BAB 4
HASIL PENELITIAN

4.1 RINGKASAN HASIL PENELITIAN

Tujuan dari penelitian ini adalah untuk mengukur keamanan *website Repository* Unjaya milik Universitas Jenderal Achmad Yani Yogyakarta dengan metode *Open Source Security Testing Methodology Manual* (OSSTMM), hasil dari penelitian ini nantinya dapat dijadikan bahan evaluasi terkait keamanan sistem yang ada di dalamnya. Setelah mendapatkan izin dari pihak pengelola *website* , penelitian ini dilakukan dengan bantuan *tool* Netcraft, Nmap, Nikto *Scanner* dan OWASP ZAP. Dari hasil penelitian untuk mencari celah keamanan yang ada di *website Repositoty* Unjaya dengan alamat URL *http://repository.unjaya.ac.id*, memberikan data pengujian bahwa *website* ini berada pada kategori *website* dengan keamanan kurang karena memiliki nilai *RAV Score* 82,8676 *ravs* atau nilai *ravs* <100 dan masih memerlukan tambahan 17.19 *ravs* untuk menjadi *website* dengan keamanan sempurna.

4.2 WAWANCARA

Pada penelitian ini proses wawancara dilakukan untuk mencari informasi terkait *website Repository* Unjaya kepada pihak pengelola dan penanggung jawab *website* dalam hal ini kewenangan diserahkan pada bagian Pusat Sistem Informasi Universitas Jenderal Achmad Yani Yogyakarta. Wawancara dilakukan pada tanggal 29 Mei 2024 pukul 10.00 s/d selesai. Wawancara dilakukan di ruang Pusat Informasi (PUSI) dengan Bapak Sigid Nugroho Adhi, S.Kom.,M.Eng sebagai narasumber. Berikut adalah pertanyaan dan jawaban yang dihasilkan dari proses wawancara yang dilakukan:

Tabel 4.1 Hasil Wawancara

No	Pertanyaan	Jawaban
1	Apakah ada standar atau kebijakan keamanan yang diikuti dalam pengembangan dan pemeliharaan *website*?	Ada semua kebijakan tercantum di *website pusi.unjaya.ac.id* dalam dokumen Peraturan Rektor UNJAYA Nomor Skep/016/UNJAYA/II/2022
2	Apakah *website* pernah diuji untuk melihat apakah ada celah keamanan yang rentan terhadap serangan umum? Jika pernah apa hasilnya?	Pengujian dengan tujuan mengetahui celah (bekerjasama dengan pihak lain untuk menguji *website*) belum pernah dilakukan, tapi ada beberapa pihak yang sebelumnya pernah memberitahukan kerentanan *website* pada pengelola.
3	Bagaimana proses pemantauan keamanan dilakukan untuk mendeteksi ancaman atau serangan yang mungkin terjadi?	Untuk proses pemantauan keamanan, pengelola memiliki kewajiban untuk memuat report setiap satu bulan sekali dan melaporkan hasil-hasil laporan dari *website* mulai dari berapa banyak percobaan penyerangan yang berhasil tercatat.
4	Berapa volume data yang disimpan di *website*? Bagaimana kebijakan perlindungan data dan privasi pengguna diterapkan?	Volume data yang disimpan di *repository.unjaya.ac.id* sebesar 6,6% dari total ruang penyimpanan 400 eGB, menggunakan cloud Nginx dan database MySQL untuk menyimpan data. Terkait kebijakan yang mengatur perlindungan data dan privasi diatur oleh Peraturan Rektor UNJAYA Nomor Skep/016/UNJAYA/II/2022
5	Bagaimana sistem *backup* data dilakukan saat terjadi keadaan darurat?	Sistem *backup* data dilakukan secara berkala, server juga sudah menggunakan *Raid* 1.
6	Apakah pernah terjadi kasus penyerangan/kendala yang mengancam keamanan *website* ini sebelumnya, dan bagaimana cara mengatasinya?	Pernah, kasus seperti ini umumnya dilakukan oleh pihak-pihak yang mengatas namakan negara-negara tertentu. Cara penanganannya dengan menambahkan filter di negara-negara terkait pada *firewall*.

Tabel 4.1 berisi pertanyaan dan jawaban dari tahap wawancara. Dari keenam pertanyaan wawancara dapat disimpulkan bahwa *website repository.unjaya.ac.id* sudah mengikuti kebijakan dari instansi terkait yaitu Universitas Jenderal Achmad Yani Yogyakarta, namun pengujian kerentanan pada *website* ini belum pernah dilakukan sebelumnya.

4.3 ANALISIS

Tahap analisis pada penelitian ini merupakan proses menentukan batasan-batasan dalam penelitian ini.

