Jurnal Informatika: Jurnal pengembangan IT

Vol. xx, No. x, Bulan 20xx
ISSN : 2477-5126, DOI:10.30591/jpit.v9ix.xxx

ANALISIS TINGKAT KEAMANAN WEBSITE PPDB SMK MUHAMMADIYAH GAMPING MENGGUNAKAN METODE PENETRATION TESTING EXECUTION STANDARD (PTES)

Dicky Rizky Pangestu [1], Eko Aribowo [2]

Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Yogyakarta
Kragilan, Tamanan, Banguntapan, Bantul, Yogyakarta 55191, Indonesia

Info Artikel

Riwayat Artikel:

Received month dd, yyyy
Revised month dd, yyyy
Accepted month dd, yyyy

Abstract – *The security of the website is something that needs to be considered in the creation of a website. This also applies to SMK Muhammadiyah Gamping, which has a website to manage new student registration online called the PPDB website of SMK Muhammadiyah Gamping. Because of this, it is necessary to carry out security testing on the website with the aim of testing the level of security and finding vulnerabilities from the security contained in the PPDB website of SMK Muhammadiyah Gamping, as well as providing recommendations for improvements to the gaps found. In this research, the method used is penetration testing execution standard (PTES) which is carried out to find system vulnerabilities in the Open Web Application Security Project (OWASP TOP 10) vulnerability list. This research uses several supporting applications, namely, OWASP Zed Attack Proxy (OWASP-ZAP) and Wapiti which are used to perform vulnerability scanning and the Burp Suite application which is used to perform penetration testing on the gaps found by the OWASP-ZAP and Wapiti applications. This research will get results in the form of vulnerability findings from the PPDB website of SMK Muhammadiyah Gamping along with the level of vulnerability and the corrective steps that can be taken to fix the vulnerabilities found in this research.*

Keywords: *OWASP TOP 10 2021, Penetration testing, PTES, Website, Website Security*

Corresponding Author:

Suttichai Premrudeeprechacharn

Email: suttichai@mail.com

Abstrak – *Keamanan dari website merupakan hal yang perlu diperhatikan dalam pembuatan dari sebuah website. Hal ini juga berlaku bagi SMK Muhammadiyah Gamping yang mempunyai salah satu website untuk memanajemen pendaftaran siswa baru secara daring yang bernama website PPDB SMK Muhammadiyah Gamping. Oleh karena hal tersebut perlu dilaksanakannya pengujian keamanan pada website tersebut dengan tujuan untuk menguji tingkat keamanan dan menemukan kerentanan dari keamanan yang terdapat pada website PPDB SMK Muhammadiyah Gamping , serta memberikan rekomendasi perbaikan pada celah yang ditemukan. Pada penelitian ini metode yang digunakan adalah penetration testing execution standard (PTES) yang dilakukan guna menemukan kerentanan sistem pada 10 daftar kerentanan Open Web Application Security Project (OWASP TOP 10), Penelitian ini menggunakan beberapa aplikasi pendukung yaitu, OWASP Zed Attack Proxy (OWASP-ZAP) dan Wapiti yang digunakan untuk melakukan vulnerability scanning dan aplikasi Burp Suite yang digunakan untuk melakukan penetration testing pada celah yang ditemukan oleh aplikasi OWASP-ZAP dan Wapiti. Penelitian ini akan mendapati hasil berupa temuan kerentanan dari website PPDB SMK Muhammadiyah Gamping beserta tingkat kerentanannya beserta Langkah perbaikan yang dapat dilakukan untuk memperbaiki kerentanan yang ditemukan dalam penelitian ini.*

Kata Kunci*: Keamanan Website, Penetration testing, PTES, OWASP TOP 10 2021, Website*

I. PENDAHULUAN

Dalam beberapa dekade ini lajunya perkembangan teknologi telah membawa perubahan mendalam dalam cara kita hidup, bekerja, dan berinteraksi. Transformasi yang sangat cepat dalam teknologi informasi, komunikasi, dan ilmu pengetahuan telah menciptakan peluang besar dan tantangan seiring perkembangan zaman. Salah satu contoh perkembangan tekonologi dalam bidang penyampaian informasi adalah dengan terciptanya sebuah website. Website atau laman memiliki definisi sebuah kumpulan halaman yang berfungsi untuk menyajikan informasi yang bisa berupa teks, gambar, animasi, media, atau kombinasi dari semuanya, baik dalam bentuk statis maupun dinamis, yang membentuk sistem terkait satu sama lain[1]. Seiring dengan perkembangan zaman penggunaan website tidak hanya digunakan hanya untuk penyampaian informasi saja, karena website juga banyak digunakan untuk pengelolaan sistem suatu lembaga atau organisasi[2]. Oleh karena hal tersebut dalam pembuatan website untuk sebuah sistem suatu lembaga keamanan dari sistem tersebut perlu diperhatikan [3].

