatics Engineering: Artificial Intelligence Roles in Industrial Revolution 4.0, IC2IE 2019*, pp. 188–192, 2019, https://doi.org/10.1109/IC2IE47452.2019.8940872.

[6] A. Goutam and V. Tiwari, “Vulnerability Assessment and Penetration Testing to Enhance the Security of Web Application,” *2019 4th International Conference on Information Systems and Computer Networks, ISCON 2019*, pp. 601–605, 2019, https://doi.org/10.1109/ISCON47742.2019.9036175.

[7] R. S. Devi, “Testing for Security Weakness of Web Applications using Ethical Hacking,” *Proceedings of the 4th International Conference on Trends in Electronics and Informatics, ICOEI 2020*, pp. 354–361, 2020, https://doi.org/10.1109/ICOEI48184.2020.9143018.

[8] I. G. N. Mantra, M. S. Hartawan, H. Saragih, and A. A. Rahman, “Web vulnerability assessment and maturity model analysis on Indonesia higher education,” *Procedia Comput Sci*, vol. 161, pp. 1165–1172, 2019, https://doi.org/10.1016/j.procs.2019.11.229.

[9] P. Pant *et al.*, “Authentication and Authorization in Modern Web Apps for Data Security Using Nodejs and Role of Dark Web,” *Procedia Comput Sci*, vol. 215, pp. 781–790, 2022, https://doi.org/10.1016/j.procs.2022.12.080.

[10] Y. Zhuang, Y. Choi, S. He, A. C. M. Leung, G. M. Lee, and A. Whinston, “Understanding Security Vulnerability Awareness, Firm Incentives, and ICT Development in Pan-Asia,” *Journal of Management Information Systems*, vol. 37, no. 3, pp. 668–693, 2020, https://doi.org/10.1080/07421222.2020.1790185.

[11] A. Tiwari, J. Prakash, S. Groß, and C. Hammer, "A Large Scale Analysis of Android — Web Hybridization," *Journal of Systems and Software*, vol. 170, p. 110775, 2020, https://doi.org/10.1016/j.jss.2020.110775.

[12] M. Liu, B. Zhang, W. Chen, and X. Zhang, "A Survey of Exploitation and Detection Methods of XSS Vulnerabilities," *IEEE Access*, vol. 7, pp. 182004–182016, 2019, https://doi.org/10.1109/ACCESS.2019.2960449.

[13] K. Kritikos, K. Magoutis, M. Papoutsakis, and S. Ioannidis, "A survey on vulnerability assessment tools and databases for cloud-based web applications," *Array*, vol. 3–4, p. 100011, 2019, https://doi.org/10.1016/j.array.2019.100011.

[14] M. Moniruzzaman, F. Chowdhury, and M. S. Ferdous, "Measuring Vulnerabilities of Bangladeshi Websites," *2nd International Conference on Electrical, Computer and Communication Engineering, ECCE 2019*, pp. 1–7, 2019, https://doi.org/10.1109/ECACE.2019.8679426.

[15] K. Sinchana, C. Sinchana, H. L. Gururaj, and B. R. Sunil Kumar, "Performance Evaluation and Analysis of various Network Security tools," *Proceedings of the 4th International Conference on Communication and Electronics Systems, ICCES 2019*, pp. 644–650, 2019, https://doi.org/10.1109/ICCES45898.2019.9002531.

[16] I. Alsmadi and F. Mira, "Website security analysis: Variation of detection methods and decisions," *21st Saudi Computer Society National Computer Conference, NCC 2018*, pp. 1–5, 2018, https://doi.org/10.1109/NCG.2018.8592962.

[17] H. Poston, "Mapping the OWASP Top Ten to Blockchain," *Procedia Comput Sci*, vol. 177, pp. 613–617, 2020, https://doi.org/10.1016/j.procs.2020.10.087.

[18] S. K. Shandilya, C. Ganguli, I. Izonin, and Prof. A. K. Nagar, "Cyber attack evaluation dataset for deep packet inspection and analysis," *Data Brief*, vol. 46, p. 108771, 2023, https://doi.org/10.1016/j.dib.2022.108771.

