e-ISSN 2962-6129
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 14 April 2022

Analisis Keamanan Sistem pada *Website* Perusahaan CV. Kazar Teknologi Indonesia dengan Metode *Vulnerability Assesment and Penetration Testing* (VAPT)

Adha Maliq Ibrahim[1], Tomi Defisa[2], Henki Bayu Seta*[3], I Wayan Widi P.*[4],
Fakultas Ilmu Komputer
Universitas Pembangunan Nasional Veteran Jakarta
adhami@upnvj.ac.id, tomidefisa@gmail.com, henkiseta@upnvj.ac.id, wayan.widi@upnvj.ac.id
Jl. Rs. Fatmawati, Pondok Labu, Jakarta Selatan, DKI Jakarta, 12450, Indonesia

Abstrak. Analisis keamanan sangat diperlukan saat ini karena semua data yang kita miliki sudah terhubung dengan internet sehingga keamanan informasi menjadi fundamental disetiap aplikasi yang kita gunakan. Badan Siber Sandi Negara (BSSN) melaporkan bahwa pada tahun 2021 tercatat 1,6 miliar anomali trafik yang terjadi di Indonesia terdiri dari *malware*, *trojan*, dan lain-lain. CV. Kazar Teknologi Indonesia merupakan sebuah perusahaan bergerak dibidang jasa teknologi informasi khususnya pada keamanan informasi. Penelitian ini menggunakan metode *Vulnerability Assessment and Penetration Testing* (VAPT). VAPT merupakan gabungan dari dua metode uji keamanan pada suatu aplikasi atau jaringan. Metode VAPT memiliki alur tahapan yang dimulai dengan *scope*, *reconnaissance*, *vulnerability detection*, *information analysis and planning*, *penetration testing*, *privilege escalation*, *result analysis*, *reporting*, dan *clean-up*. Hasil penelitian ini ditemukan kerentanan dari hasil Nessus sebanyak 42 kerentanan, OpenVAS sebanyak 10 kerentanan, OWASP ZAP sebanyak 10 kerentanan, dan WPScan kerentanan informasi. *Penetration testing* menggunakan teknik seperti analisis jaringan menggunakan Wireshark, *bypass password*, *brute force*, *inspect element* melalui *web browser*, dan *port scanning* dengan perintah dari nmap. Untuk menjaga server dan aplikasi *web* tetap aman, dapat dilakukan kegiatan *maintenance* oleh perusahaan untuk menjaga server dan aplikasi *web* sehingga mengurangi dampak jika terjadi eksploitasi oleh *attacker*.

Kata kunci: *website*, keamanan informasi, VAPT, Nessus, OpenVAS, OWASP ZAP, WPScan, *penetration testing*, *maintenance*.

1. PENDAHULUAN

Diawal tahun 2021 pengguna internet Indonesia mencapai 202,6 juta. Dalam hal ini penggunaan internet di Indonesia mengalami peningkatan 15,5 persen dibandingkan di bulan Januari 2020[1]. Selain dari penambahan jumlah internet, pengguna di Indonesia menghabiskan waktu berinternet rata-rata 8 jam 52 menit, sehingga dapat dikatakan bahwa kegiatan masyarakat tidak pernah lepas dalam menggunakan internet setiap harinya.

Pengguna internet di Indonesia semakin meningkat setiap tahunnya, maka keamanan informasi menjadi hal yang sangat penting dalam menjamin privasi data pengguna, menjamin data pengguna tidak dapat diubah kecuali oleh pengguna itu sendiri, dan data dapat diakses kapanpun oleh pengguna. Namun hal tersebut belum terlaksana secara maksimal, Badan Siber Sandi Negara (BSSN) menemukan 1,6 Miliar serangan siber pada tahun 2021 dengan serangan siber tertinggi sampai terendah terjadi pada bidang akademik, swasta, pemerintah daerah, pemerintah pusat, hukum, dan personal[2].

Dalam hal ini, penulis melakukan penelitian yaitu analisis keamanan *website* untuk mengetahui dan menguji tingkat keamanan *website* pada perusahaan CV. Kazar Teknologi Indonesia. Perusahaan CV. Kazar Teknologi Indonesia merupakan perusahaan swasta yang bergerak dibidang teknologi informasi. Perusahaan ini menyediakan jasa seperti perbaikan komputer atau laptop, penghapusan virus dan *spyware*, pemulihan dan pencadangan data, topologi jaringan, dan penjualan *hardware* dan *software*. Analisis web dilakukan terhadap *website* CV. Kazar Teknologi Indonesia

karena pada *website* tersebut dapat melakukan pengiriman pesan dari klien ke perusahaan dan menjamin pengirim pesan tersebut merupakan klien dan penerima pesan tersebut merupakan perusahaan terkait, selain itu *website* perusahaan dalam penelitian ini saat penulis melakukan *information gathering*, informasi sensitif pada *website* perusahaan ini terekspos dan dibutuhkan analisis kemanan lebih lanjut. Metode analisis keamanan yang digunakan oleh penulis yaitu metode *Vulnerability Assessment and Penetration Testing* (VAPT).