Meningkatkan keamanan dari sebuah sistem website adalah upaya yang digunakan untuk memastikan bahwa sistem website tidak mempunyai celah, kerentanan dan risiko untuk diserang oleh para penyerang yang dapat merugikan suatu organisasi atau perusahaan[3]. Semakin tinggi keamanan dari suatu website maka semakin tinggi juga keamanan

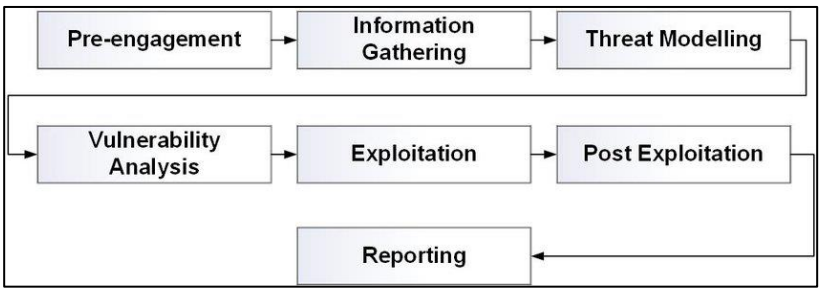
dari informasi yang ada pada sistem website tersebut [4]. Dengan semakin tingginya keamanan dari suatu website maka website tersebut tentu akan lebih aman dari serangan yang sering terjadi pada sistem suatu website. Namun saat ini masih ada pengembang atau pemilik suatu sistem website yang masih mengabaikan keamanan website tersebut[5].

Keamanan dari website PPDB SMK Muhammadiyah Gamping menjadi hal yang perlu diperhatikan. Karena pada website PPDB SMK Muhammadiyah Gamping terdapat risiko celah keamanan pada sistem website tersebut, oleh karena hal tersebut perlu dilakukannya analisis keamanan pada website PPDB SMK Muhammadiyah Gamping guna menemukan celah keamanannya. Ada 2 teknik yang bisa digunakan untuk menemukan kerentanan keamanan sistem pada sebuah website, adapun 2 teknik tersebut ialah vulnerabillity assessment dan penetration testing[3] . Vulnerabillity assessment adalah sebuah teknik mencari celah keamanan website melalui proses scanning sistem untuk menemukan celah keamanan dari suatu website dan melakukan peninjauan terhadap kerentanan yang ditemukan, sedangkan penetration testing merupakan analisis keamanan suatu sistem dengan mensimulasikan serangan terkontrol guna mengidentifikasi kerentanan terhadap sistem yang sudah ada[6].

Penelitian ini akan melakukan pengujian pada website PPDB SMK Muhammadiyah Gamping dengan melakukan vulnerability assessment dan penetration testing pada website guna menemukan celah keamanan sistem website dan melakukan analisis terhadap celah yang ditemukan serta melakukan perbaikan pada kerentanan pada keamanan sistem yang ditemukan. Selain itu, pada penelitian ini menggunakan metode penetration testing execution standard untuk menguji keamanan dari website PPDB SMK Muhammadiyah Gamping terhadap kerentanan Open Web Application Security Project (OWASP) 2021. Penelitian ini juga menggunakan alat bantu seperti OWASP ZAP, Acunetix yang digunakan untuk melakukan vulnerability assessment dan Burp Suite yang digunakan untuk melakukan penetration testing[8]. Diharapkan pada penelitian ini dapat memberikan hasil berupa temuan celah keamanan pada website website PPDB SMK Muhammadiyah Gamping serta memberikan rekomendasi perbaikan terhadap celah yang ditemukan untuk meningkatkan keamanan website tersebut.

