ISSN 1978-0524 (print) | 2528-6374 (online)
http://journal.uad.ac.id/index.php/JIFO/index

Analysis Of SIPS.BAWASLU.GO.ID Web Security Level Using OWASP ZAP And Acunetix

Chandra Surya[1], Eko Aribowo[2]

[1]Program Studi Informatika, Universitas Ahmad Dahlan, Yogyakarta
[2]Program Studi Informatika, Universitas Ahmad Dahlan, Yogyakarta
Jl.Ringroad Selatan, Kragilan, Tamanan Yogyakarta, 55191
[1]chandra1900018101@webmail.uad.ac.id, [2]ekoab[at]tif.uad.ac.id
* Corresponding Author

Received 25 February 2015; accepted 8 May 2015; published 13 May 2015

ABSTRACT

Website SIPS BAWASLU RI merupakan website sistem informasi penyelesaian sengketa pemilihan dan pemilu yang terdiri dari sub sistem informasi meliputi permohonan sengketa baik secara online maupun offline. Hasil dari penelitian ini menampilkan beberapa kerentanan-kerentanan pada website SIPS BAWASLU RI , setiap bagiannya akan ditampilkan level risk, mulai dari high, medium, dan low. Penelitian ini menggunakan tools OSWASP ZAP, tools kedua akan menggunakan Acunetix, dalam proses information gathering menggunkanan tools MALTEGO, tools MALTEGO akan menampilkan informasi dari web tersebut.Hasil dari analisis website sips.bawaslu.go.id ditemukan beberapa bagian yang level risknya *high, medium, low,* dan *informational*. Setelah mendapatkan hasil vunerability scanning, selanjutnya adalah melakukan pengujian attacking dengan menggunakan tools attacking seperti, *Metasploit dan Burpsuite*. Pada pengujian attacking beberapa kerentanan dapat dibuktikan. Nantinya hasil pengujian *attacking* akan dimasukkan pada tahapan analisis. Apabila pengujian tersebut telah dijabarkan dalam tahapan analisis selanjutnya adalah memberikan rekomendasi perbaikan.

KEYWORDS
keamanan
Web
Penetration Testing
OWASPZAP
Scanning
Burpsuite

1. Introduction

Banyak tidak diketahui bahwa banyak sisi kelemahan dari internet itu sendiri, sebagai contoh adalah aplikasi web, aplikasi web sangat rentan dari serangan *hacker*, terkadang mereka tidak memproteksi web mereka dari berbagai serangan, mulai dari serangan malware, phising, DOS (*Denial Of Service*), Eksploitasi, dll. Sehingga sampai detik ini tidak ada *website* yang aman dari berbagai serangan. Salah satu cara untuk memproteksi suatu web yaitu dengan mengananalisis tingkat keamanan web itu sendiri[2].

Terkait dengan penelitian ini objek yang digunakan adalah aplikasi website sips.bawaslu.go.id. Aplikasi sips.bawaslu.go.id merupakan website Sistem Informasi Penyelesaian Sengketa pemilihan dan pemilu, informasi mengenai website sips.bawaslu.go.id bahwasannya beberapa waktu yang lalu website sips.bawaslu.go.id mendapat serangan, oleh karena itu web yang menjadi objek penelitian sangat direkomendasikan agar menerapkan analisis keamanan terhadap aplikasi, yang bertujuan untuk meminimalisir terjadinya gangguan pada kinerja aplikasi berbasis web sehingga harus adanya evaluasi terhadap keamanan sistem aplikasi. Dengan adanya Analisis Keamanan Aplikasi Web sips.bawaslu.go.id dengan tujuan menemukan keretanan dan menguji pada aplikasi sehingga pemilik aplikasi web tersebut dapat memperbaiki dan meningkatkan keamanan dari sebuah aplikasi [3].

Pada peneltian kali ini tahapan pertama yang dilakukan adalah Vulnerability scanning dengan menggunakan tools OWASP ZAP dan Acunetix untuk mendeteksi kerentanan seperti injeksi SQL dan XSS, private IP *disclosure, application error disclosure*, hasil vulnerability scanning dari OWASP ZAP dan Acunetix akan menjadi acuan dalam tahapan attacking. Tahapan attacking menjadi pembuktian terhadap hasil vulnerability scanning. Tools yang digunakan dalam tahapan attacking berdasarkan dengan kebutuhan hasil vulnerabitly scanning. Setelah melakukan attacking tahapan selanjutnya adalah dengan melakukan analisis terhadapa kerentanan tersebut, setelah melakukan analisis langkah selanjutnya adalah melakukan rekomendasi perbaikan terhadap system[4].

Penjabaran penelitian terdahulu sebagai acuan tolak ukur yang mendasari tinjauan pustaka penelitian ini. Setelah penjabaran penelitian terdahulu selanjutnya adalah penjabaran teori yang menjadi komponen pendukung penelitian ini.Penelitian yang dianalisis oleh Dedy Hariyadi, Faulinda Ely Nastiti dengan judul penelitian Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta. Keamanan web suatu instansi pendidikan sangatlah penting, sebab web didalam web instansi pendidikan memuat data-data penting, baik data pelajar, data guru atau dosen, dan database. Objek penelitian yang dituju adalah Universitas Duta Bangsa Surakarta, penelitian ini dilakukan karena menurut Badan Siber dan Sandi Negara tahun 2020 serangan web defacement kepada instansi perguruan tinggi sangat tinggi, dan Universitas Duta Bangsa Surakarta menjadi salah satu objek serangan web defacement, oleh karena itu penelitian ini dilakukan untuk menganalisis website Universitas Dutas Bangsa Surakarta menggunakan metode sudomy dan OWASP ZAP dengan beberapa tahapan analisis yang dilakukan antara lain : Network Mapping, Vulnerability Identification, dan Information Gathering[4].

1.1. Pengertian Website

Website merupakan kumpulan halaman pada suatu domain di internet yang dirancang untuk tujuan yang dituju dan saling berkaitan dan bisa diakses dengan lingkup luas melalui halaman utama (home page) memakai suatu browser dengan URL website. Salah satu contoh mendasar dari suatu *Website* adalah mempunyai informasi/content yang bersifat statis dengan pengertian jarang diubah*[9]*.

1.2. Pengertian Information Gathering

Tahap information gathering merupakan tahap unutk memperoleh informasi dari suatu website dan domain, dalam tahap ini peneliti menggunakan Internet untuk mencari informasi secara detail dari target (Perusahaan atau Orang), dalam tahap information gathering tools yang digunakan terbagi dalam 2, yaitu dengan menggunakan tools teknikal dan non-teknikal, tools teknikal seperti WHOIS dan tools non-teknikal seperti Search Engine. Information Gathering tidak mengharuskan penulis untuk terhubungan dengan sistem target. Informasi bisa didapatkan melalui sumber-sumber publik seperti internet, dan organisasi-organisasi yang mempunyai informasi public, seperti perpustakaan dan lain-lain[11]..