Beberapa penelitian terkait telah banyak dilakukan, contohnya adalah "*Vulnerability Assesment* untuk Mencari Celah Keamanan WEB Aplikasi *E-Learning* Pada Universitas XYZ". Dalam penelitiannya, penulis menggunakan tools nessus sebagai *vulnerability scanning* dan hasilnya berupa CVSS *score* sebagai acuan penlilaian kerentanan pada web yang sedang diujikan. Penulis melakukan penelitian dengan tahapan *identifying scope, gathering information, executing scans, analysing false positives, xploiting vulnerabilities,* dan *generating reports*. Selain penggunaan nessus, tools yang digunakan selama penelitian oleh penulis yaitu Nmap, whois, dig, dan nslookup. Hasil dari penelitian ini yaitu *website e-learning* mendapatkan nilai 9,8 pada overall risk level yang dapat diartikan sebagai kerentanan yang tinggi[3]. Selanjutnya, "Pengujian Kerentanan Sistem dengan Menggunakan Metode *Penetration Testing* di Universitas XYZ". Metode yang dilakukan penulis yaitu pentest dengan tahapan *planning* and *reconnaissance, scanning, gaining access, maintaning access,* dan *analysis*. *Planning* and *reconnaissance* dilakukan dengan melakukan wawancara dengan pihak administrator, tahapan *scanning* menggunakan Nmap, selanjutnya *gaining access* dilakukan paket *sniffing* dan ARP *spoofing poisoning tools* menggunakan *cain and abel*, tahapan *maintaining access* dilakukan setelah mendapatkan hasil dari *gaining access*, dan terakhir pengujian *stress testing* dengan serangan DDoS. Hasil dari penelitian ini yaitu *tools cain and abel* mampu membaca seluruh paket jaringan, dan jenis *password* yang digunakan masih plaintext. *Stress testing* menggunakan DDoS tidak ada efek yang ditimbulkan[4]. Dan, "*Vulnerability Assessment and Penetration Testing* (VAPT) *Framework: Case Study of Government's Website*". Dalam melakukan penelitiannya, penulis menggunakan *tools* yaitu Nmap, Fiddler, Nikto, WebScarab, W3af, Firefox extension yaitu firebug, Cenzic Hailstrom, Core Impact, Nessus, dan Metasploit Framework. Pengujian dilakukan pada *website* pemerintah Indonesia, dan hasil pengujian menemukan berbagai kerentanan yaitu *directory listing, full path disclosure, PHP info disclosure, folder webserver disclosure* dan potensi ancaman lainnya yang menghadirkan kerentanan dengan resiko 2 *critical*, 6 *medium*, dan 2 *low*[5].

Berdasarkan latar belakang yang telah dipaparkan diatas tentang VAPT, bahwa setiap sistem memiliki kerentanan dan sistem tersebut harus diuji keamanannya, penelitian ini dapat membantu mendeteksi kerentanan dan juga melakukan pengujian pada kerentanan yang ditemukan. Sehingga, penelitian ini dibutuhkan untuk mendeteksi dan menguji kerentanan pada *website* yang akan diteliti.

2. LANDASAN TEORI.

2.1. CIA Triad

CIA Triad telah digunakan sebagai definisi praktis kemanan informasi sejak awal adanya bidang keamanan siber[6]. Prinsip dari CIA Triad bahwa asset kemanan siber didefinisikan oleh tiga aspek yang berbeda dan terdiri dari *Confidentiality* (Kerahasiaan) merupakan informasi hanya tersedia untuk pengguna yang dituju. Selanjutnya, *Integrity* (Integritas) ialah membuktikan bahwa informasi tidak dilakukan perubahan. Terakhir, *Availability* (Ketersediaan) adalah informasi harus tersedia untuk pengguna yang dituju.

2.2. *Common Vulnerability Scoring System* (CVSS)

Common Vulnerability Scoring System (CVSS) yaitu sistem skor kerentanan yang menyediakan cara untuk *capture* karakteristik kerentanan, dan menghasilkan *numerical score* yang menggambarkan tingkat keparahannya (*severity*), serta representasi tekstual dari skor tersebut. *Numerical score* kemudian dapat diterjemahkan kedalam representasi kualitatif seperti *low, medium, high,* dan *critical*. Hal ini untuk membantu organisasi menilai dan memprioritaskan proses *vulnerability management* dengan tepat[7].

2.3. *Ethical Hacking*

Ethical Hacking yaitu seorang *hacker* beretika ditugaskan oleh suatu perusahaan yang bertujuan untuk melakukan pengujian keamanan sistem dan jaringan perusahaan tersebut dengan menggunakan teknik yang sama dengan *black hat hacker*. Seorang yang melakukan kegiatan *ethical hacking* disebut *ethical hacker*[8].

2.4. *Vulnerability Assessment*

Vulnerability assessment adalah metode untuk mengenali, menghitung, dan mengevaluasi kerentanan dalam sistem. Pada proses saat ini, seperti jaringan dan sistem operasi dipertimbangkan untuk mengetahui keberadaan *vulnerability* yang sering ditemukan dan jarang ditemukan. *Vulnerability* terjadi karena desain suatu software yang tidak relevan, atau banyak *vulnerability* yang terlihat akibat dari kesalahan konfigurasi, teknik dari *vulnerability assessment* yaitu *static analysis*, *manual testing*, *automated testing*, dan *fuzz testing*[9].