[19] L. Erdődi, Å. Å. Sommervoll, and F. M. Zennaro, "Simulating SQL injection vulnerability exploitation using Q-learning reinforcement learning agents," *Journal of Information Security and Applications*, vol. 61, p. 102903, 2021, https://doi.org/10.1016/j.jisa.2021.102903.

[20] Md. M. Hassan *et al.*, "Broken Authentication and Session Management Vulnerability: A Case Study of Web Application," *Int. J. Simul. Syst. Sci. Technol*, vol. 19, no. 2, pp. 1-11, 2018, https://doi.org/10.5013/IJSSST.a.19.02.06.

[21] A. W. Marashdih, Z. F. Zaaba, K. Suwais, and N. A. Mohd, "Web Application Security: An Investigation on Static Analysis with other Algorithms to Detect Cross Site Scripting," *Procedia Comput Sci*, vol. 161, pp. 1173–1181, 2019, https://doi.org/10.1016/j.procs.2019.11.230.

[22] G. Kaur, B. Pande, A. Bhardwaj, G. Bhagat, and S. Gupta, "Efficient yet Robust Elimination of XSS Attack Vectors from HTML5 Web Applications Hosted on OSN-Based Cloud Platforms," *Procedia Comput Sci*, vol. 125, pp. 669–675, 2018, https://doi.org/10.1016/j.procs.2017.12.086.

[23] F. Caturano, G. Perrone, and S. Pietro Romano, "Discovering reflected cross-site scripting vulnerabilities using a multiobjective reinforcement learning environment," *Comput Secur*, vol. 103, p. 102204, 2021, https://doi.org/10.1016/j.cose.2021.102204.

[24] M. Krishnan, Y. Lim, S. Perumal, and G. Palanisamy, "Detection and defending the XSS attack using novel hybrid stacking ensemble learning-based DNN approach," *Digital Communications and Networks*, p. S2352864822001997, 2022, https://doi.org/10.1016/j.dcan.2022.09.024.

[25] S. Nagpure and S. Kurkure, "Vulnerability Assessment and Penetration Testing of Web Application," *2017 International Conference on Computing, Communication, Control and Automation, ICCUBEA 2017*, pp. 1–6, 2018, https://doi.org/10.1109/ICCUBEA.2017.8463920.

[26] A. Wijayanto, E. Utami, and A. B. Prasetio, "Analysis of Vulnerability Webserver Office Management of Information And Documentation Diskominfo using OWASP Scanner," in *2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS)*, pp. 1–5. 2020, https://doi.org/10.1109/ICORIS50180.2020.9320833.

[27] M. A. Helmiawan, E. Firmansyah, I. Fadil, Y. Sofivan, F. Mahardika, and A. Guntara, "Analysis of Web Security Using Open Web Application Security Project 10," *2020 8th International Conference on Cyber and IT Service Management*, pp. 1-5, 2020, https://doi.org/10.1109/CITSM50537.2020.9268856.

[28] R. Rojas, A. Muedas, and D. Mauricio, "Security maturity model of web applications for cyber attacks," in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, pp. 130–137, 2019, https://doi.org/10.1145/3309074.3309096.

[29] S. Alazmi and D. C. De Leon, "A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners," *IEEE Access*, vol. 10, pp. 33200–33219, 2022, https://doi.org/10.1109/ACCESS.2022.3161522.

[30] N. Karangle, A. K. Mishra, and D. A. Khan, "Comparison of Nikto and Uniscan for measuring URL vulnerability," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–6, 2019, https://doi.org/10.1109/ICCCNT45670.2019.8944463.

[31] R. S. Devi and M. M. Kumar, "Testing for Security Weakness of Web Applications using Ethical Hacking," in *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, pp. 354–361, 2020, https://doi.org/10.1109/ICOEI48184.2020.9143018.

[32] J. Pauli, "Web Server Hacking," in *The Basics of Web Hacking*, pp. 19–40, 2013, https://doi.org/10.1016/B978-0-12-416600-4.00002-2.