II. METODE

Metode yang digunakan pada penelitian ini adalah metode *Penetration Testing Execution Standard* (PTES). Dalam melakukan penetration testing menggunakan metode PTES, langkah awal yang harus dilakukan adalah melakukan komunikasi awal dengan memaparkan alasan dilakukannya pengujian penetration testing, pengumpulan informasi, pembuatan resiko keamanan dan pengujian dibalik layar [7]. Adapun tahapan dari metode PTES dapat dilihat pada Gambar 3.1.



Gambar. 1 Tahapan Metode PTES

III. HASIL DAN PEMBAHASAN

A. *Pre-engagement*

Pada tahap pre-engagment dilakukan perencanaan dan menentukan target pengujian serta melakukan perizinan kepada pihak SMK Muhammadiyah Gamping untuk melakukan pengujian keamanan pada website PPDB SMK Muhammadiyah Gamping. Adapun hasil dari tahap ini adalah pada Tabel 1 berikut.

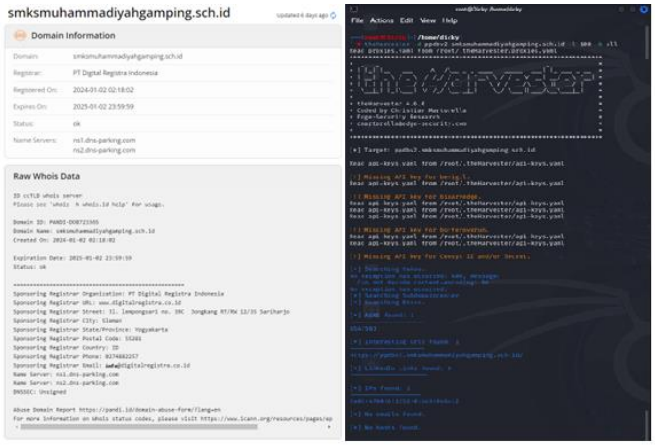
Tabel. 1
HASIL PRE-ENGAGMENT

Kegiatan	Status	Hasil
Penyampaian Target Pengujian	Terlaksana	Mendapatkan target pengujian penelitian yaitu *website* PPDB SMK Muhammadiyah Gamping

Penyampaian Tujuan Pengujian	Terlaksana	Tersampaikannya tujuan pengujian penelitian yaitu mencari kerentanan sistem pada *website* PPDB SMK Muhammadiyah Gamping dan memberikan rekomendasi perbaikan
Analisis Kesiapan Organisasi	Terlaksana	Kesiapan dari SMK Muhammadiyah Gamping dalam hal keamanan *website* masih terbilang rendah karena belum adanya programmer tetap yang mengelola *website* PPDB SMK Muhammadiyah Gamping
Menyusun *Roles Of Engagment* (ROS)	Terlaksana	Timeline penelitian dilaksanakan secara 1 bulan Pengujian dilaksanakan secara *online* pada cloning *website* PPDB SMK Muhammadiyah Gamping agar tidak mengganggu kinerja *website* PPDB SMK Muhammadiyah Gamping Penyampaian metode serta alat uji penelitian pada pihak SMK Muhammadiyah Gamping Pengajuan surat rekomendasi penelitian pada SMK Muhammadiyah Gamping
Menyusun Jalur Komunikasi	Terlaksana	Mendapatkan kontak staff admin *website* PPDB SMK Muhammadiyah Gamping

B. Information Gathering

Pada tahap information gathering dilakukan pengumpulan data yang dapat membantu dalam menemukan celah keamanan pada website PPDB SMK Muhammadiyah Gamping [9]. Pada tahap ini pengumpulan data dilakukan menggunakan aplikasi Whois dan TheHarvester untuk mengumpulkan informasi mengenai website PPDB SMK Muhammadiyah Gamping, hasil dari information gathering dapat dilihat pada Gambar 2.



Gambar. 2 Hasil Information Gathering

C. Threat Modeling

Tahap *Threat Modeling* adalah tahap untuk menentukan kerentanan yang ada pada *website* PPDB SMK Muhammadiyah Gamping. Pada tahap ini peneliti akan melakukan *scanning* kerentanan atau *vulnerability scanning* pada *website* target guna menemukan kerentanan yang ada pada *website* PPDB SMK Muhammadiyah Gamping. Hasil dari tahap ini dapat dilihat pada Tabel II berikut ini.