Tabel 4.2 Analisis

No	Analisis		Keterangan
1	Aset	Objek penelitian	*http://repository.unjaya.ac.id*
2	*Zona Engagement*	Mekanisme proteksi	Mekanisme sistem aktif melalui *firewall*
		Proteksi/layanan	Menyediakan akses untuk konten-konten akademik seperti skripsi, karya ilmiah, jurnal dan publikasi lain
3	Skop	Energi listrik	*Diesel Backup System* (DBS) adalah energi alternatif yang digunakan apabila terjadi padam listrik
		Kebijakan	Peraturan Rektor UNJAYA Nomor Skep/016/UNJAYA/II/2022
		Hosting dan *Banwith* Internet	Dua jalur *bandwith*, internet dan *website*
4	*Vektor*		*Vektor* dua arah yaitu *vektor* dari dalam dan *vektor* dari luar. Karena jaringan yang digunakan dalam penelitian ini adalah jaringan internet luar dan jaringan internet lokal
5	*Channel*		*Data network channel*

No	Analisis	Keterangan
6	Tipe Tes	*Black box testing* tes mandiri oleh peneliti atas izin pengelola
7	*Rules of engagement*	1.Wawancara dan Studi Pustaka 2.Analisis 3.Implementasi 4.Penilaian menggunakan RAV dan STAR 5. Laporan

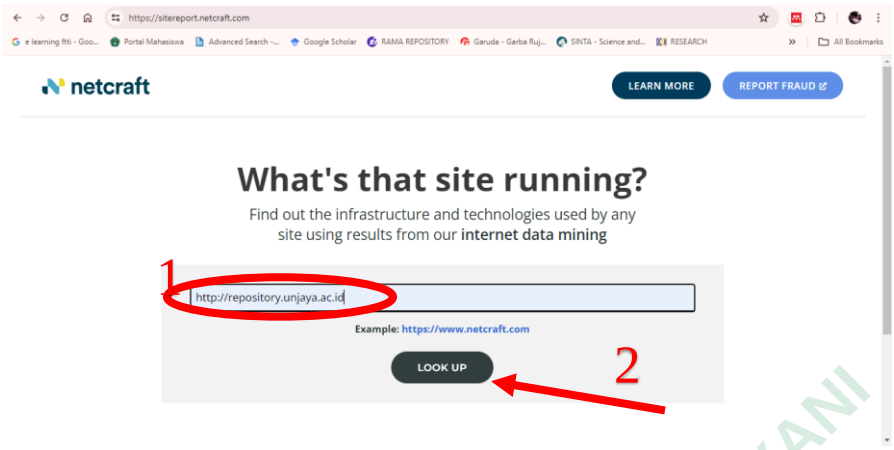
Tabel 4.2 menunjukan hasil dari tahapan analisis dalam menentukan aset, *zona engagement*, skop, *vektor*, *channel*, tipe tes dan *rules of engagement* dari *website repository.unjaya.ac.id*.

4.4 IMPLEMENTASI

Tahap implementasi pada penelitian ini terdiri dari empat langkah yang harus dilakukan dengan urut agar informasi yang diperoleh dari tahapan ini dapat digunakan dengan baik tanpa ada kendala pada tahapan selanjutnya yaitu penilaian RAV dan STAR.

4.4.1 *Reconnaissance / Information Gathering*

Tahapan *Reconnaissance* / information *gathering* dilakukan untuk mengumpulkan informasi dari website *Repository* Unjaya menggunakan *https://sitereport.netcraft.com* . Akses *website* melalui google chrome, seperti gambar 4.1 berikut.



Gambar 4.1 *Website* Netcraft

Gambar 4.1 menunjukan tampilan dari halaman utama *website* Netcraft pada bar yang ditandai merah dimasukan URL dari *website* tujuan (*repository.unjaya.ac.id*), lalu klik *Look UP button* dan tungggu beberapa saat sampai hasil pemindaian keluar.

