Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 7 Nomor 2, September 2023, pp. 753-764
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Analisis Security Mitigation dengan Metode Vulnerability Assesment and Penetration Testing (VAPT) (Kasus Website Kerja Praktek dan Pengabdian Masyarakat)

Muhammad Iqbal Fadillah[1], Umar Yunan Kurnia Septi Yanto[2], Muhammad Fathinuddin[3]
[1,2,3]Universitas Telkom, Indonesia
e-mail: iqbalfadillah@student.telkomuniversity.ac.id[1], umaryunan@telkomuniversity.ac.id[2], muhammadfathinuddin@telkomuniversity.ac.id[3]

Abstract

The current development of technology is progressing rapidly in line with the ease of accessing information through various means, whether through mobile applications or websites. This convenience has had a significant impact on various industries, governments, and educational institutions that utilize websites as information support for learning and teaching activities, including at XYZ Faculty. The website is used to manage student activities in Internship and Community Service (ICS). In previous research, vulnerability assessment was conducted to identify vulnerabilities on the website; however, no mitigation was implemented for the vulnerabilities found. Therefore, security mitigation is needed to address the risks associated with these vulnerabilities. The method used in this process is Vulnerability Assessment and Penetration Testing (VAPT) with gray box testing techniques, as well as the tools Burp Suite, Acunetix, and Nessus. Vulnerability analysis was performed on the identified vulnerabilities on the website to determine a list of vulnerabilities for further exploitation. Through testing on this ICS website, nine vulnerabilities were found, including one high-level vulnerability, four medium-level vulnerabilities, and four low-level vulnerabilities. These vulnerabilities were then mitigated, and the results showed that four out of the nine vulnerabilities were successfully mitigated, improving the website's security compared to before.

Keywords*: Vulnerability, VAPT, exploitation, website, mitigation.*

Abstrak

Perkembangan dunia teknologi saat ini semakin pesat seiring dengan kemudahan akses informasi melalui berbagai cara baik melalui aplikasi berbasis mobile ataupun website. Kemudahan tersebut memberikan dampak yang cukup luas terhadap berbagai kegiatan industri, pemerintahan hingga institusi pendidikan yang memanfaatkan teknologi website sebagai penunjang informasi bagi kegiatan belajar dan mengajar termasuk pada Fakultas XYZ. website tersebut digunakan untuk mengelola kegiatan mahasiswa dalam Kerja Praktek dan Pengabdian masyarakat (KPPM). Pada penelitian sebelumnya telah dilakukan vulnerability assessment untuk menemukan kerentanan pada website tersebut namun belum dilakukan mitigasi dari kerentanan yang ditemukan, oleh karena itu diperlukan security mitigation untuk mengatasi resiko dari kerentanan tersebut. Metode yang digunakan dalam proses ini yaitu Vulnerability Assesment and Penetration Testing (VAPT) dengan teknik gray box testing dan juga dengan tools Burp Suite, Acunetix dan Nessus. Celah kerentanan yang ditemukan pada website dilakukan analisis untuk menentukan daftar kerentanan untuk dilakukan eksploitasi lebih lanjut. Dari pengujian pada website KPPM ini ditemukan 9 kerentanan, diantaranya 1 kerentanan dengan tingkat high, 4 dengan tingkat medium dan 4 kerentanan dengan tingkat low. Kerentanan tersebut selanjutnya dilakukan mitigasi dan hasil mitigasi yang telah dilakukan menunjukan 4 dari 9 kerentanan berhasil di mitigasi dengan baik sehingga keamanan website menjadi lebih baik dari sebelumnya.

Kata kunci*: Kerentanan, VAPT, Eksploitasi, Website, Mitigasi.*

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 7 Nomor 2, September 2023, pp. 753-764
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

1. PENDAHULUAN

Seiring dengan adanya kemudahan akses informasi melalui berbagai cara. Adapun informasi tersebut pada awalnya adalah sekumpulan fakta yang memberikan suatu gambaran ataupun bukti dari persoalan yang kemudian dikelola agar dapat diterima oleh pengguna [1]. Informasi tentu diakses oleh banyak orang, maka keamanan dari informasi sangat penting agar hanya orang yang memiliki wewenang saja yang dapat mengakses data informasi tersebut. Jika data tersebut diakses oleh pihak yang tidak bertanggung jawab maka banyak pihak akan merasa dirugikan akan hal itu. Oleh karena itu keamanan informasi merupakan sesuatu hal yang harus dilindungi dari resiko serangan yang mungkin akan terjadi di masa yang akan datang [2].