1.3. Pengertian Vulnerability Assesment

Vulnerability Assessment adalah metode pengujian yang memiliki sifat yang berhubungan dengan penerapan suatu automation Vulnerability scanner. Dalam proses pengujian penetration test, orang yang melakukan pengujian akan mencoba melakukan validasi dari suatu hasil yang dihasilkan dan menjelaskan penjelasan seperti rekomendasi akan suatu issue yang valid. Oleh karena itu, hasil dari penetration test ini belum dapat dijadikan sebagai acuan utama, hal ini dianggap kurang bisa mengidentifikasi akan resiko yang dihasilkan secara maksimal. Disisi lain Penetration Test berfokus pada bidang yang lain seperti pada bidang signature yang dipunyai oleh setiap automation Vulnerability scanner, kegiatan dapat dikatakan belum bisa sepenuhnya menjadi acuan dalam hal

melakukan pengujian (flow) dari masalah yang pada umumnya terdapat di dalam implementasi suatu aplikasi[10].

1.4. Pengertian Penetration Testing

Proses serangan yang dilakukan seperti sql injection, xss, clickjacking, dll, bertujuan untuk menentukan dan mengetahui macam – macam serangan yang mungkin terjadi karena kelemahan sistem. Alur baku tahapan penetration testing menjadi acuan dalam tahapan penelitian[9].

1.5. Pengertian OWASP

OWASP (Open Web Application Security Project) adalah komunitas terbuka yang mendedikasikan untuk membuat sebuah organisasi yang bertujuan untuk mengembangkan, membeli, dan memelihara aplikasi yang terpercaya. Di OWASP pengunjung akan menemukan semua bebas dan terbuka. Seluruh tools, dokumen, forum, dan cabang OWASP bebas dan terbuka bagi semua orang yang tertarik memperbaiki aplikasi keamanan. OWASP mendukung pendekatan keamanan aplikasi sebagai masalah perseorangan, proses, dan masalah teknologi karena pendekatan paling efektif terhadap keamanan aplikasi membutuhkan perbaikan diseluruh area. OWASP adalah jenis organisasi baru yang bebas dari tekanan komersial sehingga memungkinkan untuk memberikan informasi terkait keamanan aplikasi yang tidak bias, praktis, dan efektif biaya[10].

1.6. Pengertian OWASP ZAP

OWASP ZAP adalah tools yang digunakan untuk penetration test dan vulnerabilities scanner yang dikembangkan oleh suatu organisasi OWASP (Open Web Application Security Project). Tools OWASP ZAP bisa mendeteksi injeksi SQL dan XSS, private IP disclosure, application error disclosure[8].Pengertian Scanning Tools

1.7. Pengertian Acunetix

Acunetix Web Vulnerability Scanner otomatis dapat memeriksa dan memindai web application yang teridentifikasi memiliki kerentanan terhadap SQL Injection , XSS, CSRF dan kerentanan web lainnya. Tool Acunetix Web Vulnerability Scanner dapat menampilkan level dari hasil scanning. Pada severity levels dari acunetix yang akan menjelaskan tingkat keamanan dari URL atau IP address yang discanning [12].

1.8. Pengertian Maltego

Maltego merupakan aplikasi open source intelligence (OSINT) dan alat analisis tautan grafis untuk mengumpulkan dan menghubungkan informasi untuk tugas-tugas investigasi. Open-source intelligence (OSINT) adalah disiplin intelijen yang berkaitan dengan kecerdasan yang dihasilkan dari informasi yang tersedia secara publik yang dikumpulkan, dieksploitasi, dan disebarluaskan pada waktu yang tepat kepada khalayak yang tepat untuk tujuan pengalamatan kebutuhan informasi dan intelijen khusus. Aplikasi Maltego dapat melakukan footprinting yaitu mengumpulkan informasi sebanyak mungkin dari situs web yang dilakukan forensik digital.Sistem operasi yang digunakan untuk menjalankan aplikasi Maltego yaitu Parrot OS yang merupakan sistem operasi open source[13].

.

2.Method

2.1. Objek Penelitian

Dalam penelitian ini objek yang digunakan adalah aplikasi website sips.bawaslu.go.id. Aplikasi sips.bawaslu.go.id adalah website Sistem Informasi Penyelesaian Sengketa pemilihan dan pemilu yang terdiri dari sub sistem informasi meliputi Permohonan

ISSN 2086-8138 (print) | 2745-7249 (online)
Jurnal Informatika
Vol. 1., No. 1, April 2020, pp. 1-8

Sengketa baik langsung maupun online, verifikasi formil dan materiil, registrasi , musyawarah/ajudikasi, putusan dan tindaklanjut putusan., website sips.bawaslu.go.id memiliki manfaat Mendigitalisasi proses permohonan sengketa, sampai dengan putusanan. Fitur SIPS antara lain permohonan online, data register permohonan, data putusan, grafik serta lainnya yang berkaitan dengan proses permohonan sengketa Bawaslu, baik data sengketa pemilihan maupun.

Sumber : (*sips.bawaslu.go.id*)

2.2. Metode pengumpulan Data

Metode pengumpulan data yang dilakukan dalam penelitian ini adalah obervasi, melalui chat wa dengan admin sips.bawaslu.go.id, bahwasannya beberapa bulan yang lalu website sips.bawaslu.go.id mengalami serangan oleh oknum yang tidak bertanggung jawab. Setelah itu mencari permasalahan yang dilakukan dan pendalaman materi lebih lanjut dengan mencari tahu metode apa yang telah digunakan serta kelebihan dan kekurangan dari masing-masing metode. Sehingga diperoleh metode yang diusulkan untuk mengetahui apakah efektif juga digunakan untuk permasalahan yang diambil pada penelitian ini.

2.3. Analisis Kebutuhan

2.3.1 Perangkat Lunak (software)

Perangkat lunak yang digunakan dalam penelitian kali ini adalah :

a. Kali Linux
b. Acunetix
c. OWASP ZAP
d. MALTEGO

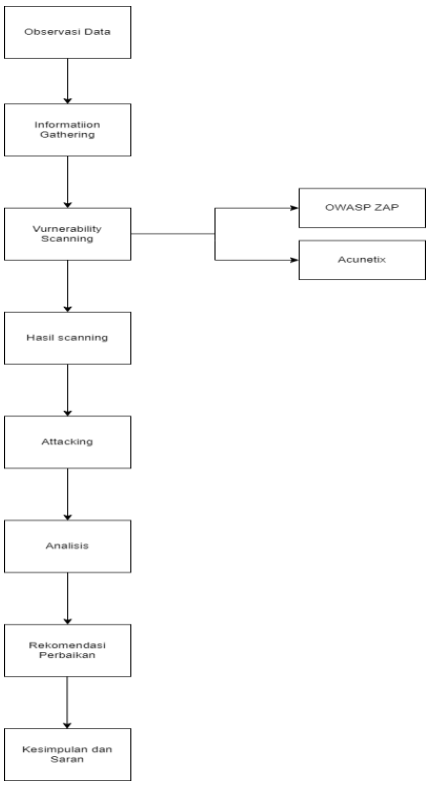
2.3.1 Perangkat Keras (Hardware)