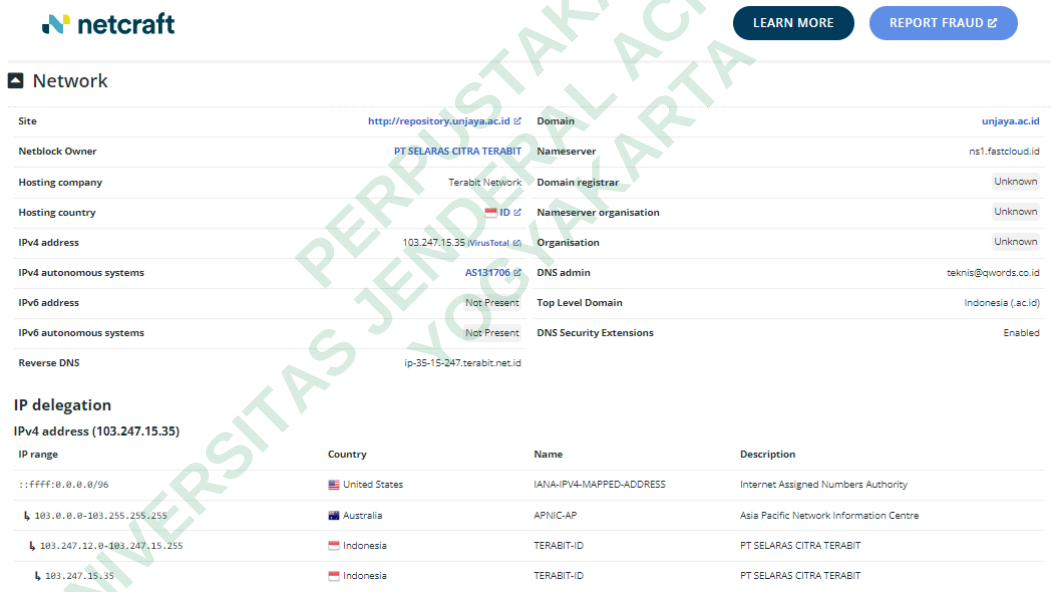
Gambar 4.2 Hasil *Background* Netcraft

Gambar 4.2 menunjukkan informasi dasar tentang *website repository.unjaya.ac.id.* Informasi yang ditampilkan adalah sebagai berikut;

Tabel 4.3 Hasil *Background*

Site title	*Not Present*
Date first seen	*February* 2021
Site rank	*Not Present*
Primary language	*English*
Description	*Not Present*

Tabel 4.3 menunjukan bahwa *website repository.unjaya.ac.id* tidak mempunyai informasi judul halaman, peringkat situs, dan deskripsi web. Web ini pertama kali terdeteksi pada Februari 2021, dan menggunakan Bahasa Inggris sebagai bahasa utama yang digunakan di web tersebut.



Gambar 4.3 Hasil *Network* & IP *Delegation*

Gambar 4.3 menunjukkan *report* dari *network* dan IP *delegation* dari *website repository.unjaya.ac.id.* Informasi yang ditampilkan adalah sebagai berikut;

- *Site*

  Menyediakan URL lengkap situs web untuk referensi.

- *Domain*

  Menunjukkan nama *domain* yang terdaftar untuk web tersebut.

- *Netblock Owner*

  Menunjukkan pemilik blok IP yang digunakan oleh web, untuk mengetahui siapa yang mengelola alamat IP situs tersebut.
- *Nameserver*

  Menunjukkan server nama (DNS) yang digunakan untuk mengarahkan lalu lintas internet ke situs ini, membantu dalam mengarahkan *domain* ke server *hosting* yang benar.
- *Hosting company*

  Menyebutkan perusahaan yang menyediakan layanan *hosting* untuk web. Ini penting untuk mengetahui siapa yang bertanggung jawab atas server fisik yang menyimpan data web.
- *Domain registrar*

  Meunjukkan pendaftar *domain*, yang biasanya bertanggung jawab untuk pengelolaan dan pemeliharaan nama *domain*.
- *Hosting country*

  Menunjukkan negara di mana server *hosting* web berada, untuk mempertimbangkan kecepatan akses dan regulasi hukum yang berlaku.
- *Nameserver organisation*

  Menunjukkan organisasi yang mengelola *nameserver*
- IPv4 *address*

  Menyediakan alamat IP dari web serta mencatat jumlah laporan deteksi virus pada alamat IP tersebut
- *Organisation*

  Menunjukkan organisasi yang terdaftar sebagai pemilik alamat IP, meskipun dalam kasus ini tidak diketahui.
- IPv4 *autonomous systems*

  Menyediakan informasi tentang Sistem Otonom (AS) yang mengelola rute internet untuk alamat IP ini. AS adalah unit administrasi yang mengontrol sekelompok IP tertentu.
- DNS admin

Memberikan alamat email kontak untuk administrator DNS, yang bertanggung jawab atas pengelolaan dan konfigurasi DNS untuk *domain*.

- IPv6 *address*

  Menunjukkan bahwa tidak ada alamat IPv6 yang tersedia untuk situs ini.

- *Top Level Domain*

  Menunjukkan bahwa situs ini menggunakan *domain* tingkat atas (TLD) yang khusus untuk institusi akademik di Indonesia.

- IPv6 *autonomous systems*

  Menunjukkan bahwa tidak ada sistem otonom IPv6 yang terkait dengan alamat ini.

- DNS *Security Extensions*

  Menunjukkan bahwa ekstensi keamanan DNS (DNSSEC) diaktifkan untuk *domain* ini, yang membantu melindungi pengguna dari serangan seperti *spoofing* DNS.

- *Reverse* DNS

  Menyediakan nama *host* yang terkait dengan alamat IP ini, sering digunakan untuk keperluan diagnostik dan manajemen jaringan.