Serangan pada *website* umumnya berdasarkan pada tiga aspek keamanan informasi tersebut, adapun serangan yang sering dilakukan untuk mengeksploitasi data pengguna yaitu serangan *Man in The Middle Attack* (MITM), *Denial of Services* (DOS), dan *SQL Injection*. Oleh karena itu diperlukan solusi untuk mengantisipasi serangan yang terjadi dengan dilakukannya *Security Testing* pada *website* sehingga dari pengujian tersebut dapat ditemukan kerentanan pada *website* lalu melakukan analisis untuk menentukan rekomendasi mitigasi kerentanan yang ditemukan agar dapat menutup celah keamanan sebagai bentuk mitigasi dan penanganan insiden dari serangan yang mungkin terjadi kedepannya.

Website Kerja Praktek dan Pengabdian Masyarakat merupakan salah satu *website* administrasi pada fakultas XYZ dimana portal ini berfungsi untuk mengelola data mahasiswa yang melakukan kegiatan kerja praktek maupun pengabdian masyarakat. Dengan adanya portal ini mahasiswa dan dosen menjadi lebih mudah dalam memilih topik, mencatat *logbook,* mengunggah laporan kegiatan serta memantau kemajuan penilaian kegiatan kerja praktek atau pengabdian masyarakat. Portal ini dibangun dengan *framework* sails.js yang berbasis bahasa javascript dan berjalan pada *Virtual Private Server* (VPS) milik fakultas xyz. Pada penelitian yang telah dilakukan sebelumnya telah dilakukan pengujian untuk menemukan kerentanan yang ada pada *website* ini namun kerentanan tersebut belum dilakukan mitigasi lebih lanjut sehingga diperlukan *security testing* kembali untuk menemukan kerentanan lebih mendalam dan rekomendasi mitigasi agar mengamankan data pengguna serta mengurangi resiko adanya serangan yang mengancam sistem *website*. Penelitian ini menerapkan teknik *penetration testing* dengan *grey box testing* yaitu penguji mengetahui sebagian informasi dari infrastruktur jaringan atau aplikasi yang akan diuji [3]. Untuk membantu dalam menemukan kerentanan pada Kerja Praktek dan Pengabdian Masyarakat (KPPM) digunakan *tools* seperti Nmap, Maltego, Burp Suite, Nessus, dan Acunetix.

Berdasarkan permasalahan tersebut maka diperlukan solusi untuk mencegah dan mengamankan data mahasiswa serta dosen pada *website* Kerja Praktek dan Pengabdian Masyarakat di fakultas XYZ. *Security mitigation* adalah jawaban untuk permasalahan tersebut agar kerentanan dapat ditemukan lebih awal sehingga dapat dilakukan mitigasi untuk menutup celah keamanan yang ada dan menguji tingkat ketahanan keamanan pada *website* terhadap serangan dari kerentanan yang ditemukan.

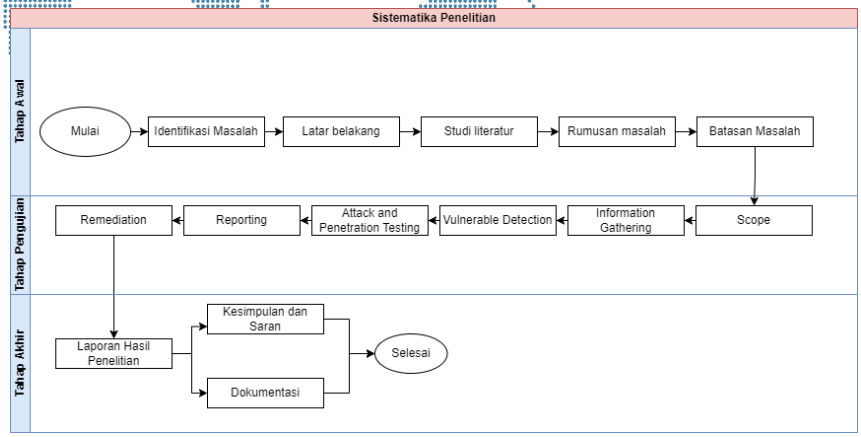
2. METODOLOGI PENELITIAN

2.1. Sistematika Penyelesaian Masalah

Sistematika penyelesaian masalah pada penelitian ini yaitu digambarkan dalam bentuk bagan proses yang terdiri dari tiga tahapan yang pertama tahap awal, lalu tahap pengujian dan tahap akhir. Dari tiga tahapan tersebut terdapat berbagai proses di

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 7 Nomor 2, September 2023, pp. 753-764
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

dalamnya. Adapun bagan sistematika penyelesaian masalah dapat dilihat pada gambar 2 berikut.