Tabel. I
HASIL THREAT MODELING

NO	Jenis Kerentanan	Tingkat risiko kerentanan	Jumlah
1	*Absence of Anti-CSRF Tokens*	Medium	7
2	*CSP: Wildcard Directive*	Medium	22
3	*CSP: script-src unsafe-inline*	Medium	22
4	*CSP: style-src unsafe-inline*	Medium	22
5	*Missing Anti-clickjacking Header*	Medium	22
6	*Vulnerable JS Library*	Medium	4
7	*Cookie without SameSite Attribute*	Low	13
8	*Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)*	Low	22
9	*Strict-Transport-Security Header Not Set*	Low	66
10	*X-Content-Type-Options Header Missing*	Low	66
11	*Backup Files*	Low	68

D. Vulnerability Assessment

Tahap vulnerability Assessment merupakan tahap untuk mengidentifikasi kerentanan yang ditemukan pada tahap threat modeling. Pada tahap ini akan mengidentifikasi temuan celah yang ditemukan pada saat melakukan vulnerability scanning apakah kerentanan tersebut termasuk dari kerentanan pada daftar OWASP TOP 10 2021 atau tidak. Untuk hasil identifikasi kerentanan dapat dilihat pada Tabel 3.

Tabel. 3
HASIL VULNERABILITY ASSESMENT

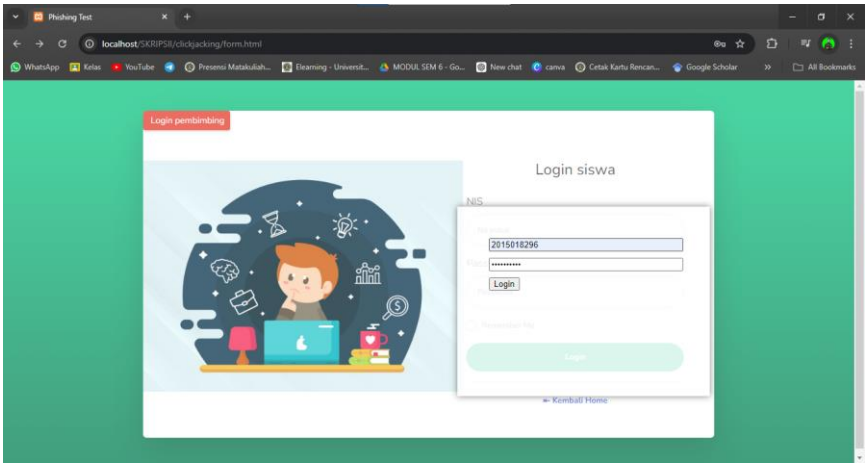
NO	Jenis Kerentanan	Tingkat risiko kerentanan	Kategori OWASP Top 10 2021	Jumlah
1	Absence of Anti-CSRF Tokens	Medium	A01:2021 - Broken Access Control	7
2	CSP: Wildcard Directive	Medium	A05:2021 - Security Misconfiguration	22
3	CSP: script-src unsafe-inline	Medium	A05:2021 - Security Misconfiguration	22
4	CSP: style-src unsafe-inline	Medium	A05:2021 - Security Misconfiguration	22
5	Missing Anti-clickjacking Header	Medium	A05:2021 - Security Misconfiguration	22
6	Vulnerable JS Library	Medium	A06:2021 – Vulnerable and Outdated Components	4
7	Cookie without SameSite Attribute	Low	A07:2021-Identification and Authentication Failures	13
8	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	A05:2021 - Security Misconfiguration	22
9	Strict-Transport-Security Header Not Set	Low	A06:2021 - Vulnerable and Outdated Components	66
10	X-Content-Type-Options Header Missing	Low	A05:2021 - Security Misconfiguration	66
11	Backupfile	Low	A01:2021 - Broken Access Control	68

E. Exploitation

Tahap exploitation adalah tahap untuk melakukan penetration testing terhadap kerentanan yang ditemukan pada tahap vulnerability assessment. Tahap exploitation ini berfokus untuk menguji apakah kerentanan yang ditemukan dapat menjadi celah keamanan untuk menyerang sistem website PPDB SMK Muhammadiyah Gamping, adapun celah yang dapat diekslpoitasi adalah sebagai berikut.