Perangkat keras yang digunakan dalam penelitian kali ini adalah :

a. Manufacture : ASUS ROG (Republic Of Game)
b. Prosessor : Intel Core i7 770HQ Quadcore 2,8GHZ
c. RAM : 8GB 2400 Mhz
d. Storage : 1 TB
e. GPU : Geforce GTX1050

ISSN 2086-8138 (print) | 2745-7249 (online)

2.4. Tahapan Penelitian



Gambar 2.1 Alur tahapan penelitian

3. Results and Discussion

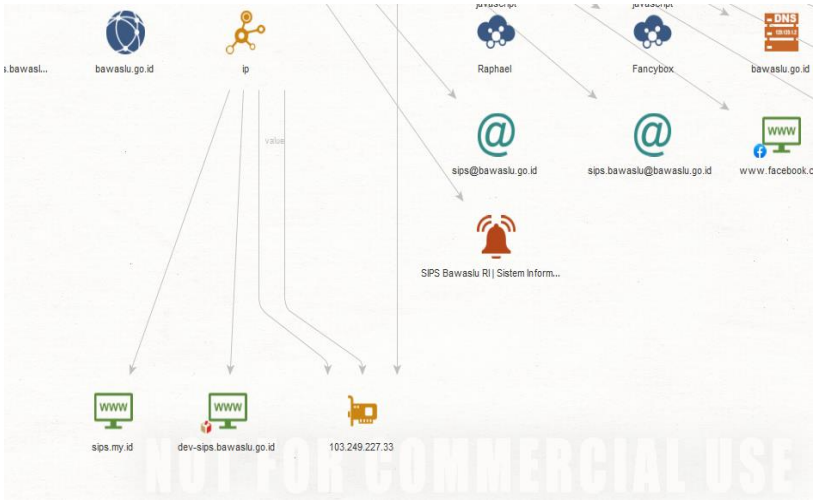
A. Observasi Data

Dalam permasalahan pada penelitian kali ini data yang didapatkan bahwasannya website sips.bawaslu.go.id beberapa waktu yang lalu mendapatkan serangan oleh oknum yang tidak bertanggung jawab berdasarkan percakapan Whatssapp dengan admin sips.bawaslu.go.id, beliau memberikan informasi bahwasannya seluruh file berbentuk pdf yang diupload ke https://sips.bawaslu.go hilang dan muncul keterangan dalam website tersebut error kode nginx, setelah mendapatkan informasi tersebut langkah selanjutnya adalah melakukan analisis terhadap website sips.bawaslu.go.id.

ISSN 2086-8138 (print) | 2745-7249 (online)
Jurnal Informatika
Vol. 1., No. 1, April 2020, pp. 1-8

B. Information Gathering

Tahap Information gathering merupakan salah satu metode dalam penelitian ini, tahapan ini berfungsi untuk mencari informasi dari target-target dengan menggunakan tools non-teknikal, tool yang digunakan dalam tahapan ini adalah MALTEGO, MALTEGO memfokuskan pencarian informasi melalu data-open source dan memvisualkan ke dalam format graph, dalam penelitian ini menggunakan MALTEGO community edition dengan platform windows + Java (x64) dan didapatkan hasil seperti gambar 3,1. Dari gambar tersebut terdapat informasi alamat IP pada website sips.bawaslu.go.id, yaitu "193.249.227.33" dan untuk alamat email yang mengelola website tersebut adalah sips@bawaslu.go.id dan sips.bawaslu@bawaslu.go.id , dan framework yang digunakan adalah Ruby on Rolls Token.



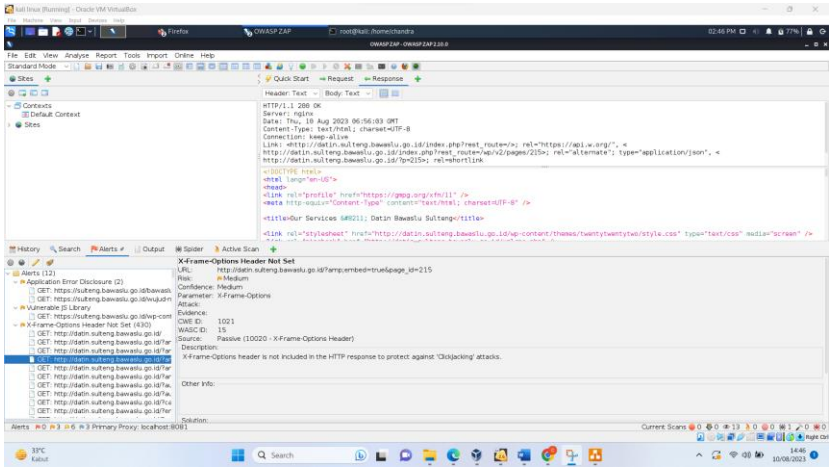
Gambar 3.1 Hasil Scanning Maltego

C. Vulnerability Scanning

Vulnerability scanning bertujuan untuk mencari celah keamanan website sips.bawaslu.go.id dengan subdomain, tools yang digunakan adalah OWASP ZAP dan Acunetix.

a. OWASP ZAP

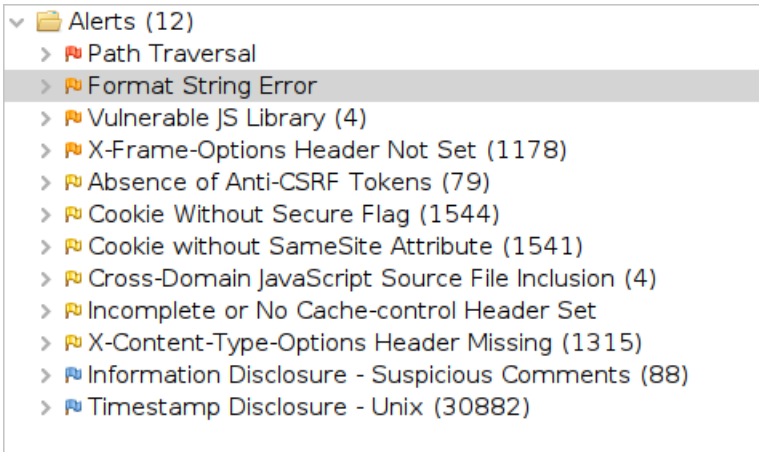
Selanjutnya peneliti menggunakan *tools* OWASP ZAP, setelah membuka tools OWASP ZAP di kali linux terdapat tampilan utama OWASP ZAP didalam tampilan utama OWASP ZAP yaitu URL to attack, Use traditional spider, Use ajax spider. Kemudian memasukkan objek yang akan di scanning ke dalam URL to attack, objek yang dimasukkan adalah sips.bawaslu.go.id, dengan mencentang kolom, Use Traditional spider, dan memilih Use ajax spider "Firefox", setelah mengisi semua prosedur yang dilakukan kemudian attack. Nantinya hasil OWASP ZAP terdapat pada menu alerts, yang menjadi acuan di dalam menu alerts ialah bagian yang high dan medium dan didapatkan hasil seperti gambar 3.2. Dari gambar tersebut didapatkan bahwa *sips.bawaslu.go.id* terdapat 3 medium alert yang pertama ialah alert application error disclosure, vurnerable JS library dan x-frame-options Header not set. Di dalam error disclosure terdapat 2 klasifikasi, pada bagian JS library terdapat 1 klasifikasi, dan pada x-frame-options Header not set terdapat 455 bagian klasifikasi.