Gambar 1. Sistematika Penyelesaian Masalah

2.1.1. Tahap Awal

Pada tahap awal yang dilakukan pertama adalah identifikasi dan observasi masalah dari penelitian yang akan dilakukan. Setelah permasalahan didapatkan langkah selanjutnya adalah membuat latar belakang yang berlandaskan dari studi literatur yang ada. Studi literatur diperlukan sebagai dasar dalam mengumpulkan informasi-informasi terkait permasalahan penelitian yang akan dilakukan. Studi literatur dapat ditemukan melalui berbagai sumber penulisan seperti jurnal terdahulu dan buku. Setelah itu menentukan rumusan masalah serta batasan masalah untuk membatasi penelitian agar lebih terfokus pada permasalahan yang akan di teliti.

2.1.2. Tahap Pengujian

Pada tahap pengujian terdiri dari langkah-langkah metode yang diterapkan penelitian ini yang meliputi *scope* yaitu identifikasi dari target yang ingin diuji yang bertujuan untuk menentukan lingkup penelitian, metode serta tools yang akan digunakan. Setelah itu dilakukan *Information Gathering* yaitu informasi dari target dikumpulkan menggunakan bantuan *tools* seperti Nmap dan Maltego sehingga dapat menjadi acuan dalam menentukan objek target secara spesifik. Kemudian dari informasi yang di dapatkan selanjutnya adalah dengan melakukan *Vulnerable Detection* untuk menemukan kerentanan dari target dengan tools Burp suite, Nessus dan Acunetix. Setelah kerentanan tersebut ditemukan dilakukan klasifikasi tingkat keparahan kerentanan tersebut yang nantinya sebagai dasar penentuan untuk dilakukan eksploitasi. Langkah selanjutnya adalah attack and penetration dimana tujuan dari langkah ini untuk mendapatkan tingkat keparahan dan validitas dari kerentanan yang ditemukan sebelumnya.

Dari hasil eksploitasi yang telah didapatkan, langkah selanjutnya adalah melakukan *reporting* kepada pihak yang berwenang untuk melaporkan kerentanan yang ditemukan dan langkah remediasi yang dapat dilakukan untuk menutup kerentanan tersebut.

2.1.3. Tahap Akhir

Tahap ini adalah tahap menyimpulkan dan membuat laporan dari tahap awal hingga tahap pengujian. Pada tahap ini laporan dibuat setelah pengujian solusi yang dapat di implementasikan ke sistem untuk menutup celah keamanan yang ditemukan. Selain itu, pada laporan ini berisi spesifikasi sistem yang diuji secara rinci, kerentanan yang

ditemukan beserta tingkat resiko dari kerentanan tersebut dan saran untuk pengembangan sistem agar lebih baik kedepannya baik itu dari segi *software* ataupun *hardware* nya.

3. HASIL DAN PEMBAHASAN

3.1. *Scope*

Pada tahap awal ini menentukan teknik pengujian yang akan digunakan dan perancangan pengujian untuk mengetahui hasil kerentanan pada *website* yang ingin diuji. Pengujian ini menggunakan *automatic testing* yang dilakukan pada port 443 yaitu HTTPS dimana proses pengujian juga menggunakan beberapa tools yang membantu pengujian yaitu Burp suite, Acunetix dan Nessus. Selain itu pada pengujian ini akan menggunakan metode *grey box testing* yaitu proses pengujian dilakukan dengan mengetahui sebagian informasi mengenai kredensial untuk akun pada *website* dan juga konfigurasi atau *script* sebagai pendukung dalam melakukan pengujian. Pada proses pengujian celah keamanan dan analisis sebuah website dibutuhkan *hardware* dan *software* yang mendukung untuk berjalannya proses tersebut. Oleh karena itu dilakukan perancangan *hardware* dan *software* yang akan digunakan dalam proses pengujian dan analisis. Spesifikasi hardware dan software yang akan digunakan pada pengujian ini dapat dilihat pada Tabel 1 dan Tabel 2.