- Missing Anti-clickjacking header

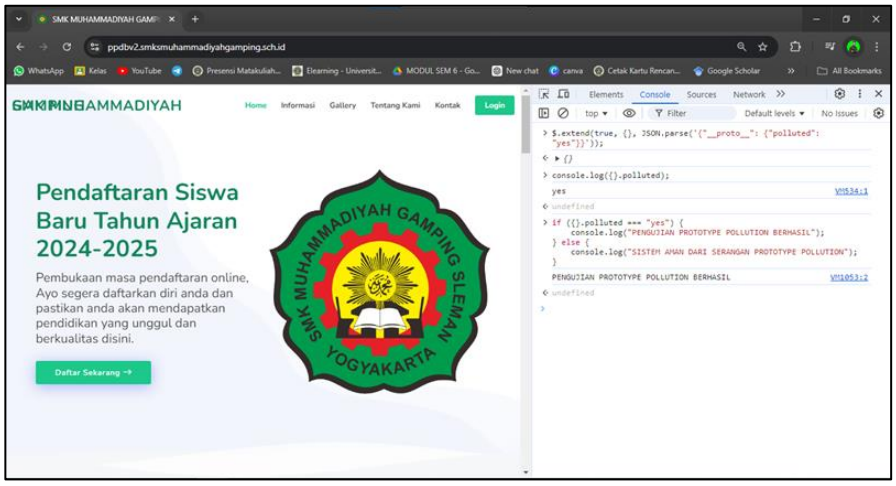
  Kerentanan Missing Anti-Clickjacking Header merupakan kerentanan dari sebuah sistem web yang tidak bisa melindungi sebuah website dari serangan clickjacking[10]. Serangan clickjacking sendiri merupakan sebuah serangan yang menargetkan kepada user dari suatu website untuk mengakses website palsu yang memiliki tampilan seperti website yang asli [11]. Untuk mengeksploitasi kerentanan ini adalah dengan memasukan tampilan dari suatu halaman website menggunakan fungsi iframe. Hasil dari eksploitasi terhadap celah ini dapat dilihat pada Gambar 3.



Gambar. 3 Hasil Eksploitasi Clickjacking

- Vulnerable JS Library

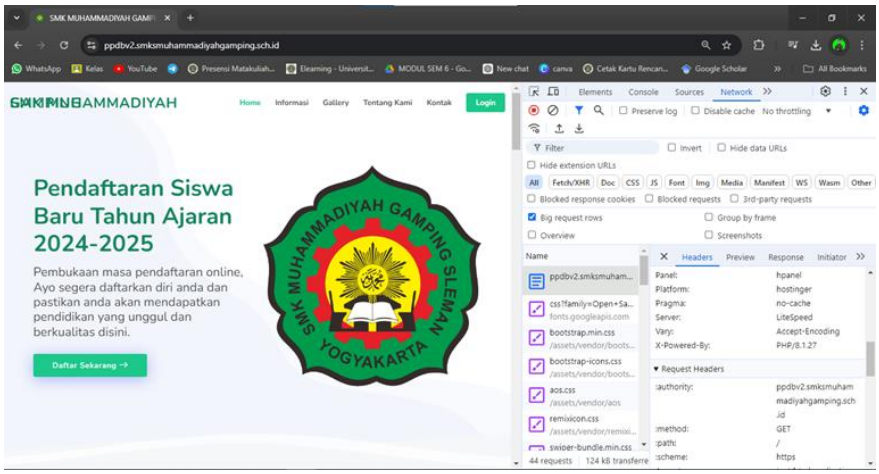
Kerentanan Vulnerable JS Library merupakan salah satu kerentanan yang terjadi dikarenakan sistem menggunakan library JavaScript yang sudah using atau lama[10]. Kerentanan ini dapat dimanfaat untuk melakukan berbagai serangan seperti Cross-Site Scripting (XSS) dan Remote Code Transfersal (RCT) tergantung pada jenis library JavaScript yang usang[11]. Pengujian terhadap celah ini dilakukan dengan mengggunakan serangan *Prototype Polution* dengan memodifikasi objek prototype dengan mengubah objek prototipe dan menambahkan properti "polluted" dengan nilai "yes". Hasil dari serangan ini dapat dilihat pada Gambar 4.