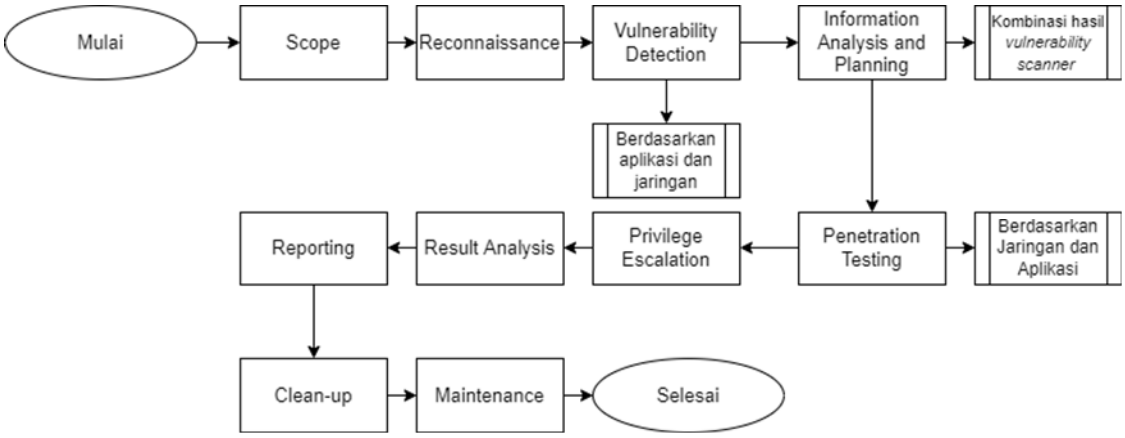
2.5. *Penetration Testing*

Penetration testing (pentest) merupakan proposisi mencoba mendapatkan *entry* yang tidak disetujui ke *resource* yang disetujui. Kegiatan ini diakui sebagai ethical hacking diumpamakan sebagai ”*breaking into your individual structure to see how hard it is to do it*.” Tugas pentest yaitu memilih teknik untuk masuk ke dalam sistem dengan menggunakan *tools* dan teknik konvensional yang dibuat oleh *hackers*[9].

2.6. *Vulnerability Assessment and Penetration Testing* (VAPT)

Vulnerability Assessment and Penetration Testing (VAPT) adalah metodologi dengan proses bertahap untuk melakukan pengujian keamanan suatu sistem aplikasi atau jaringan. Dengan *vulnerability assessment* (VA) merupakan proses scanning suatu sistem aplikasi atau jaringan untuk mengetahui adanya kelemahan dan celah didalamnya, sedangkan *penetration testing* (PT) yaitu langkah setelah dilakukannya *vulnerability assessment* (VA) untuk melakukan percobaan mengeksploitasi sistem atau jaringan secara resmi bertujuan mengetahui kemungkinan eksploitasi dalam sistem. VAPT dalam prosesnya, memliki 9 tahapan proses yaitu dimulai dengan *scope, reconnaissance, vulnerability detection, information analysis and planning, penetration testing, privilege escalation, result analysis, reporting,* dan *clean-up*[10].

3. METODE PENELITIAN



Gambar 1. Metode Penelitian

Berdasarkan diagram alur metode penelitian pada **Gambar 1**, dapat dijelaskan sebagai berikut ini:

1. ***Scope***

   Scope terdiri dari *white box, black box,* dan *grey box*. Dalam penelitian ini menggunakan pendekatan secara *black box*.

2. ***Reconnaissance***

Pada tahapan *reconnaissance*, dalam penelitian ini mendapatkan informasi mengenai sistem yang akan diuji. Informasi yang didapat berupa sistem operasi, jaringan, *subdomain*, dan lain-lain. **Tabel 1** merupakan *tools* yang digunakan pada tahapan *reconnaissance*.

Tabel 1. *Reconnaissance Tools*

Nama Alat	Fungsi
Nmap	Mengetahui port yang tersedia dan status port serta OS server yang digunakan
Whois	Mengetahui informasi langganan web hosting dan pemilik sistem *website*.
Sublist3r	Mengetahui subdomain yang ada pada *website* target.
Nslookup	Scanning pada DNS.
Wappalyzer	Pemindaian pada *website* untuk mengetahui teknologi yang digunakan

3. ***Vulnerability Detection***

Penelitian ini menggunakan teknik *vulnerability assessment* yaitu *automated testing*. Pemilihan teknik tersebut dilakukan agar waktu penelitian tidak terlalu lama dan mendapatkan akurasi yang baik. Untuk menutupi kelemahan pada teknik ini, menggunakan empat *tools* dengan masing-masing dua *tools* untuk pemindaian kerentanan berdasarkan jaringan, dan dua *tools* untuk pemindaian kerentanan berdasarkan aplikasi. **Tabel 2** merupakan daftar *tools* yang digunakan.

Tabel 2. *Vulnerability Detection Tools*

Nama Alat	Fungsi
Nessus	Melakukan pemindaian kerentanan pada jaringan.
OpenVAS	Melakukan pemindaian kerentanan pada jaringan.
OWASP ZAP	Melakukan pemindaian kerentanan pada aplikasi web.
WPScan	Melakukan pemindaian kerentanan pada aplikasi web WordPress.

4. ***Information Analysis and Planning***

Setelah melakukan *vulnerability detection*, kegiatan selanjutnya yaitu melakukan analisa terhadap temuan kerentanan yang didapat pada *tools vulnerability scanner*. Hasil dari dua *tools* pemindaian pada jaringan dan dua *tools* pemindaian pada aplikasi dilakukan analisa dan masing-masing *tools* akan dilakukan kombinasi agar dalam tahapan *penetration testing* lebih terstruktur. Setelah melakukan analisa, selanjutnya menyiapkan *tools* untuk melakukan tahapan berikutnya.

5. ***Penetration Testing***

Didalam tahapan ini, *tools* yang akan digunakan sesuai kerentanan yang ditemukan.

6. ***Privilage Escalation***

Proses selanjutnya, setelah berhasil melakukan eksploitasi terhadap objek penelitian. Penulis berusaha meningkatkan hak akses pada sistem sehingga pada saat melakukan eksploit, penulis melakukan eksploitasi dengan hak akses yang sudah dibuatnya.