Tabel 1. Spesifikasi *Hardware* yang digunakan

Nama Komponen	**Informasi**	
Komputer Host	Processor	Intel(R) Core (TM) i5-8265U CPU @ 1.60GHz (8 CPUs), ~1.8GHz
	Memory	12 GB
	Storage	931.51GB
	System Type	64-bit
	Operating System	Windows 11 Home Single Language 64-bit (10.0, Build 22623)
Komputer Virtual	Processor	Intel(R) Core (TM) i5-8265U CPU @ 1.60GHz (8 CPUs), ~1.8GHz
	Memory	4 Core
	Storage	30 GB
	System Type	64-bit
	Operating System	Kali Linux 2023.1

Tabel 2. Spesifikasi *Software* yang digunakan

Perangkat	**Informasi**
Operating System	Kali Linux
Virtual Machine	VirtualBox
Scanning Tools	Nmap
Vulnerability Scanning and Analysis Tools	Maltego
	Burpsuite
	Nessus

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 7 Nomor 2, September 2023, pp. 753-764
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

3.2. *Information Gathering*

Pada tahap ini dilakukan pengumpulan informasi dari website yang akan diuji. Pengumpulan informasi ini akan menggunakan tools Nmap dan Maltego. Berikut hasil pengujian menggunakan *tools* tersebut dapat dilihat pada Tabel 3.

Tabel 3. Hasil *Information Gathering*

Spesifikasi	**Keterangan**
Nama Domain	kppm.virtualfri.id
IP Address	103.41.206.192
Port	22/OpenSSH,3307/MySQL, 3310/MySQL, 443/nginx, 80/nginx, 8001, 8080, 8084, 81/Apache httpd, 82/Apache httpd, 84/Apache httpd 85/Apache httpd
Operating System	Ubuntu

3.3. *Vulnerable Detection*

Vulnerability Detection adalah tahapan dimana melakukan pengujian terhadap suatu target untuk menemukan celah keamanan. Pada penelitian ini akan menggunakan *tools* Burp Suite, Nessus dan Acunetix untuk melakukan *vulnerability detection.*

3.3.1. Hasil *Scanning* dengan Burp Suite

Pengujian untuk analisis kerentanan yang ditemukan pada penelitian ini salah satunya menggunakan Burpsuite. Burp suite digunakan untuk menemukan kerentanan pada *website* Kerja Praktek dan Pengabdian Masyarakat (KPPM) pada URL "https://kppm.virtualfri.id/". Hasil kerentanan yang terdeteksi oleh Burp Suite dapat dilihat pada Tabel 4.

Tabel 4. Hasil Pengujian dengan Burp Suite

Vulnerability	**Severity, Confidence**
Vulnerable version of the library 'axios' found	High, Tentative
TLS certificate	Medium, Certain
Vulnerable version of the library 'bootstrap' found	Medium, Tentative
Vulnerable version of the library 'jquery' found	Medium, Tentative
Client-side JSON injection (DOM-based)	Low, Firm
Strict transport security not enforced	Low, Certain
Vulnerable JavaScript dependency	Low, Tentative
Source code disclosure	Low, Tentative
Email addresses disclosed	Information, Certain
Cacheable HTTPS response	Information, Certain
Vulnerable version of the library 'axios' found	High, Tentative
TLS certificate	Medium, Certain

3.3.2. Hasil *Scanning* dengan Nessus

Nessus merupakan salah satu tools yang digunakan dalam penelitian ini untuk menemukan kerentanan yang ada pada *website* Kerja Praktek dan Pengabdian Masyarakat ini. Pada pengujian ini target yang digunakan adalah IP Address 103.41.206.192 dimana IP ini merupakan IP yang di dapatkan melalui

proses Intelligence Gathering Sebelumnya dan pada port 443 yaitu *port* HTTPS yang digunakan *website* Kerja Praktek dan Pengabdian Masyarakat (KPPM). Langkah pengujian dengan Nessus dimulai dari menentukan target, lalu memilih jenis *scan* dan konfigurasi opsi yang akan dilakukan. Setelah itu hasil di dapatkan dan di analisis serta identifikasi berdasarkan kategori kerentanan yang ditemukan. Adapun hasil pengujian yang terdeteksi dijelaskan pada Tabel 5 berikut.