Gambar. 4 Hasil Pengujian Vulnerable JS Library

- Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

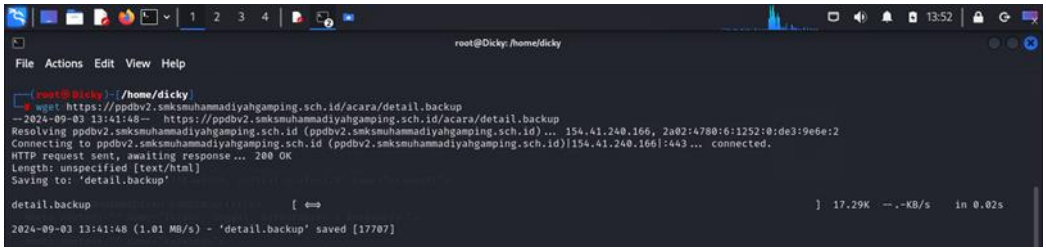
Kerentanan Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) terdeteksi apabila header membocorkan terlalu banyak informasi dari sistem website tersebut[10]. Kerentanan ini dapat dimanfaatkan oleh penyerang untuk mencari kelemahan dari sistem backend dari website tersebut untuk mencari fingerprint guna melakukan serangan ke website target[12]. Hasil pengujian dari kerentanan ini dapat dilihat pada Gambar 5.



Gambar. 5 Hasil Pengujian Kerentanan X-Powered-By

- Backup File

Kerentanan Backup File terdeteksi apabila sebuah sistem terdapat file yang tidak ditampilkan dalam website namun file tersebut dapat diakses menggunakan perintah tertentu[10]. File yang dapat diakses ini dapat dimanfaatkan guna mencari informasi terhadap sistem file maupun informasi penting yang seharusnya tidak diperlihatkan oleh website tersebut[13].



Gambar. 6 Pengujian Kerentanan Backup File

F. Post-Exploitation

Tahap post-exploitation merupakan tahap untuk memberikan hasil eksploitasi pada tiap celah yang ditemukan dan sudah diuji dan memberikan dampak dari kerentanan tersebut. Hasil dari tahap post-exploitation dilaporkan berdasarkan temuan celah keamanan pada tahap threat modeling dan hasil pengujian pada tahap exploitasi[14]. Hasil dari tahap post-exploitation dapat dilihat pada Tabel 4.

Tabel. 4
HASIL POST-EXPLOITATION

NO	Jenis Kerentanan	Metode Eksploitasi	Hasil Eksploitasi	Dampak Eksploitasi
1	Absence of Anti-CSRF Tokens	Menggunakan Script untuk mengubah nis dan password dari akun korban	Tidak Berhasil	Tidak berdampak karena pengujian gagal
2	CSP: Wildcard Directive	Melakukan request terhadap website menggunakan protokol HTTP	Tidak Berhasil	Tidak berdampak karena website dapat mengubah request http menjadi HTTPS.
3	CSP: script-src unsafe-inline	Menggunakan serangan XSS dengan memasukan script pada URL	Tidak Berhasil	Tidak berdampak karena website memvalidasi karakter pada URLnya.
4	CSP: style-src unsafe-inline	Melakukan modifikasi pada elemen website yang memiliki atribut CSS menggunakan script.	Tidak Berhasil	Tidak berdampak karena script yang dieksekusi tidak bisa mengubah tampilan elemen target
5	Missing Anti-clickjacking Header	Menggunakan script “iframe” untuk memuat tampilan halaman login website untuk melakukan serangan phising	Berhasil	Halaman login dapat dimuat dan dimanipulasi menjadi situs phising untuk mendapatkan data akun pengguna
6	Vulnerable JS Library	Melakukan serangan polluted property pada library jquery-3.3.1.min.js	Berhasil	Mengubah nilai dari objek property dengan nilai yang dibuat berdasarkan script.
7	Cookie without SameSite Attribute	Melakukan serangan CSRF dengan memanfaatkan session cookie	Tidak Berhasil	Tidak berdampak karena script CSRF tidak berhasiil mengubah data dengan memanfaatkan session cookie

8	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Melakukan fingerprint untuk mengetahui versi sistem backend dengan memanfaatkan header X-Powered-By	Berhasil	Mendapatkan fingerprint berupa versi PHP yang digunakan dalam membangun website PPDB SMK Muhammadiyah Gamping
9	Strict-Transport-Security Header Not Set	Melakukan request terhadap website menggunakan protokol HTTP	Tidak Berhasil	Tidak berdampak karena website dapat mengubah request http menjadi HTTPS.
10	X-Content-Type-Options Header Missing	Menggunggah sebuah script ke server dengan memberikan format file ".txt" untuk dijalankan pada URL	Tidak Berhasil	Tidak berdampak karena website tidak mengeksekusi isi file saat dibuka menggunakan URL
11	Backupfile	Mengunduh file backup yang tertinggal dan menganalisis isi file	Berhasil	File berisi source code dari page tersebut dan dapat digunakan untuk mencari fingerprint dari website.