7. ***Result Analysis***

Kegiatan ini melakukan analisa terhadap hasil dari *penetration testing* yang dilakukan. Memberikan daftar mengenai kerentanan yang berhasil dan gagal dilakukan saat melakukan *penetration testing*.

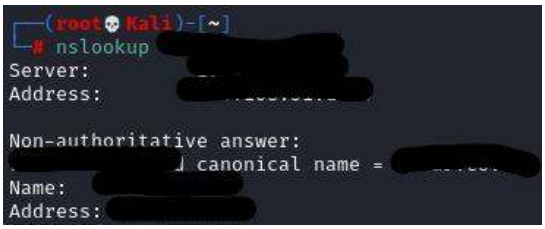
8. ***Reporting***
   Setelah hasil analisis dilakukan, *reporting* dilakukan untuk memberikan rekomendasi dalam memperbaiki kerentanan yang dilakukan pengujian pada tahap *penetration testing* pada objek penelitian sehingga kerentanan tersebut segera diatasi oleh penanggungjawab sistem *website* perusahaan CV. Kazar Teknologi Indonesia.
9. ***Clean-up***
   Tahapan ini merupakan tahapan yang harus dilakukan, dengan melakukan pembersihan pada sistem yang telah diuji ke kondisi semula. Hal ini wajib dilakukan, agar sistem tidak dilakukan eksploitasi oleh peretas (*hacker*) yang tidak bertanggungjawab.
10. ***Maintenance***
    Tahapan ini merupakan tahapan yang ditambahkan oleh penulis untuk melakukan pemberian saran pemeliharaan atau maintenance pada *website* penelitian sehingga apabila terjadi serangan oleh *hacker*, penanggungjawab sistem dapat melakukan tindakan yang sesuai.

4. HASIL DAN PEMBAHSAN

4.1. *Reconnaissance*

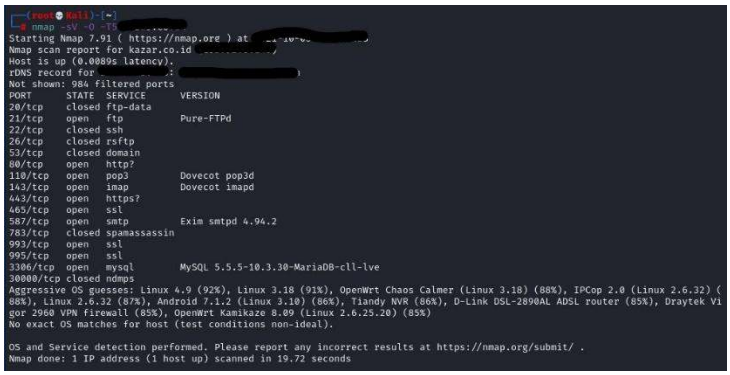
Informasi yang didapatkan akan dimanfaatkan sebaik-baiknya untuk mencari kerentanan pada sistem target. *Tools* yang digunakan dalam pengujian ini yaitu Whois, NSlookup, Sublist3r, Nmap, dan Wappalyzer.

Gambar 2. Whois



Gambar 3. NSlookup

Gambar 4. Sublist3r



Gambar 5. Nmap

Gambar 6. Wappalyzer

Dari **Gambar 2**, **Gambar 3**, **Gambar 4**, **Gambar 5**, dan **Gambar 6** merupakan hasil dari *tools* yang digunakan pada *reconnaissance*. Pada **Gambar 2** menginformasikan tentang registrasi domain pada *tool* Whois, **Gambar 3** memberikan informasi *domain name system* serta *ip server* yang digunakan pada objek penelitian dan dihasilkan melalui *tool* Nslookup, **Gambar 4** hasil Sublist3r yang menginformasikan mengenai *subdomain* yang dimiliki pada objek penelitian, **Gambar 5** informasi *port* dari Nmap menghasilkan status *port* apakah *open, closed, filtered*, dan lain-lain serta *service, version,* dan OS yang digunakan pada *server*, dan **Gambar 6** merupakan informasi dari Wappalyzer mengenai teknologi apa yang digunakan untuk membuat aplikasi web.

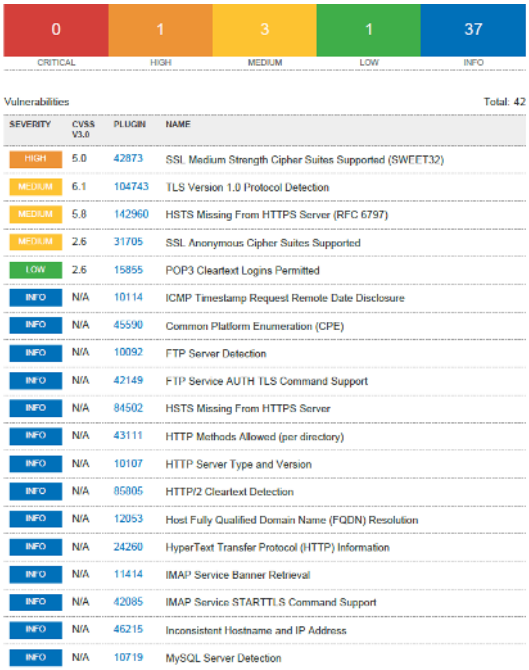
4.2. *Vulnerability Detection, Information Analysis and Planing*

Tools yang digunakan dalam proses ini dikategorikan menjadi dua bagian yaitu berdasarkan jaringan dan aplikasi. Berdasarkan jaringan yaitu Nessus, dan OpenVAS sementara berdasarkan aplikasi yaitu OWASP ZAP dan WPScan.