Tabel 5. Hasil Pengujian dengan Nessus

Vulnerability	Severity	Port
Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	Critical	81, 86, 85, 89
PHP Unsupported Version Detection	Critical	81, 82, 83, 84, 86, 85, 89, 90
Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF	Critical	85,89
Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow	Critical	85
JQuery 1.2 < 3.5.0 Multiple XSS	Medium	443
Web Application Potentially Vulnerable to Clickjacking	Medium	85, 88, 443
HSTS Missing from HTTPS Server (RFC 6797)	Medium	443
Web Server Transmits Cleartext Credentials	Low	85,88
Web Server Allows Password Auto-Completion	Low	443

3.3.3. Hasil *Scanning* dengan Acunetix

Acunetix merupakan salah satu perangkat lunak yang berfungsi dalam menganalisis dan memindai kerentanan pada suatu website ataupun jaringan. Acunetix pada penelitian ini digunakan sebagai tools untuk menemukan kerentanan pada *website* Kerja Praktek dan Pengabdian Masyarakat. Adapun Skenario pengujian yang pertama adalah menentukan target website. Selanjutnya adalah memilih profile test dimana pada pengujian ini menggunakan *full scan* agar pengujian menguji dari segi website dan sisi jaringannya juga. Setelah itu menentukan tingkat kecepatan dari pengujian. Selanjutnya setelah pengujian telah di lakukan maka dapat di analisis hasilnya dengan melihat kerentanan yang ditemukan dan kategori berdasarkan tingkat dampak yang ditimbulkan. Lalu pada langkah terakhir adalah membuat *report*, pada tahap ini *report* yang digunakan adalah *comprehensive report* agar laporan menjelaskan secara detail dari kerentanan yang telah ditemukan.

Pada Tabel 6 dibawah ini merupakan hasil yang kerentanan yang berhasil ditemukan menggunakan Acunetix. Hasil pengujian ini secara spesifik menguji pada domain KPPM pada port 443 dan menghasilkan sembilan kerentanan yang terdiri dari dua kerentanan tingkat *medium* dan enam kerentanan dengan tingkat *low*.

Tabel 6. Hasil Pengujian dengan Acunetix

Vulnerability	Severity	Confidence
CORS (Cross-Origin Resource Sharing) origin validation failure	Medium	95
Vulnerable JavaScript libraries	Medium	100
Clickjacking: X-Frame-Options header	Low	95
Cookies with missing, inconsistent, or contradictory properties	Low	100

Vulnerability	Severity	Confidence
Cookies without HttpOnly flag set	Low	100
Cookies without Secure flag set	Low	100
HTTP Strict Transport Security (HSTS) not implemented	Low	95
Sensitive pages could be cached	Low	95
TLS/SSL certificate about to expire	Low	100

3.4. *Attack and Penetration*

Berdasarkan hasil pengujian menggunakan tiga tools yaitu burp suite, Acunetix dan Nessus. Setiap *tools* ini memiliki kelebihan serta fitur yang beragam sehingga dapat mengidentifikasi kerentanan pada sistem yang diuji. Dengan menggabungkan hasil dari ketiga *tools* ini tentunya mendapatkan pemahaman yang lebih komprehensif mengenai kerentanan yang ditemukan dan evaluasi lebih lanjut dari tingkat resiko terkait. Dasar dari penentuan daftar kerentanan ini yaitu kerentanan tersebut memiliki risiko yang tinggi sehingga perlu tindakan lebih lanjut, kerentanan tersebut memiliki kesamaan dengan hasil dari pengujian *tools* lainnya, dan kerentanan tersebut dapat diatasi jika kerentanan lainnya telah di perbaiki. Adapun daftar kerentanan tersebut dijelaskan pada Tabel 7 berikut.

Tabel 7. Daftar Kerentanan

Vulnerability	Severity
Vulnerable version of the library 'axios' found	High
TLS certificate	Medium
Vulnerable version of the library 'bootstrap' found	Medium
Vulnerable version of the library 'jquery' found	Medium
CORS (Cross-Origin Resource Sharing) origin validation failure	Medium
HTTP Strict Transport Security (HSTS) not implemented	Low
Source code disclosure	Low
Clickjacking: X-Frame-Options header	Low
Cookies without HttpOnly flag set	Low