G. Reporting

Tahap reporting adalah tahap terakhir dari metode Penetration testing Execution Standard. Tahap reporting adalah tahap untuk melaporkan hasil temuan celah yang berhasil dieksploitasi dan memberikan rekomendasi perbaikan serta langkah perbaikannya[15]. Adapun hasil reporting dari pengujian dapat dilihat pada Tabel 5.

Tabel. 5
HASIL REPORTING

NO	Jenis Kerentanan	Deskripsi Kerentanan	Dampak Kerentanan	Rekomendasi Perbaikan
1	Missing Anti-clickjacking Header	Header anti-clickjacking seperti X-Frame-Options tidak diatur, memungkinkan aplikasi web di-"frame" dalam situs lain. Ini membuat aplikasi rentan terhadap serangan clickjacking.	Penyerang dapat menggunakan teknik clickjacking untuk memanipulasi pengguna agar melakukan tindakan berbahaya tanpa disadari.	- Tambahkan header X-Frame-Options: DENY atau SAMEORIGIN
2	Vulnerable JS Library	Aplikasi menggunakan *library* JavaScript yang rentan, yang telah teridentifikasi memiliki kelemahan keamanan pada versi yang sedang digunakan.	Penyerang dapat mengeksploitasi kerentanan dalam pustaka untuk menjalankan serangan XSS, RCE (Remote Code Execution), atau manipulasi lainnya.	- Update pustaka JavaScript ke versi terbaru yang aman
3	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Server mengungkapkan informasi tentang teknologi atau	Penyerang dapat menggunakan informasi ini untuk melakukan serangan	- Nonaktifkan header X-Powered-By pada

		platform yang digunakan melalui header HTTP X-Powered-By. Ini memberikan informasi tambahan kepada penyerang tentang potensi target.	yang lebih spesifik berdasarkan platform atau versi perangkat lunak yang digunakan.	konfigurasi server web
4	Backupfile	File cadangan atau file konfigurasi yang sensitif ditemukan di direktori web dan dapat diakses oleh publik. File ini sering mengandung informasi penting seperti konfigurasi sistem atau data pengguna.	Penyerang dapat mengunduh file tersebut untuk mendapatkan informasi sensitif, seperti kredensial, konfigurasi, atau kode sumber, yang dapat digunakan untuk serangan lebih lanjut.	- Hapus file cadangan dari direktori web

IV. SIMPULAN

Setelah dilakukan pemindaian dan pengujian kerentanan pada website PPDB SMK Muhammadiyah Gamping terhadap kerentanan OWASP TOP 10 2021 didapati hasil bahwa website PPDB SMK Muhammadiyah Gamping celah kerentanan yang dapat dieksploitasi. Pada tahap vulnerability scanning didapati bahwa website PPDB SMK Muhammadiyah Gamping memiliki 11 kerentanan dengan tingkat medium dan low, kerentanan tersebut adalah Absence of Anti-CSRF Tokens, CSP: Wildcard Directive, CSP: script-src unsafe-inline, CSP: style-src unsafe-inline, Missing Anti-clickjacking Header, Jenis Kerentanan, Vulnerable JS Library, Cookie without SameSite Attribute, Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s), Strict-Transport-Security Header Not Set dan X-Content-Type-Options Header Missing dan Backup file. Setelah dilakukan pengujian terhadap kerentanan tersebut didapati bahwa kerentanan Missing Anti-clickjacking Header, Vulnerable JS Library dan Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) dan Backupfile dapat dimanfaatkan untuk melakukan penyerangan terhadap website. Kemudian diberikan rekomendasi perbaikan terhadap kerentanan tersebut dengan tujuan untuk menutup celah yang ada agar tidak ada yang menyalahgunakan kerentanan tersebut.