4.2.1 Berdasarkan Jaringan

Dari hasil kerentana yang ditemukan pada Nessus dan OpenVAS akan dikombinasikan dan diurutkan berdasarkan *severity* lalu kemudian dari *score* kerentanannya masing-masing.

Nessus



0	1	3	1	37
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 42

SEVERITY	CVSS V3.0	PLUGIN	NAME
HIGH	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.8	142960	HSTS Missing From HTTPS Server (RFC 6797)
MEDIUM	2.6	31705	SSL Anonymous Cipher Suites Supported
LOW	2.6	15855	POP3 Cleartext Logins Permitted
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10092	FTP Server Detection
INFO	N/A	42149	FTP Service AUTH TLS Command Support
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	85805	HTTP/2 Cleartext Detection
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11414	IMAP Service Banner Retrieval
INFO	N/A	42085	IMAP Service STARTTLS Command Support
INFO	N/A	46215	Inconsistent Hostname and IP Address
INFO	N/A	10719	MySQL Server Detection

Gambar 7. Hasil Nessus

Dari hasil *scanning* kerentanan pada **Gambar 7** oleh Nessus. Beberapa kerentanan tidak dilakukan ujicoba hal ini dikarenakan kerentanan tersebut tidak memiliki dampak yang besar atau hanya bersifat informasi yang tidak sensitif.

OpenVAS

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location
SSL/TLS: Missing `secure` Cookie Attribute	6.4 (Medium)	99 %	[redacted]		2096/tcp
SSL/TLS: Missing `secure` Cookie Attribute	6.4 (Medium)	99 %	[redacted]		2083/tcp
SSL/TLS: Missing `secure` Cookie Attribute	6.4 (Medium)	99 %	[redacted]		2087/tcp
Sensitive File Disclosure (HTTP)	5.0 (Medium)	70 %	[redacted]		2096/tcp
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	5.0 (Medium)	98 %	[redacted]		443/tcp
Sensitive File Disclosure (HTTP)	5.0 (Medium)	70 %	[redacted]		2083/tcp
Sensitive File Disclosure (HTTP)	5.0 (Medium)	70 %	[redacted]		2086/tcp
Sensitive File Disclosure (HTTP)	5.0 (Medium)	70 %	[redacted]		2095/tcp
Sensitive File Disclosure (HTTP)	5.0 (Medium)	70 %	[redacted]		2082/tcp
Sensitive File Disclosure (HTTP)	5.0 (Medium)	70 %	[redacted]		2087/tcp
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	[redacted]		2095/tcp
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	[redacted]		2082/tcp
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	[redacted]		21/tcp
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	[redacted]		2079/tcp
IMAP Unencrypted Cleartext Login	4.8 (Medium)	70 %	[redacted]		143/tcp
POP3 Unencrypted Cleartext Login	4.8 (Medium)	70 %	[redacted]		110/tcp
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	[redacted]		2077/tcp
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	[redacted]		2086/tcp
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	[redacted]		2086/tcp
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	[redacted]		2083/tcp
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	[redacted]		2087/tcp
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	[redacted]		2096/tcp

Gambar 8. Hasil OpenVAS

Hasil *scanning* kerentanan pada **Gambar 8** oleh OpenVAS menampilkan pengulangan kerentanan yang ditemukan, sehingga salah satu dari kerentanan yang mengalami pengulangan diujicoba. Selain itu, ada beberapa kerentanan yang tidak dilakukan pengujian karena memiliki dampak yang rendah.

4.2.2 Berdasarkan Aplikasi

OWASP ZAP menemukan kerentanan pada aplikasi web dengan *severity* dari *Medium* sampai *info*, sementara pada WPScan kerentanan yang ditemukan dengan *severity info*. Namun hasil dari WPScan dapat menunjang kerentanan lain yang ditemukan untuk dilakukan *pentest*.

OWASP ZAP

Name	Risk Level
X-Frame-Options Header Not Set	Medium
Absence of Anti-CSRF Tokens	Low
Cookie No HttpOnly Flag	Low
Cookie without SameSite Attribute	Low
Incomplete or No Cache-control Header Set	Low
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low
Timestamp Disclosure - Unix	Low
X-Content-Type-Options Header Missing	Low
Charset Mismatch	Informational
Information Disclosure - Suspicious Comments	Informational

Gambar 9. Hasil OWASP ZAP

Hasil dari **Gambar 9** beberapa kerentanan tidak dilakukan pengujian hal ini dikarenakan kerentanan tersebut hanya sekedar informasi atau tidak memiliki dampak yang besar.

WPScan

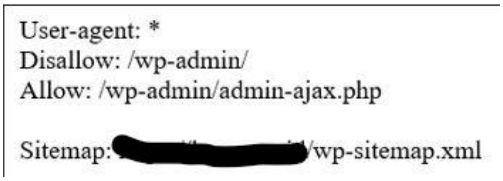
Gambar 10. Hasil WPScan

Gambar 10 merupakan hasil *scanning* dari WPScan yang menemukan *severity info* lebih banyak dari *tools vulnerability* yang lain, namun *info* ini sangat dapat digunakan untuk menunjang pengujian pada kerentan dari kategori jaringan dan aplikasi.