Gambar 3.2 Hasil scanning OWASP ZAP

b. Acunetix

Tools selanjutnya ialah Acunetix website application scanner merupakan perangkat lunak yang dikembangkan untuk melakukan scanning. Tools Acunetix memilik kemampuan untuk memberikan solusi dari kelemahan yang ditemukan dan mengelola traceability dari setiap vulnerabilities tersebut. Pada tampilan Acunetix enampilkan tampilan proses scanning Acunetix pada website sulteng.bawaslu.go.id, di dalam tampilan proses scanning Acunetix terdapat menu “Scan Information”, “Vulnerabilites”, “Site Structure”, “Events, Activity”, dan “Target Information”. Di dalam menu “Scan Information” terdapat “Acunetix Threat LEVEL”, “scan duration” dan “request”, dan di dalam menu Activity terdapat tampilan “Start URL changes (Initial request to http://sips.bawaslu.go.id/was redirected to https://sips.bawaslu.go.id/)”, tampilan kedua ialah “(Scanning of sips.bawaslu.go.id started)”, dan terakhir terdapat tampilan “Antivirus not found”, dan tampilan ketiga ialah “Target Information” dengan deskripsi (Address: sips.bawaslu.go.id, scan nginx, dan Operation system: Unknown). Jika telah menjabarkan tampilan proses scanning Acunetix, langkah selanjutnya ialah menunggu proses scanning, apabila proses scanning telah selesai, penulis membuka halaman Vulnerabilities untuk melihat celah keamanan pada website sips.bawaslu.go.id. Pada gambar 3.3 merupakan hasil scanning Acunetix terdapat beberapa celah keamanan yaitu Path Traversal, Format String Error, Vulnerable JS Library



Gambar 3.3 Hasil scanning Acunetix

D. Hasil Scanning

Pada tahapan adalah proses identifikasi mengenai celah keamanan, evaluasi, dan mengklasifikasikan jenis kerentanan berdasarkan *risk* dengan *security level*. Pada *owasp* security level berupa *high, medium, low.* Dan pada *Acunetix* diukur menggunakan *severity* berupa *high, medium, low*, dan *confidence* diukur dengan *certain, firm, tentative.*

a. OWASP ZAP

Table 3.1 Hasil pengujian OWASP ZAP

No	Alert Group	Severity	Alert Count
1.	Path Traversal	High	10
2.	Format String Error	High	1
3.	Vulnerable JS Library	Medium	3
4.	X-Frame Options Header Not Set	Medium	1
5.	Absence Of Anti-CSRF Tokens	Medium	2
6.	Cookie Without Secure Flag	Low	-
7.	Cookie's without Samseite Attribute	Low	4

8.	Cross Domain Java Script Source File Inclusion	Low	1
9.	Incomplete or No Cache-control Header Not Set	Low	2

b. Acunetix

Table 3.2 Hasil pengujian Acunetix

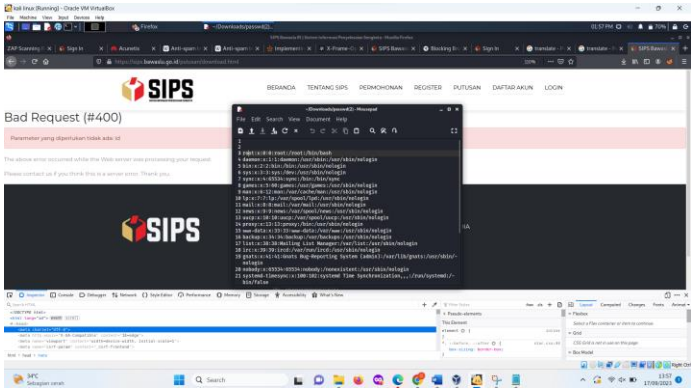
No	Alert Group	Severity	Alert Count
1.	Cross Site Scripting	High	10
2.	Directrory Traversal	High	1
3.	Development Configuration File	Medium	3
4.	TLS 1.0 enabled	Medium	1
5.	Vulnera JS Library	Medium	2
6.	Clickjacking : X-Frame Options header missing	Low	-
7.	Cookie's without secure flag	Low	4
8.	Documention File	Low	1
9.	Login Page Password-Guesing attack	Low	2

E. Attacking

a. Owasp Zap

1) Path Traversal

Path traversal merupakan kerentanan yang ditemukan dalam hasil vulnerability scanning dengan level alert high, OWASP ZAP mendeskripsikan bagian URL yang akan diserang yaitu pada bagian "https:sips.bawaslu.go.id/putusan/download.hmtl?id=", dengan method "GET", parameter bagian "id", setelah menjabarkan parameter yang akan diserang, selanjutnya adalah proses serangan dengan membuka halaman URL target beserta dengan script path traversal yaitu"https:sips.bawaslu.go.id/putusan/download.hmtl?id=..%2f..%2F..%2F..%2F..%2
F..%2F..%2F..%2etc%2Fpasswd" pada halaman firefox, apabila menjalankan url beserta script makan akan muncul tampilan seperti pada gambar 3.4.

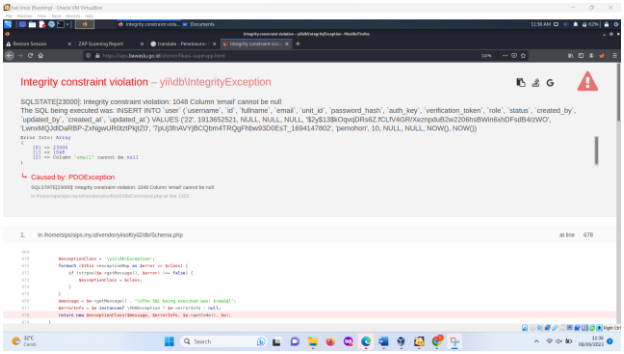


Gambar 3.4 Hasil pengujian Path Traversal

Dari gambar 3.4 disimpulkan bahwa menampilkan daftar direktori yang berisi username dan password, berdasarkan pengujian ini dapat disimpulkan bahwa pengujian serangan path traversal berhasil dilakukan.