[33] K. V. V. N. L. Sai Kiran, R. N. K. Devisetty, N. P. Kalyan, K. Mukundini, and R. Karthi, "Building a Intrusion Detection System for IoT Environment using Machine Learning Techniques," *Procedia Comput Sci*, vol. 171, pp. 2372–2379, 2020, https://doi.org/10.1016/j.procs.2020.04.257.

[34] I. Mantra, M. S. Hartawan, H. Saragih, and A. A. Rahman, "Web Vulnerability Assessment and Maturity Model Analysis on Indonesia Higher Education," *Procedia Comput Sci*, vol. 161, pp. 1165–1172, 2019, https://doi.org/10.1016/j.procs.2019.11.229.

[35] A. Subasi and E. Kremic, "Comparison of Adaboost with MultiBoosting for Phishing Website Detection," *Procedia Comput Sci*, vol. 168, pp. 272–278, 2020, https://doi.org/10.1016/j.procs.2020.02.251.

[36] A. F. Otoom, W. Eleisah, and E. E. Abdallah, "Deep Learning for Accurate Detection of Brute Force attacks on IoT Networks," *Procedia Comput Sci*, vol. 220, pp. 291–298, 2023, https://doi.org/10.1016/j.procs.2023.03.038.

[37] Q. Zhou, J. Yu, and D. Li, "A dynamic and lightweight framework to secure source addresses in the SDN-based networks," *Computer Networks*, vol. 193, p. 108075, 2021, https://doi.org/10.1016/j.comnet.2021.108075.

[38] H. Poston, "Mapping the OWASP Top Ten to Blockchain," *Procedia Comput Sci*, vol. 177, pp. 613–617, 2020, https://doi.org/10.1016/j.procs.2020.10.087.

[39] F. Caturano, G. Perrone, and S. Pietro Romano, "Discovering reflected cross-site scripting vulnerabilities using a multiobjective reinforcement learning environment," *Comput Secur*, vol. 103, p. 102204, 2021, https://doi.org/10.1016/j.cose.2021.102204.

[40] G. De Carvalho Bertoli *et al.*, "An End-to-End Framework for Machine Learning-Based Network Intrusion Detection System," *IEEE Access*, vol. 9, pp. 106790–106805, 2021, https://doi.org/10.1109/ACCESS.2021.3101188.

[41] E. Filiol, F. Mercaldo, and A. Santone, "A Method for Automatic Penetration Testing and Mitigation: A Red Hat Approach," *Procedia Comput Sci*, vol. 192, pp. 2039–2046, 2021, https://doi.org/10.1016/j.procs.2021.08.210.

[42] J.-S. Cho, S.-S. Yeo, and S. K. Kim, "Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value," *Comput Commun*, vol. 34, no. 3, pp. 391–397, 2011, https://doi.org/10.1016/j.comcom.2010.02.029.

BIOGRAPHY OF AUTHORS

Muchammad Zaidan, A student majoring in informatics in 2018 who is currently pursuing undergraduate education, he also takes the field of interest in Network Security. Not only that, he pursued expertise in the field of Software Engineering, namely in the manufacture of queuing machines at a company. Email: muchammadzaidan@webmail.umm.ac.id. Orcid: 0009-0007-0874-2120.

Febyola Noeraini, Students majoring in Informatics in 2018 who are currently pursuing undergraduate education at the University of Muhammadiyah Malang. Have an interest and focus in the field of Network Security. Email: febyolanoeraini@webmail.umm.ac.id.

Zamah Sari, He earned a Bachelor of Engineering (ST) in 2002 at the University of Muhammadiyah Malang and then continued his S2 education at Brawijaya University in 2013 and heard the acquisition of a Master of Engineering (MT). Until now, he joined as a permanent lecturer in the field of informatics at the University of Muhammadiyah Malang. He is also active in conducting various researches in developing information systems. Email: zamahsari@umm.ac.id.

Denar Regata Akbi, He earned his Bachelor of Computer (S.Kom) degree in 2010 at the University of Muhammadiyah Malang and then he continued his S2 education at the Ten November Institute of Technology. Until finally obtaining a Master of Computer (S.Kom) degree in 2016. Currently, he is a permanent lecturer at the University of Muhammadiyah Malang. Email: dnarregata@umm.ac.id.