Berikut penjelasan dari kerentanan tersebut:

a) Vulnerable version of the library ‘axios’ found
   Versi Library Axios pada *website* target yaitu versi **0.19.0-beta.1.** Dimana pada versi ini memiliki kerentanan terhadap serangan Regular Expression Denial of Service (ReDoS) yaitu serangan yang menyerang algoritma sehingga membuat sistem menjadi sangat lambat atau menyebabkan kegagalan pada sistem aplikasi.
b) TLS Certificate
   Kerentanan ini disebabkan oleh *server website* yang tidak memiliki sertifikat keamanan yang tervalidasi oleh *software* penguji kerentanan.
c) Vulnerable version of the library 'jquery' found
   Jquery yang digunakan versi 3.3.1 dimana pada versi sebelum 3.4.0 yang digunakan dalam Drupal, Backdrop CMS, dan produk-produk lain, mengalami masalah dalam penggunaan jQuery.extend(true, {}, ...) karena adanya Object.prototype pollution.

d) Vulnerable version of the library 'bootstrap' found
Website target menggunakan versi Bootstrap 3.3.7 yang rentan terhadap serangan XSS (Cross-Site Scripting) pada atribut data-template tooltip atau popover. Kerentanan tersebut terdapat pada versi Bootstrap sebelum 3.4.1 dan 4.3.x sebelum 4.3.1

e) Cross-Origin Resource Sharing (CORS) origin validation failure
CORS mendefinisikan mekanisme untuk mengaktifkan permintaan cross-origin pada sisi klien. Website ini menggunakan CORS dengan cara yang tidak aman

f) HTTP Strict Transport Security (HSTS) not implemented
Website belum menerapkan HTTP Strict Transport Security (HSTS) karena header Strict Transport Security hilang dari respons.

g) Source code disclosure
Source code yang di simpan di sisi server terkadang dapat ditemukan oleh pengguna. Dimana seharusnya kode tersebut mungkin memiliki informasi sensitif.

h) Clickjacking: X-Frame-Options header
Clickjacking adalah teknik serangan untuk menipu pengguna web agar mengklik sesuatu yang berbeda dari apa yang mereka anggap mereka klik, sehingga berpotensi mengungkapkan informasi rahasia

i) Cookies without HttpOnly flag set
Satu atau lebih cookie tidak memiliki flag HTTP Only. Dampaknya Cookies dapat di akses dari script dari sisi klien

Sebelum dilakukan mitigasi lebih lanjut, untuk mengetahui tingkat keparahan dan validitas dari kerentanan yang ditemukan dilakukan *penetration testing*. Adapun hasil dari *penetration testing* dapat dilihat pada Tabel 8 berikut

Tabel 8. Hasil *Penetration Testing*

Jenis Kerentanan	**Hasil Penetration Testing**
HSTS Missing from HTTPS Server	Diuji menggunakan aplikasi pihak ketiga yaitu hstspreload, website KPPM terlihat belum terdapat HSTS pada header. Pengujian lebih lanjut yaitu dengan mengirimkan request url dengan HTTP lalu mengecek respon dari request tersebut dengan inspect network pada browser. Dari pengujian ini disimpulkan penerapan HSTS belum terimplementasi dengan baik yang dibuktikan dengan masih terdapat respons http tersebut
Cross-Origin Resource Sharing (CORS) origin validation failure	target yang telah diuji ditemukan miskonfigurasi pada access-control-allow-origin sehingga menyebabkan rentan terhadap serangan domain jahat
Source code disclosure	Hasil pengujian website KPPM ketika menggunakan ”view page source” pada halaman website KPPM terdapat file source code yang dapat diakses secara bebas.
Clickjacking: X-Frame-Options header	Pengujian dilakukan dengan burp clickbandit dan menghasilkan website dapat memanipulasi tombol login dan dapat mengalihkan ke web lain

Jenis Kerentanan	Hasil Penetration Testing
Cookies without HTTPOnly Flag set	hasil pengujian kerentanan ini memiliki dampak pencurian sesi dan pencurian informasi pengguna dimana penyerang dapat mengakses akun pengguna tanpa perlu memasukkan kredensial otentikasi dari sesi dan cookie yang di dapatkan.

3.5. *Remediation*

3.5.1. Perancangan Mitigasi

Berdasarkan analisis pengujian yang telah dilakukan, untuk menghindari dan meminimalisir kerentanan yang ditemukan diperlukan rekomendasi mitigasi yang dapat diterapkan terhadap sistem website. Adapun rekomendasi perbaikan dijelaskan pada Tabel 9 berikut.