4.3. *Penetration Testing*

4.3.1 Berdasarkan Jaringan

Salah satu pengujian atau *pentest* berdasarkan jaringan yaitu ***Sensitive File Disclosure (HTTP)*** dengan ***severity Medium*** dan ditemukan oleh **OpenVAS** dengan ***score* 5.0**. Pengujian kerentanan ini yaitu dengan cara mengakses direktori tertentu tanpa *account* dengan *privilage* yang tinggi seperti *admin*. Pengujiannya yaitu dengan mengakses direktori robots.txt pada halaman web objek penelitian, sehingga didapatkan seperti berikut:

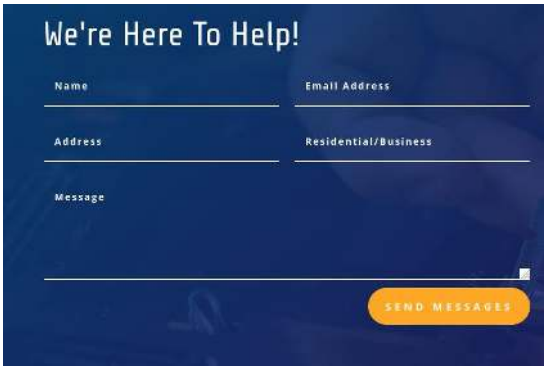


Gambar 11. Akses robots.txt

Pada **Gambar 11** ditemukan direktori /wp-sitemap.xml ketika mencoba akses dengan menambahkan domain utama maka akan mengarahkan ke tampilan yang berisikan sub direktori yang dimiliki.

4.3.2 Berdasarkan Aplikasi

Salah satu pengujian atau *pentest* berdasarkan aplikasi yaitu ***Incomplete or No Cache-control Header Set*** dengan *severity* ***Low***. Kerentanan ini terjadi yaitu tidak ada *cache-control* pada *form*, pengujiannya yaitu dengan cara pengecakan tombol *submit "Send Message"* pada **Gambar 12** berikut:



Gambar 12. Login form *website* target

Pengecekan dilakukan dengan cara *inspect element* dari tombol tersebut, hasil dari *inspect element* diperlihatkan pada **Gambar 13**.

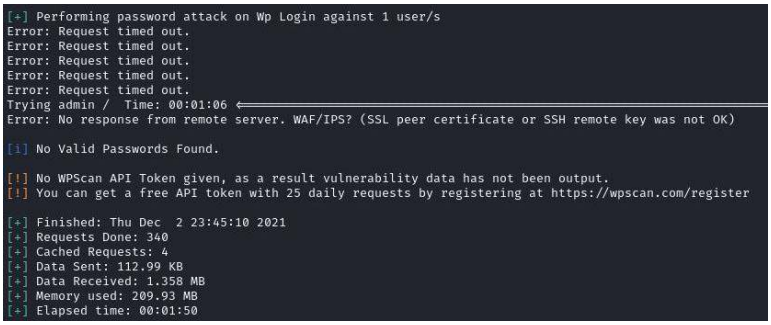
```
<div class="et_contact_bottom_container"> flex
  <button class="et_pb_contact_submit et_pb_button" type="submit" name="et_builder_submit_button">send messages</button>
```

Gambar 13. Inspect Element *Button* Submit

Dari **Gambar 13** tidak adanya *cache-control* hal ini dikarenakan tombol *submit* tidak memiliki fungsi seperti *value* atau *id* sehingga tidak ada proses terhadap *database*.

4.4. *Privilage Escalation*

Kegiatan ini dilakukan untuk meningkatkan hak akses dari *user* dengan *privilage* yang terbatas menjadi *super user* dengan hak akses penuh. Untuk melakukannya, harus mendapatkan *username* dengan tingkat *super user* hal ini didapatkan saat melakukan *scanning vulnerability* pada WPScan dan didapatkan berjumlah 2 *username*. Setelah didapatkan *username*, untuk melakukan *login* dapat menggunakan teknik *brute-force* dan *wordlist* yang digunakan untuk *password brute-force* yaitu *wordlist* yang didapat dengan cara mencari informasi pribadi dari pemilik akun admin.



Gambar 14. Proses *Brute Force*

Gambar 14 memperlihatkan proses *brute-force* menggunakan WPScan. Namun hal ini gagal dilakukan dikarenakan *firewall* pada objek target memblokir *IP address* peneliti sehingga gagal dalam melakukan

login dengan *super user*.

4.5. *Result Analysis*

Hasil dari tahapan *pentest* pada kerentanan yang sudah dilakukan pengujiannya. Kerentanan yang diuji apakah hasil pengujiannya berhasil (positif) atau tidak berhasil (negatif).

Tabel 3. *Result Analysis* Berdasarkan Jaringan

Nama Kerentanan	*Severity*	*Score*	Hasil Pengujian	
			Positif	Negatif
SSL Medium Strength Cipher Suites Supported SWEET 32 (Nessus)	*High*	5.0		□
SSL/TLS: Missing 'secure' Cookie Attribute (OpenVAS)	*Medium*	6.4	□	
TLS Version 1.0 Protocol Detection (Nessus)	*Medium*	6.1		□
HSTS Missing From HTTPS Server (RFC 6797) (Nesus)	*Medium*	5.8		□
Sensitive File Disclosure (HTTP) (OpenVAS)	*Medium*	5.0	□	
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS (OpenVAS)	*Medium*	5.0		□
Cleartext Transmission of Sensitive Information via HTTP(OpenVAS)	*Medium*	4.8	□	
FTP Unencrypted Cleartext Login(OpenVAS)	*Medium*	4.8	□	
IMAP Unencrypted Cleartext Login(OpenVAS)	*Medium*	4.8	□	
POP3 Unencrypted Cleartext Login (OpenVAS)	*Medium*	4.8	□	
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (OpenVAS)	*Medium*	4.3		□
SSL/TLS: Diffie-Helman Key Exchange Insufficient DH Group Strength (OpenVAS)	*Medium*	4.0	□	
POP3 Cleartext Logins Permitted (Nessus)	*Low*	2.6	□	
FTP Server Detection	*Info*	-	□	
HTTP Server Type and Version	*Info*	-	□	
HyperText Transfer Protocol (HTTP) Information	*Info*	-	□	
IMAP Service STARTTLS Command Support	*Info*	-	□	
MySQL Server Detection	*Info*	-	□	
WebDAV Detection	*Info*	-		□