Untuk penelitian selanjutnya diharpakan peneliti menggunakan metode berbeda dan aplikasi pengujian berbeda guna mendapatkan hasil yang lebih maksimal. Kemudian perlu dilakukannya perbaikan pada sistem keamanan website PPDB SMK Muhammadiyah Gamping terhadap kerentanan yang ditemukan pada penelitian ini agar keamanan dari website dapat lebih ditingkatkan

UCAPAN TERIMAKASIH

Terimakasih kepada Universitas Ahmad Dahlan, Dosen Pembimbing dan teman teman yang telah mendukung dan membimbing dalam penelitian ini. Serta orangtua dan keluarga yang selalu memberikan semangat dan do'a sampai menyelesaikan penelitian ini..

DAFTAR PUSTAKA

[1] A. Keamanan Website and B. Cut, "Analisa Keamanan Website Terhadap Serangan Cross-Site Request Forgery (CSRF)," Kandidat : Jurnal Riset dan Inovasi Pendidikan, vol. 1, pp. 21–29, Oct. 2019, [Online]. Available: http://jurnal.abulyatama.ac.id/index.php/kandidat

[2] I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," Jurnal Informasi dan Teknologi, vol. 4, pp. 160–165, Oct. 2022, doi: 10.37034/jidt.v4i3.236.

[3] G. Ary, S. Sanjaya, G. Made, A. Sasmita, D. Made, and S. Arsa, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," Aug. 2020.

[4] S. Utoro et al., "Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard," Dec. 2020.

[5] Y. Thurfah Afifa Rosaliah and B. Hananto, Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM xxx. 2021.

[6] A. I. Rafeli, H. B. Seta, and W. Widi, "Pengujian Celah Keamanan Menggunakan Metode OWASP Web Security Testing Guide (WSTG) pada Website XYZ," JURNAL INFORMATIK, vol. 18, Aug. 2022.

[7] A. Rochman, R. Rohian Salam, dan Sandi Agus Maulana Sekolah Tinggi Manajemen Ilmu Komputer, and S. Likmi, "DI RUMAH SAKIT XYZ," ANALISIS KEAMANAN WEBSITE DENGAN INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK (ISSAF) DAN OPEN WEB APPLICATION SECURITY PROJECT, vol. 2, no. 4, 2021.

[8] T. Ariyadi, T. Langgeng Widodo, N. Apriyanti, and F. Sasti Kirana, "Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP Analysis of Bina Darma University Academic Information System Security Vulnerabilities Using the OWASP," May 2023.
[9] A. Zirwan, "Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner," Jurnal Informasi dan Teknologi, pp. 70–75, Mar. 2022, doi: 10.37034/jidt.v4i1.190.
[10] A. F. Hasibuan, Tommy, and Handoko DIvi, "Analisis Keretanan Website Dengan Aplikasi Owasp Zap," Jurnal Ilmu Komputer dan Sistem Informasi (JIRSI), vol. 2, May 2023.
[11] M. Yaqi, "Vulnerability Assessment dan Penetration Testing (Vapt) Menggunakan Metode Zero Entry Hacking (Zeh) Terhadap Website Studi Kasus: Dinas Penanaman Modal Dan Ptsp Kota Tangerang Selatan," Aug. 2023.
[12] A. Dharmawan, Y. Prihati, and H. Listijo, "PENETRATION TESTING MENGGUNAKAN OWASP TOP 10 PADA DOMAIN XYZ.AC.ID," Jurnal Elektro Luceat, vol. 8, Jul. 2022.10.47709/digitech.v3i2.2855.
[13] A. Fatihah and P. Dinarto, "Analisis Keamanan Aplikasi Website Menggunakan Metode Penetration Testing Berdasarkan Framework ISSAF Pada Perusahaan Daerah XYZ," INNOVATIVE: Journal Of Social Science Research, vol. 4, pp. 4536–4549, 2024.
[14] M. Hasibuan and A. M. Elhanafi, "Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box," sudo Jurnal Teknik Informatika, vol. 1, no. 4, pp. 171–177, Dec. 2022, doi: 10.56211/sudo.v1i4.160.
[15] C. D. Ihrom, "Analisis Keamanan Website Ppdb Online SMK Nuurul Bayan Kalapanunggal Menggunakan Metode Penetration Testing Dan Vulnerability Assessment," 2024.