2) Format string error

Dalam bagian vulnerability Format string error OWASP ZAP mendeskripsikan kesalahan format string terjadi ketika data yang dikirimkan dari string input dievaluasi sebagai perintah oleh aplikasi. Kerentanan fromat string eror URL target yang di deskripsikan oleh OWASP ZAP adalah "https://sips.bawaslu.go.id/site/verifikasi-superapp.html", dengan method "POST", parameter bagian Verifikasi[password], selanjutnya adalah proses attacking dengan membuka halaman URL target yaitu https://sips.bawaslu.go.id/site/verifikasi-superapp.html, setelah membuka halaman tersebut, selanjutnya adalah memasukkan script pada bagian parameter Verifikasi[password], script yang digunakan adalah "ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s", impelentasi dari penggunaan script tersebut akan ditampilkan dalam gambar 3.8

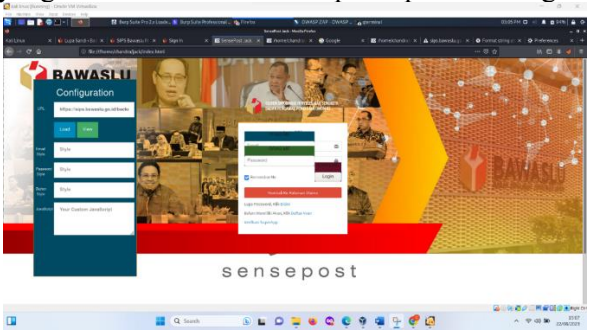


Gambar 3.1 Integirty constarint violation

Hasil pengujian pada gambar 3.8 disimpulkan setelah menjalankan script tersebut akan muncul tampilan halaman integrity constraint violation. Integrity constraint violation atau biasa disebut pelanggaran batasan integritas terjadi ketika pernyataan insert, update, atau delete statement violates pada primary key, foreign key, check.

3) X-Frame Options Header Not Set

Pengujian attacking selanjutnya adalah X-Frame Options Header Not set, pengujian ini dilakukan untuk membuktikan potensi serangan clickjacking pada website sips.bawaslu.go.id. pengujian dilakukan dengan menggunakan tools sensepostjack. Langkah pertama yang dilakukan adalah memasukkan salah satu parameter URL, dalam penelitian ini parameter URl yang dimasukkan adalah “https://sips.bawaslu.go.id seperti pada gambar 3.9

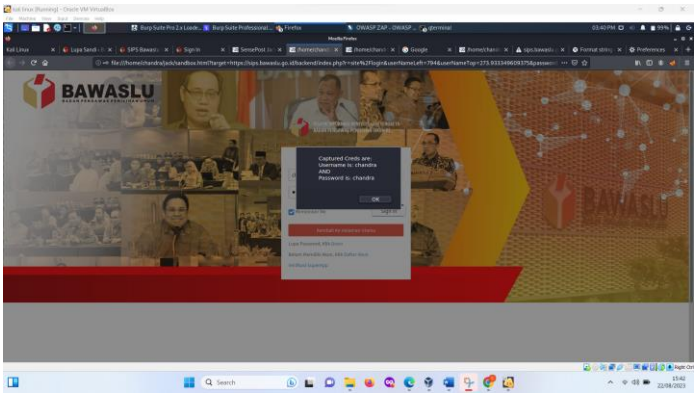


Gambar 3.9 Icon Sensepostjack

Pada gambar 3.9 berisi icon dari sensepostjack yang dapat diterapkan dalam website “https://sips.bawaslu.go.id/” , icon tersebut dapat dimodifikasi menjadi form login, apabila website “https://sips.bawaslu.go.id/” sudah dimodifikasi menjadi form login, langkah selanjutnya adalah mengclick icon view untuk melihat hasil website yang sudah dimodifikasi seperti pada gambar 3.10.

Gambar 3.10 Form Login Sensepostjack

Gambar 3.10 merupakan tampilan dari website "https://sips.bawaslu.go.id/" yang sudah dimodifikasi menjadi form login, selanjutnya adalah memasukkan "Email" dan "password", apabila sudah mengisi form login tersebut nantinya akan muncul pop up seperti gambar 3.11

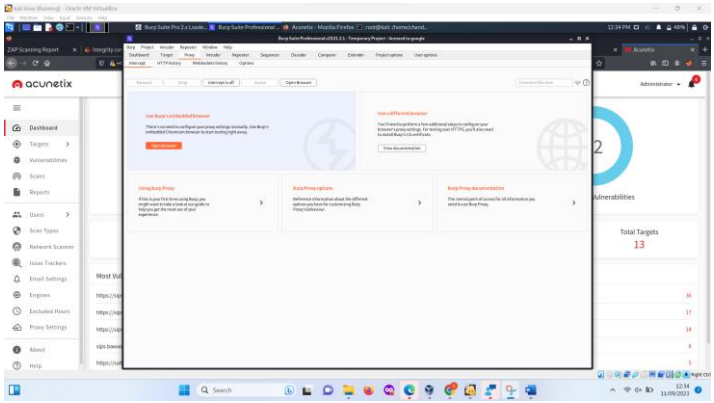


Gambar 3.2 Hasil pengujian Sensepostjack

b. Acunetix

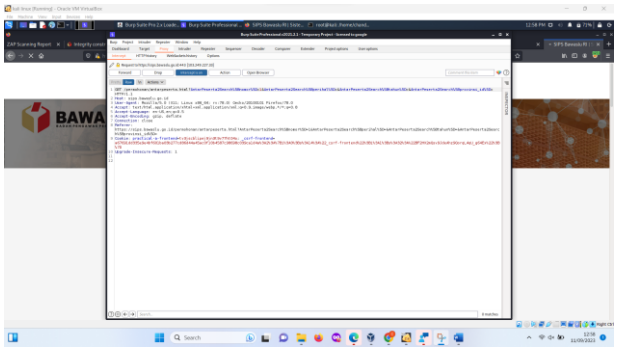
1) Cross Site scripting

Salah satu kerentanan berdasarkan hasil vulnerability scanning menggunakan Acunetix pada tabel adalah cross site scripting terdapat 11 kerentanan cross site scripting dengan severity high pengujian cross site scripting pada tahapan attacking akan menggunakan tools Burp Suite, Langkah pertama dalam pengujian cross site scripting pada website sips.bawaslu.go.id adalah membuka tools burpsuite pada kali linux seperti pada gambar 3.12.