Tabel 4. *Result Analysis* Berdasarkan Aplikasi

Nama Kerentanan	*Severity*	Hasil Pengujian	
		Ya	Tidak
X-Frame-Options Header Not Set	*Medium*		□

Nama Kerentanan	*Severity*	Hasil Pengujian	
		Ya	Tidak
Absence of Anti-CSRF Tokens	*Low*		
Cookie No HttpOnly Flag	*Low*		
Cookie without SameSite Attribute	*Low*		
Incomplete or No Cache-control Header Set	*Low*		
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	*Low*		
Information Disclosure - Suspicious Comments	*Info*		

4.6. *Reporting*

Tabel 5. *Reporting* Berdasarkan Jaringan

Nama Kerentanan	Rekomendasi Perbaikan Kerentanan
SSL Medium Strength Cipher Suites Supported SWEET 32 (Nessus)	Melakukan konfigurasi ulang aplikasi web dan gunakan enkripsi dengan kompleksitas yang rumit.
SSL/TLS: Missing 'secure' Cookie Attribute (OpenVAS)	Melakukan konfigurasi untuk seluruh *cookie* yang dikirim melalui SSL/TLS dengan konfigurasi *secure.*
TLS Version 1.0 Protocol Detection (Nessus)	Nonaktifkan penggunaan TLS dengan versi 1.0 dan gunakan versi paling terbaru.
HSTS Missing From HTTPS Server (RFC 6797) (Nesus)	Lakukan konfigurasi pada *remote* web server untuk menggunakan HSTS
Sensitive File Disclosure (HTTP) (OpenVAS)	Melakukan konfigurasi ulang pada server web agar informasi sensitif tidak dapat diakses.
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS (OpenVAS)	Melakukan konfigurasi *service* ini dengan tidak menerima *cipher suite* yang rentan.
Cleartext Transmission of Sensitive Information via HTTP(OpenVAS)	Menerapkan transmisi data sensitif melalui koneksi SSL/TLS yang terenkripsi dan selalu pastikan pengguna aplikasi web terkoneksi SSL/TLS yang aman.
FTP Unencrypted Cleartext Login(OpenVAS)	Mengaktifkan FTPS atau menerapkan koneksi dengan perintah 'AUTH TLS'.
IMAP Unencrypted Cleartext Login(OpenVAS)	Melakukan konfigurasi *remote server* untuk selalu menerapkan koneksi terenkripsi melalui SSL/TLS dengan perintah 'STARTTTLS'
POP3 Unencrypted Cleartext Login (OpenVAS)	Melakukan konfigurasi *remote server* untuk selalu menerapkan koneksi terenkripsi mealui SSL/TLS dengan perintah 'STLS'
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (OpenVAS)	Menonaktifkan protokol TLSv1.0 dan TLSv1.1, selanjutnya gunakan versi paling terbaru.
SSL/TLS: Diffie-Helman Key Exchange Insufficient DH Group Strength Vulnerability (OpenVAS)	Melakukan *deploy Elliptic-Curve Diffie-Hellman* (ECDHE) dengan 2048 bit agar enkripsi yang digunakan lebih kuat.

Nama Kerentanan	Rekomendasi Perbaikan Kerentanan
POP3 Cleartext Logins Permitted (Nessus)	Hubungi *hosting* vendor untuk memperbaiki atau mengenkripsi *traffic* dengan SSL/TLS menggunakan *stunnel.*
FTP Server Detection	Lakukan penutupan *port* jika tidak menggunakan *port* ini.
HTTP Server Type and Version	Lakukan penutupan *port* karena sudah menggunakan *port* HTTPS.
HyperText Transfer Protocol (HTTP) Information	Lakukan penutupan *port* karena sudah menggunakan *port* HTTPS.
IMAP Service STARTTLS Command Support	Lakukan konfigurasi ulang agar *port* IMAP menggunakan STARTTLS *service.*
MySQL Server Detection	Lakukan penutupan *port* karena penyerang dapat melakuakan serangan dari *port MySQL.*
WebDAV Detection	Lakukan penyembunyian informasi agar tidak terdeteksi saat melakukan pemindaian.

Tabel 6. *Reporting* Berdasarkan Aplikasi

Nama Kerentanan	Rekomendasi Perbaikan Kerentanan
X-Frame-Options Header Not Set	Aktifkan pengaturan seluruh halaman aplikasi web dengan perintah *X-Frame-Options* yaitu *SAMEORIGIN* atau *DENY*.
Absence of Anti-CSRF Tokens	Gunakan *ESAPI Session Management* dan melakukan pengecekan *HTTP Referer header* untuk melihat apakah permintaan berasal dari halaman web yang diinginkan.
Cookie No HttpOnly Flag	Pastikan seluruh *cookie* telah mengaktifkan *HttpOnly Flag*.
Cookie without SameSite Attribute	Pastikan *SameSite Attribute* pada seluruh *cookie* dilakukan pengaturan ke ‘lax’ atau idealnya ‘strict’
Incomplete or No Cache-control Header Set	Selalu pastikan *cache-control HTTP Header* dilakukan pengaturan dengan *no-cache*, *no-store*, dan harus memvalidasi ulang.
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Memastikan server web, server aplikasi, *load balancer*, dan lain lain melakukan konfigurasi untuk tidak menampilkan “*X-Powered-By” headers*.
Information Disclosure - Suspicious Comments	Menghapus semua *comments* yang mengembalikan informasi yang dapat membantu *hacker*, dan perbaiki konfigurasi aplikasi web mendasar yang dapat ditemukan oleh *hacker*.