Tabel 9. Perancangan Mitigasi

Vulnerability	Tahapan mitigasi
Software Unsupported version	Lakukan upgrade library yang terpasang di web server, berdasarkan hasil pengujian sebelumnya adalah dengan melakukan upgrade pada beberapa library berikut: -Axios 0.21.1 > 1.4.0 -Bootstrap > 5.3.0 -JQuery 3.3.1 > 3.7.0
TLS certificate	Perbarui dan terapkan sertifikat TLS/SSL pada web server menggunakan sertifikat yang terpercaya
CORS (Cross-Origin Resource Sharing) origin validation failure	Untuk menerapkan konfigurasi CORS agar dapat membuka akses lintas domain, dapat menambahkan baris code berikut pada security.js cors: { allRoutes: true, allowOrigins: "*", allowCredentials: false, allowRequestMethods: "GET, POST, PUT, DELETE, OPTIONS, HEAD", allowRequestHeaders: "content-type, authorization", },
HTTP Strict Transport Security (HSTS) not implemented	Untuk menerapkan hsts pada website dapat mengaktifkan modul hsts pada security.js. Isi dari modul tersebut sebagai berikut hsts: { enable: true, maxAge: 31536000, includeSubDomains: true, preload: true, },
Source code disclosure	Melakukan cek keseluruhan terkait penulisan kode dan melakukan update framework sails.js ke versi terbaru.
Clickjacking: X-Frame-Options header	konfigurasi HTTP X Frame-Options atau Content-

Vulnerability	Tahapan mitigasi

	Security Policy dapat diatur sebagai "DENY" untuk memblokir penggunaan tag iframe secara umum. Jika ingin memperbolehkan penggunaan tag iframe hanya pada alamat yang sama, dapat diubah menjadi "SAMEORIGIN". perubahan ini akan mencegah konten halaman website dimuat oleh situs lain saat menggunakan tag iframe. Berikut adalah config nya pada file http.js:
	order:["cookieParser", "session", "bodyParser", "compress", "poweredBy", "frameOptions", "hsts", "router", "www", "favicon"],
	frameOptions: function (req, res, next) {
	res.set("X-Frame-Options","SAMEORIGIN");
	next();
	},

Cookies without HttpOnly flag set	Untuk mencegah pencurian session dan cookies dapat menerapkan cookies menjadi httponly dengan nilai true pada file security.js
Source code disclosure	Melakukan cek keseluruhan terkait penulisan kode dan melakukan update framework sails.js ke versi terbaru.

3.5.2. Pengujian Ulang Pasca Mitigasi

Berdasarkan mitigasi yang telah dilakukan pada poin tahap sebelumnya, kerentanan yang ditemukan untuk menutup celah tersebut dilakukan perbaikan dari segi kode dan konfigurasi aplikasi. Adapun langkah selanjutnya adalah dengan melakukan uji ulang untuk mengetahui apakah dari implementasi mitigasi yang telah dilakukan dapat mengatasi kerentanan tersebut. Hasil dari pengujian ulang dapat dilihat pada Tabel 10 berikut.

Tabel 10. Pengujian ulang pasca mitigasi

Vulnerability Scanning Pra Mitigasi	Vulnerability Scanning Pasca Mitigasi	Keterangan
Vulnerable version of the library 'axios' found	Vulnerable version of the library 'axios' found	Sudah dilakukan upgrade library namun perlu dilakukan pengecekan keseluruhan dari segi kode nya
TLS certificate	-	Kerentanan berhasil ditutup
Vulnerable version of the library 'bootstrap' found	Vulnerable version of the library 'bootstrap' found	Sudah dilakukan upgrade library namun perlu dilakukan pengecekan keseluruhan dari segi kode nya
Vulnerable version of the library 'jquery' found	-	Kerentanan berhasil ditutup
CORS (Cross-Origin Resource Sharing) origin validation failure	-	Kerentanan berhasil ditutup
HTTP Strict Transport Security (HSTS) not implemented	-	Kerentanan berhasil ditutup

Vulnerability Scanning Pra Mitigasi	Vulnerability Scanning Pasca Mitigasi	Keterangan
Source *code* disclosure	Source code disclosure	Memerlukan pengecekan lebih lanjut dari segi kode keseluruhan dan pengecekan dari segi server untuk memastikan konfigurasi keamanan telah di terapkan.
Clickjacking: X-Frame-Options header	-	Kerentanan berhasil ditutup
Cookies without HttpOnly flag set	Cookies without HttpOnly flag set	Implementasi telah dilakukan namun kerentanan ini memerlukan pengecekan lebih lanjut terkait konfigurasi *cookie*.