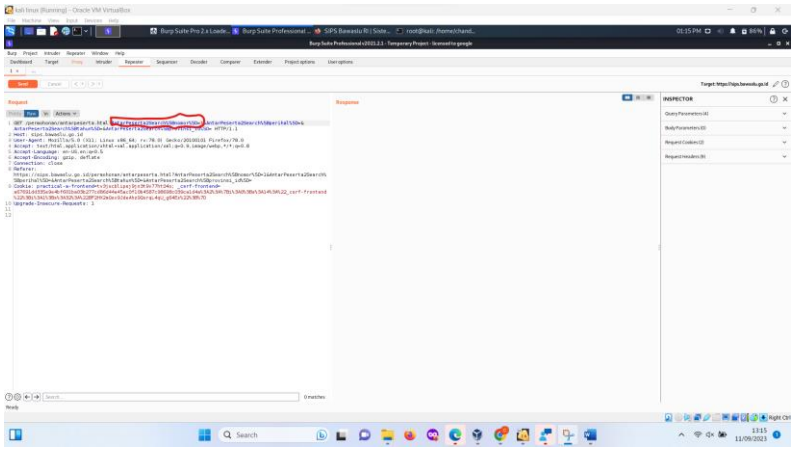
Gambar 3.12 Burpsuite

Selanjutnya merupakan tampilan tools burpsuite pada kali linux, setelah membuka tools burpsuite, selanjutnya adalah membuka URL target pada firefox, salah satu parameter URL target yang digunakan adalah "https://sips.bawaslu.go.id/permohonan/antarpeserta.html,AntarPeserta2Search
[nomor]. Sebelum membuka URL tersebut di firefox, terlebih dahalu menyalakan intercept pada Burpsuite, Setelah menyalakan intercept pada burpsuite seperti pada gambar 4.25 lalu membuka halaman URL target yaitu "https://sips.bawaslu.go.id/permohonan/antarpeserta.html,AntarPeserta2Search
[nomor], maka otomatis intercept akan menangkap request dari URL tersebut, seperti pada gambar 3.13



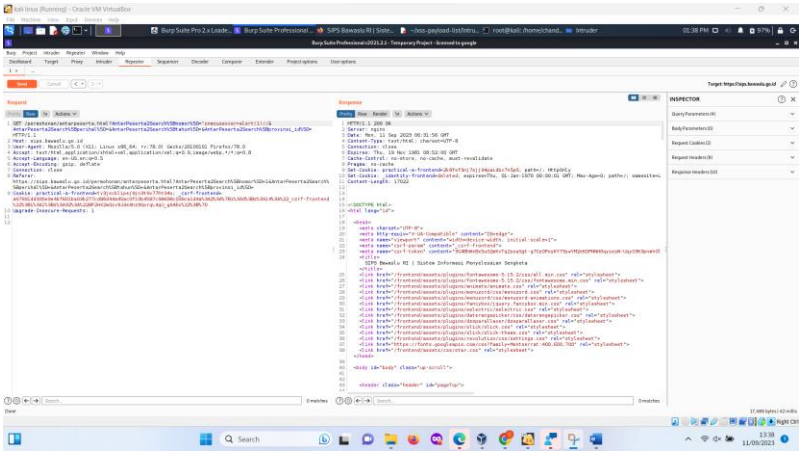
Gambar 3.13 Request Intercept

Setelah intercept menangkap request dari URL tersebut yang ditunjukkan pada gambar 4.26 tahapan selanjutnya adalah mengirimkan hasil intercept pada repeater, salah satu parameter dari hasil repeater yang nantinya akan dimasukkan XSS script, parameter yang digunakan adalah "AntarPeserta%2Search%5nomor%5D", seperti pada gambar 3.14.



Gambar 3.14 Parameter AntarPeserta%2Search%5nomor%5D

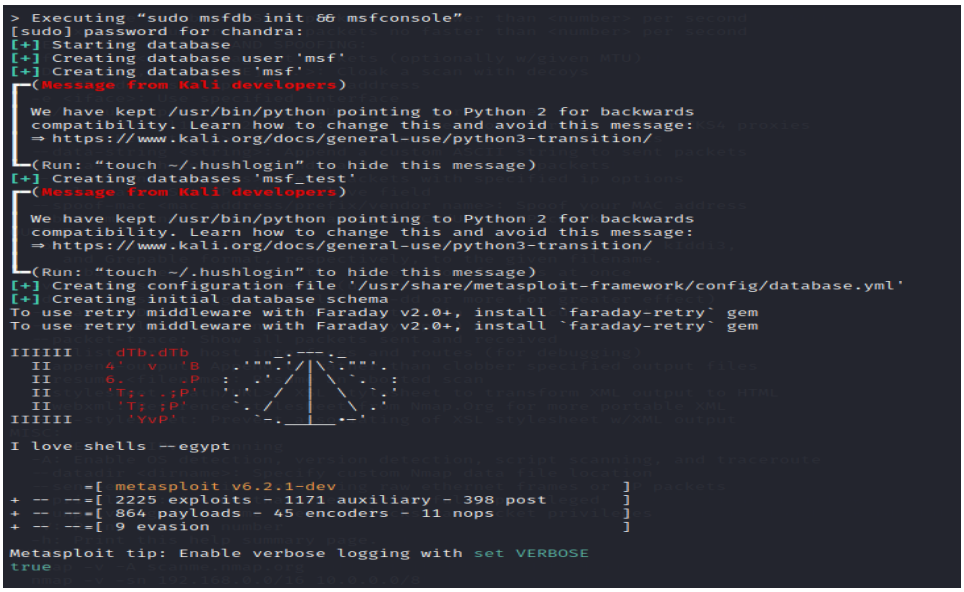
Gambar 3.14 merupakan tampilan halaman parameter yang akan dimasukkan XSS script, setelah menentukan parameter yang akan dimasukkan XSS script, tahapan selanutnya adalah memasukkan XSS script pada parameter tersebut, XSS script yang digunakan adalah "onmouseover=alert(1)", kemudian memasukkan script "onmousepver=alert(1)" pada parameter "AntarPeserta%2Search%5nomor%5D=" lalu mengirimkan request tersebut seperti pada gambar 3.15



Gambar 3.15 Request Cross Site scripting

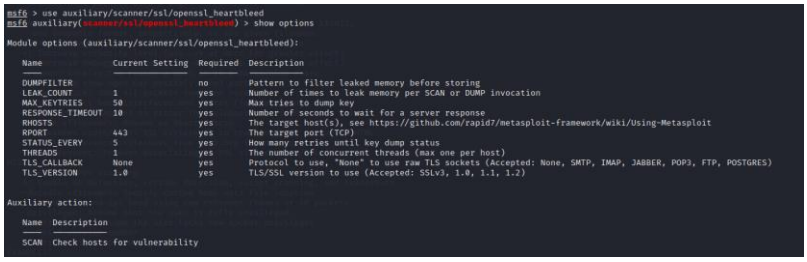
2) TLS 1.0 enabled

TLS 1.0 tidak dianggap sebagai "kriptografi kuat" seperti yang didefinisikan dan diwajibkan oleh Standar Keamanan Data PCI 3.2. ketika digunakan untuk melindungi informasi sensitif yang ditransfer ke atau dari situs web. Menurut PCI, "30 Juni 2018 adalah batas waktu untuk menonaktifkan SSL/TLS awal dan menerapkan protokol enkripsi yang lebih aman, untuk melakukan pembuktian apakah ssl pada ip 103.249.227.33 yang merupakan alamat IP sips.bawaslu.go.id terbuka, pembuktian dilakukan dengan menggunakan tools Metasploit. Oleh karena tools Metasploit dapat melihat respon dari TLS 1.0 enabled langkah pertama yang dilakukan adalah membuka tools Metasploit pada kali linux dengan mengetikkan syntax "sudo msfdb init && msfconsole" seperti pada gambar 3.16