4.7. *Clean-up*

Proses ini tidak berhasil dilakukan karena dalam penelitian ini tidak mendapatkan akses user dengan *privilage super user*. Namun, pada penelitian ini tidak melakukan modifikasi secara *user interface*, *database*, dan jaringan pada sistem sehingga proses ini tidak harus dilakukan.

4.8. *Maintenance*

Pemeliharaan atau *maintenance* selalu dilakukan untuk memiliki keamanan yang sangat baik, beberapa langkah yang dapat dilakukan oleh pihak perusahaan untuk melakukan pemeliharaan sistem berdasarkan

hasil penelitian yang telah dilakukan:

1. Melakukan penutupan *port* yang tidak seharusnya dibuka atau terdeteksi oleh alat pemindaian *port*.
2. Dalam membuat suatu aplikasi web diharuskan mengikuti *best practice*.
3. Melakukan kegiatan rutin terkait VAPT minimal 3 bulan sekali.
4. Membuat *vulnerability management* dan *patch management* dari hasil VAPT yang dilakukan.

5. KESIMPULAN

Jenis kerentanan pada sistem *website* perusahaan CV. Kazar Teknologi Indonesia dikategorikan dengan dua jenis kerentanan yaitu berdasarkan aplikasi dan berdasarkan jaringan. Berdasarkan jaringan, kerentanan yang ditemukan Nessus berjumlah 1 *High*, 3 *Medium*, 1 *Low*, dan 37 *Info*, kemudian kerentanan yang ditemukan pada OpenVAS berjumlah *Medium* 9, dan *Low* 1. Selanjutnya, pengujian berdasarkan jaringan yang diujikan yaitu 1 *High*, 11 *Medium*, 1 *Low*, dan 6 *Information*, pengujian dikatakan positif dalam hasil pengujian yaitu terjadi pada protokol SSL/TLS, kemudian pada port HTTP, FTP, IMAP, POP3, dan MySQL. Selanjutnya, kerentanan berdasarkan aplikasi yang ditemukan OWASP ZAP berjumlah 1 *Medium*, 7 *Low*, dan 2 *Info*. Pengujian yang diujikan berdasarkan aplikasi yaitu 1 *Medium*, 5 *Low*, dan 1 *Info*, pengujian dikatakan positif dalam hasil pengujian yaitu tidak adanya CSRF, *cookie* yang bermasalah seperti tidak adanya HttpOnly dan tanpa adanya *SameSite Attribute*, terekspos informasi server melalui X-Powered-By, dan terjadinya *information disclosure*. Hasil kerentanan pada WPScan bersifat *Information* dan kerentanan tersebut dimanfaatkan oleh penulis untuk membantu keseluruhan pengujian berdasarkan jaringan dan berdasarkan aplikasi. Selain itu, *Severity* dan *Score* didapat berdasarkan dari database *tools* VA yang digunakan sehingga masing-masing VA memiliki penilaiannya masing-masing dalam menentukan *Severity* dan *Score*.

Referensi

[1] G. P. Riyanto, “Jumlah Pengguna Internet Indonesia 2021 Tembus 202 Juta,” *kompas.com*, Feb. 23, 2021.

[2] D. Rahmawati, “BSSN Temukan 1,6 Miliar Serangan Siber Sepanjang 2021, Mayoritas Malware,” *detiknews*, Jakarta, Mar. 07, 2022.

[3] M. Aziz, “VULNERABILITY ASSESMENT UNTUK MENCARI CELAH KEAMANAN WEB APLIKASI E-LEARNING PADA UNIVERSITAS XYZ,” *JECSIT*, vol. 1, no. 1, pp. 101–109, 2021.

[4] J. A. Ginting and I. G. N. Suryantara, “PENGUJIAN KERENTANAN SISTEM DENGAN MENGGUNAKAN METODE PENETRATION TESTING DI UNIVERSITAS XYZ,” *INFOTECH J.*, vol. 7, no. 1, pp. 41–46, 2021, doi: 10.37365/jti.v7i1.105.

[5] A. Almaarif and M. Lubis, “Vulnerability Assessment and Penetration Testing (VAPT) Framework: Case Study of Government’s Website,” *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 10, no. 5, pp. 1874–1880, 2020, doi: 10.18517/ijaseit.10.5.8862.

[6] J. Van Der Ham, “Toward a Better Understanding of ‘Cybersecurity,’” *Digit. Threat. Res. Pract.*, vol. 2, no. 3, pp. 3–5, 2021, doi: 10.1145/3442445.

[7] First, “Common Vulnerability Scoring System v3.0: User Guide,” *first.org*, 2021. https://www.first.org/cvss/v3.0/user-guide (accessed Nov. 21, 2021).

[8] G. Aryo Utomo, “Ethical Hacking,” *CyberSecurity dan Forensik Digital.*, vol. 2, pp. 8–15, 2019.

[9] B. A. Chandrakant and J. P. Prakash, “VULNERABILITY ASSESSMENT AND PENETRATION TESTING AS CYBER DEFENCE,” *IJEAST*, vol. 4, no. 2, pp. 72–76, 2019.

[10] A. F. Zulfi, “EVALUASI KEAMANAN APLIKASI SISTEM INFORMASI MAHASISWA MENGGUNAKAN FRAMEWORK VAPT (STUDI KASUS : SISTER UNIVERSITAS JEMBER),” Institut Teknologi Sepuluh Nopember, 2017.