4. SIMPULAN

Dari hasil *Vulnerability Detection* menggunakan tools Burp Suite, Acunetix dan Nessus dengan menggunakan target *website* KPPM menghasilkan daftar kerentanan dengan hasil yang berbeda-beda. Pada pengujian dengan Burp suite terdapat 11 kerentanan yang terdiri dari 1 kerentanan tingkat *High*, 4 kerentanan tingkat *low*, dan 3 kerentanan tingkat *informational*. Lalu pengujian dengan nessus yang dilakukan pada port 443 Https ditemukan 3 kerentanan dengan tingkat *medium*, 1 kerentanan dengan tingkat *low* dan 2 kerentanan dengan tingkat *informational*. Sedangkan pengujian dengan Acunetix ditemukan 2 kerentanan dengan tingkat *medium*, 7 kerentanan tingkat *low*, dan 2 kerentanan dengan tingkat *informational*. Dari kerentanan yang telah ditemukan dengan ketiga *tools* tersebut ditentukan daftar kerentanan yang akan dilakukan eksploitasi dan mitigasi. Kerentanan tersebut dipilih berdasarkan tingkat kerentanan, kesamaan, dan kerentanan yang dapat diatasi jika kerentanan lain dapat di perbaiki. Kerentanan tersebut yaitu Vulnerable version of the library 'axios', 'bootstrap' and 'JQuery' found, TLS certificate,Cross-Origin Resource Sharing (CORS) origin validation failure, HTTP Strict Transport Security (HSTS) not implemented Source code disclosure, clickjacking X-Frame-Options header, dan Cookies without HttpOnly flag set.

Mitigasi yang dilakukan terhadap kerentanan yang ditemukan adalah dengan memperbaharui TLS Certificate, dan Library ke versi yang terbaru, mengubah konfigurasi untuk kerentanan yang memiliki masalah pada security header seperti Clickjacking, CORS, HSTS not implemented dan Cookies without HttpOnly. Lalu melakukan pengecekan keseluruhan untuk kerentanan source code disclosure. Setelah mitigasi dilakukan pengujian ulang untuk mengetahui kerentanan yang berhasil diatasi dan belum dapat diatasi. Dari pengujian ulang pasca mitigasi yang telah dilakukan, kerentanan yang berhasil diatasi adalah HSTS, CORS, Clickjacking, TLS Certificate dan JQuery Library. Sementara kerentanan yang belum dapat diatasi memerlukan analisis alasan lebih lanjut mengenai hasil *vulnerable detection* pasca mitigasi yang masih terdeteksi dari kerentanan tersebut.

DAFTAR PUSTAKA

[1] J. T. Umar, L. Baja, K. Batam-Indonesia, P. Kelengkapan, R. Al Amin, and E. A. Wibowo, "Pengaruh Kelengkapan Data ,Ketelitian, Kecepatan Terhadap Kepuasan Konsumen Pada Pt. Federal International Finance (FIF) Cabang Batam," *Jurnal Manajemen dan Kewirausahaan*, vol. 1, no. 1, 2021.

[2] S. Shah and B. M. Mehtre, "A Modern Approach to Cyber Security Analysis Using Vulnerability Assessment and Penetration Testing," *International Journal of Electronics Communication and Computer Engineering*, vol. 4, no. 6, 2013.

[3] J. N. Goel and B. M. Mehtre, "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology," in *Procedia Computer Science*, 2015. doi: 10.1016/j.procs.2015.07.458.

[4] J. T. Umar, L. Baja, K. Batam-Indonesia, P. Kelengkapan, R. Al Amin, and E. A. Wibowo, "Pengaruh Kelengkapan Data ,Ketelitian, Kecepatan Terhadap Kepuasan Konsumen Pada Pt. Federal International Finance (FIF) Cabang Batam," *Jurnal Manajemen dan Kewirausahaan*, vol. 1, no. 1, 2021.

[5] S. Shah and B. M. Mehtre, "A Modern Approach to Cyber Security Analysis Using Vulnerability Assessment and Penetration Testing," *International Journal of Electronics Communication and Computer Engineering*, vol. 4, no. 6, 2013.