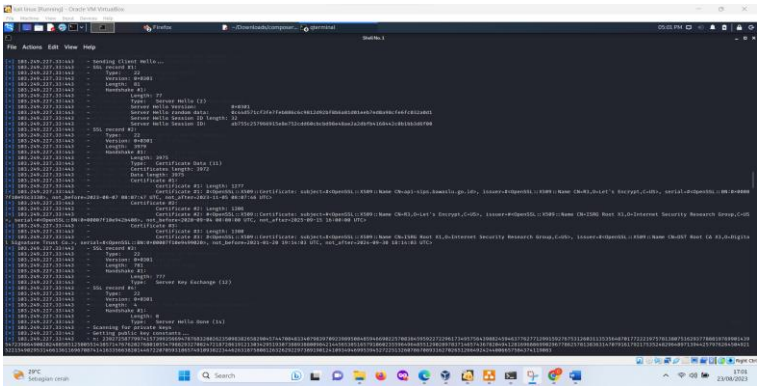
Gambar 3.3 Metasploit

Gambar 3.16 menampilkan hasil dari tools Metaspolit pada kali linux, apabila tools Metasploit telah dibuka langkah selanjutnya adalah menggunakan salah satu komponen pada Metasploit yaitu "scanning ssl heartbleed" dengan memasukkan syntax "use auxiliary/scanner/ssl/openssl_heartbleed" seperti yang ditampilkan pada gambar 3.17



Gambar 3.17 OpenSSL Heartbleed

Gambar 3.17 menampilkan dari penggunaan "scanner/ssl/openssl_heartbleed", apabila sudah masuk ke dalam "scanner/ssl/openssl_heartbleed" langkah selanjutnya adalah memasukkan ip address dan port target, target pada penelitian kali ini adalah https://sips.bawaslu.go.id dengan port 443, apabila sudah menentukan ip address target dan port, selanjutnya adalah memasukkan ip address dengan menggunakan syntax "set RHOST 103.249.227.33" dan memasukkan port dengan menggunakan syntax "set RPORT 443". Seperti pada gambar 3.18

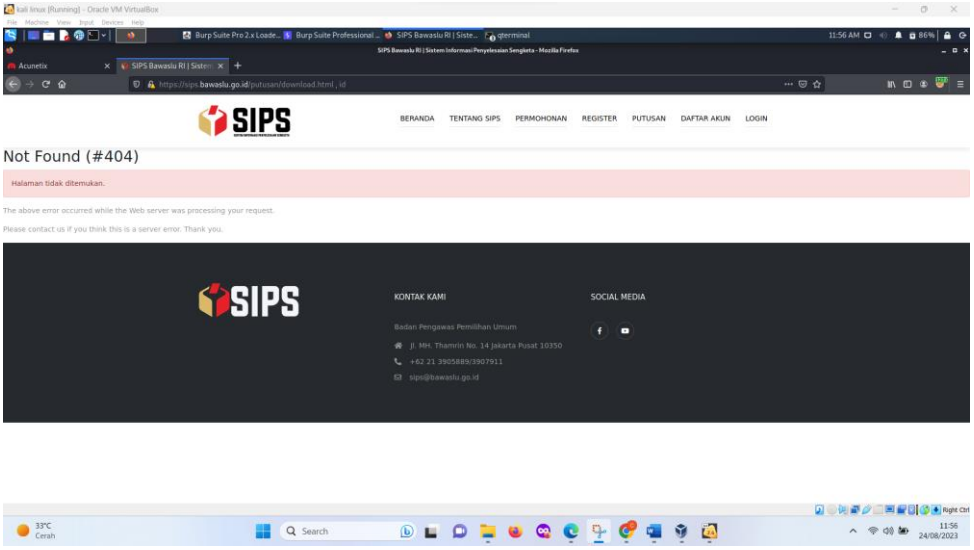


Gambar 3.18“scanner/ssl/openssl_heartbleed”

Pada gambar 3.18 menampilkan hasil dari “scanner/ssl/openssl_heartbleed”, hasil dari scanning tersebut adalah tidak terdapat vurnerabilities dalam openSSL, tetapi dalam permasalahan ini Metasploit dapat berkomunikasi dengan server dan mampu menarik data acak dari memori server.

3) *Directory Traversal*

Dalam hasil vulnerability scanning menggunakan Acunetix ditemukan kerentanan Path Traversal dengan severity high, dalam tahapan attacking sebagai pembuktian kerentanan Path Traversal tools yang digunakann adalah Burpsuite . Apabila tools Burp-suite sudah dijalankan langkah selanjutnya adalah membuka website target berdasarkan vurnerability affect acunetix yaitu “https:sips.bawaslu.go.id/putusan/download.html, id”, sebelum membuka website tersebut nyalakan intercept terlebih dahulu seperti pada gambar 3.19.



Gambar 3.19 tampilan website berdasarkan vurnerability affects

Gambar 3.19 menampilkan tampilan website berdasarkan vurnerability affects “https:sips.bawaslu.go.id/putusan/download.html, id”, apabila website tersebut sudah dijalankan otomatis intercept burp-suite akan menangkap HTTP request, intercept dapat menangkap http request dari

website tersebut, selanjutnya adalah mengirimkan http request tersebut ke repeater dengan cara mengklik kanan cursor lalu memilih menu send to repeater, nantinya hasil dari send to repeater. selanjutnya adalah memasukkan script path traversal ke parameter "id=", script yang digunakan untuk menemukan directory traversal adalah "../../../../../../../../../../etc/passwd", lalu masukkan script tersebut pada parameter "GET putusan/download.html?id="../../../../../../../../../../etc/passwd", kemudian send request, hasilnya adalah script tersebut dapat dijalankan dan menampilkan directory-directory username dan password pada website tersebut. Seperti pada gambar 3.20.

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time
Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network
Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd
Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus
Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
Debian-exim:x:105:109::/var/spool/exim4:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
sshd:x:107:65534::/run/sshd:/usr/sbin/nologin
sips:x:1000:1000:sips,,,:/home/sips:/bin/bash
mysql:x:108:112:MySQL Server,,,:/var/lib/mysql:/bin/false
ntp:x:109:113::/home/ntp:/bin/false
```

Gambar 3.20 Response Script

4. Conclusion

Dalam penelitian pengujian website sips.bawaslu.go.id menggunakan metode penetration testing dan Vulnerability scanner dengan tools OWASP ZAP dan Acunetix yang digunakan untuk menemukan celah keamanan dan bertujuan untuk meningkatkan keamananan pada sips.bawaslu.go.id setelah melakukan semua tahapan penelitian maka diambil beberapa kesimpulan yang dijelaskan sebagai berikut :

a. Dalam tools OWASP ZAP ditemukan beberapa celah keamanan yang dikategorikan high, medium, low, informational. Pada tools Acunetix ditemukan beberapa celah keaman dengan severity high, medium, low, informational.

b. Hasil pengujian yang dilakukan terdapat kesamaan jenis kerentanan pada owasp dan acunetix namun berbeda dalam penemaan kerentanan tersebut, contohnya seperti serangan directory traversal , dalam tools OWASP ZAP penamaan kerentanannya adalah directory

traversal, sedangkan dalam tools Acunetix penamaan directory traversal adalah path traversal. Kesamaan jenis kerentanan yang kedua adalah clickjacking, dalam tools OWASP AP kerentanan clickjacking terdapat pada bagian X-Frame Options Header Not Set, sedangkan pada Acunetix kerentanan clickjacking terdapat pada bagian Clickjacing : X-Frame Options Hedaer Missing.

c. Pada OWASP ZAP ditemukan kerentanan yaitu yaitu Path Traversal, pengujian pada path traversal berhasil dengan menggunakan script

d. "%2f..%2F..%2F..%2F..%2F..%2F..%2F..%2etc%2Fpasswd", dan kerentanan kedua yaitu format srring error, pengujian kerentanan format string error berhasil, hasilnya adalah database dapat menangkap parameter password yang berasal dari hasil ZAP Attack, yang ketiga adalah X-Frame Options Header Not Set yang terbukti dengan menggunakan tools sensepostjack, dan Vulnerable JS Library hal tersebut tidak berdampak pada kerahasiaan system, pada kerentanan ini hanya berisi rekomendasi agar versi moment.js di update ke versi yang terbaru untuk mencegah segala kemungkinan yang dapat membahayakan keamanan sistem. Selain terdapat kerentanan yang berhasil dibuktikan terdapat juga beberapa kerentanan yang tidak dapat dibuktikan, kerentanan tersebut adalah Absence Of Anti-CSRF Tokens, Cookie without secure flag, dan cookie without samesite attribute. Pada kerentanan Absence Of Anti-CSRF Tokens sudah menggunakan CSRF tokens, Cookie without secure flag sudah sudah menggunakan HttpOnly, dan cookie without samesite attribute sudah menggunakan attribute samesite dengan tipe "lax".

e. Pada tahapan attacking tools yang digunakan adalah Metasploit dan burpsuite. Tools Metasploit digunakan untuk membuktikan kerentanan TLS 1.0 enabled yang ditemukan berdasarkan vulnerability scanning menggunakan acunetix. Tools burpsuite digunakan dalam membuktikan kerentanan Cross-site scripting dan directory traversal.

f. Pada aplikasi acunetix terdeteksi beberapa kerentanan yaitu cross site scripting, directory traversal, TLS 1,0 enabled, Vulenrable JS Library, dan Clickjacking : X-Frame Options Headrer Missing. Pada kerentanan Cross-site scripting memiliki severity high, nampun pada saat pengujian serangan cross-site scripting pada tahapan attacking, serangan tersebut gagal. Kerentanan yang kedua yaotu directory traversal dengan severity high, serangan directory traversal dapat mengungkap script termasuk file yang dapat diakses untuk membaca informasi sensitive yang berisi username dan password. Kerentanan yang ketiga adalah TLS 1.0 Enabled, TLS 1.0 tidak dianggap sebagai "kriptografi kuat" seperti yang didefinisikan dan diwajibkan oleh Standar Keamanan Data PCI 3.2. ketika digunakan untuk melindungi informasi sensitif yang ditransfer ke atau dari situs web. Menurut PCI, "30 Juni 2018 adalah batas waktu untuk menonaktifkan SSL/TLS awal dan menerapkan protokol enkripsi yang lebih aman. Kerentanan yang keempat adalah clickcjacking : X-Frame Options Hedaer Missing dengan severity low, namun kerentanan ini berhasil, pembuktiannya terdapat pada tahapan attacking dengan menggunakan script Iframe . kerentanan yang keempat adalah Vulnerable JS library, kerentanan ini tidak berdampak pada system website, kerentanan ini hanya beirisi pembaharuan terhadap library Javascript.

References

[1] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," J. Algoritm., vol. 18, no. 1, pp. 77–86, 2021, doi: 10.33364/algoritma/v.18-1.827.

[2] G. Guntoro, L. Costaner, and M. Musfawati, "Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning)," JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform., vol. 5, no. 1, p. 45, 2020, doi: 10.29100/jipi.v5i1.1565.

[3] A. W. Kuncoro and F. Rahma, "Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review," Automata, vol. 3, no. 1, pp. 1–5, 2021, [Online]. Available: https://www.sciencedirect.com

[4] D. Hariyadi and F. E. Nastiti, "Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta," J. Komtika (Komputasi dan Inform., vol. 5, no. 1, pp. 35–42, 2021, doi: 10.31603/komtika.v5i1.5134.

[5] dan S. A. M. Agus Rochman, Rizal Rohian Salam, "ANALISIS KEAMANAN WEBSITE DENGAN INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK (ISSAF) DAN OPEN WEB APPLICATION SECURITY PROJECT (OWASP) DI RUMAH SAKIT XYZ," vol. 2, no. 4, p. 6, 2021.

[6] E. Listartha, G. Arna, J. Saskara, D. Gede, and S. Santyadiputra, "Vulnerability Testing and Security Penetration on Prodi XYZ Thesis Management Web Applications," Sci. Comput. Sci. Informatics J., vol. 4, no. 2, pp. 1–14, 2021.

[7] B. Ghozali, K. Kusrini, and S. Sudarmawan, "Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating," Creat. Inf. Technol. J., vol. 4, no. 4, p. 264, 2019, doi: 10.24076/citec.2017v4i4.119.

[8] Y. Yudiana, A. Elanda, and R. L. Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP Top 10," CESS (Journal Comput. Eng. Syst. Sci., vol. 6, no. 2, p. 185, 2021, doi: 10.24114/cess.v6i2.24777.

[9] J. J. B. H. Yum Thurfah Afifa Rosaliah, "Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM," Senamika, vol. 2, no. September, pp. 752–761, 2021.

[10] A. Aliefyan, "Penetration Testing Untuk Mengetahui Kerentanan Keamanan Aplikasi Web Menggunakan Standar OWASP 10 pada domain Web Perusahaan Penetration Testing Untuk Mengetahui Kerentanan Keamanan Aplikasi Web," ResearchGate, no. July, 2020.

[11] M. Riasetiawan, A. Wisnuaji, D. Hariyadi, and T. Febrianto, "Pengembangan Aplikasi Information Gathering Menggunakan Metode Hybrid Scan Berbasis Graphical User Interface," Cyber Secur. dan Forensik Digit., vol. 4, no. 1, pp. 44–48, 2021, doi: 10.14421/csecurity.2021.4.1.2449.

[12] A. Zirwan, "Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner," J. Inf. dan Teknol., vol. 4, no. 1, pp. 70–75, 2022, doi: 10.37034/jidt.v4i1.190.

[13] A. Andria, "Forensik Digital Sistem Informasi Berbasis Web," JAMI J. Ahli Muda Indones., vol. 2, no. 2, pp. 33–44, 2021, doi: 10.46510/jami.v2i2.73.

ISSN 2086-8138 (print) | 2745-7249 (online)
Jurnal Informatika
Vol. 1., No. 1, April 2020, pp. 1-8