Informasi ini membantu memahami struktur jaringan, keamanan, dan manajemen situs web *Repository* Unjaya yang penting untuk administrasi jaringan, keamanan siber, dan analisis teknis.

Tabel 4.4 *Network Report*

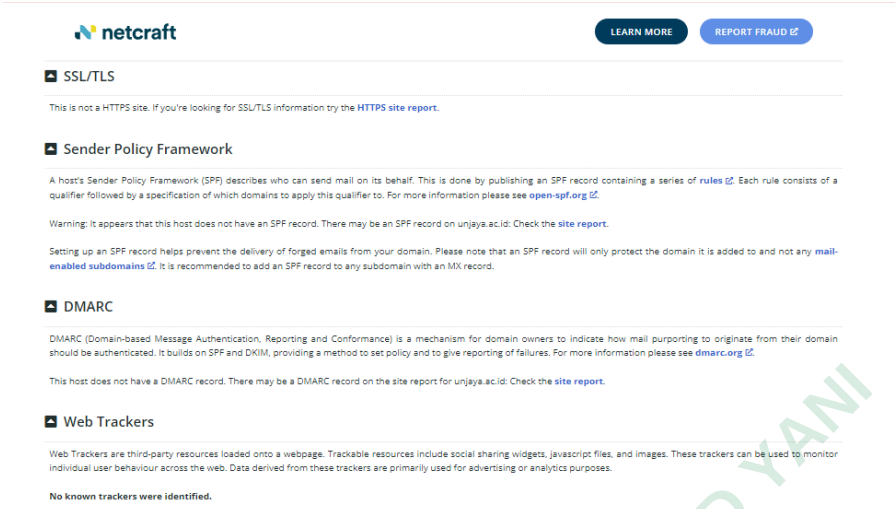
Temuan	Keterangan
Site	*http://repository.unjaya.ac.id*
Domain	unjaya.ac.id
Netblock Owner	PT SELARAS CITRA TERABIT
Nameserver	*ns1.fastcloud.id*
Hosting company	Terabit *Network*
Domain registrar	*Unknown*
Hosting country	Indonesia (ID)

Temuan	Keterangan
Nameserver organisation	*Unknown*
IPv4 *address*	103.247.15.35 (VirusTotal:6)
Organisation	*Unknown*
IPv4 *autonomous systems*	AS31709
DNS admin	teknis@vodvds.co.id
IPv6 *address*	*Not Present*
Top Level Domain	Indonesia (.ac.id)
IPv6 *autonomous systems*	*Not Present*
DNS *Security Extensions*	*Enabled*
Reverse DNS	ip-35-15-247.terabit.net.id

Tabel 4.5 IP *Delegation Report*

IP *range*: ::ffff:0.0.0.0/96	IPv4 *address*	103.247.15.35
	Country	United States
	Name	IANA-IPv4-Mapped-Address
	Description	Internet Assigned Numbers Authority
IP *range*: 183.0.0.0 – 83.255.255.255	*Country*	Australia
	Name	Apnic-Ap
	Description	Asia Pacific Network Information Centre
IP *range*: 183.247.12.0 – 183.247.15.255	*Country*	Indonesia
	Name	Terabit-ID
	Description	PT Selaras Citra Terabit
IP *range*: 183.247.15.0 – 183.247.15.35	*Country*	Indonesia
	Name	Terabit-ID
	Description	Pt Selaras Citra Terabit

Tabel 4.4 dan Tabel 4.5 menunjukan hasil pemindaian dari Netcraft yang menunjukan informasi dari *Network* dan IP *Delegation.*



Gambar 4.4 Peningkatan Keamanan *Website*

Gambar 4.4 menunjukan hasil pemindaian Netcraft menampilkan informasi tentang *Secure Sockets Layer* (SSL) dan *Transport Layer Security (*TLS) atau protokol keamanan yang dirancang untuk mengenkripsi data yang dikirimkan antara server web dan browser pengguna, sehingga informasi sensitif seperti data login, detail kartu kredit, dan data pribadi lainnya terlindungi dari penyadap. Sedangkan TLS adalah versi terbaru dan lebih aman dari SSL. Informasi kedua adalah *Sender Policy Framework* (SPF) atau protokol autentikasi email yang digunakan untuk mencegah spam dan *spoofing* email. Informasi ketiga tantang *Domain-based Message Authentication, Reporting, and Conformance* (DMARC) atau protokol autentikasi email yang dibangun di atas SPF dan DKIM (*Domain Keys Identified Mai*. Informasi terakhir yang didapat adalah informasi mengenai Web *Tracker* atau skrip yang digunakan untuk melacak aktivitas dan perilaku pengguna di situs web.

Tabel 4.6 Peningkatan Keamanan *Website*

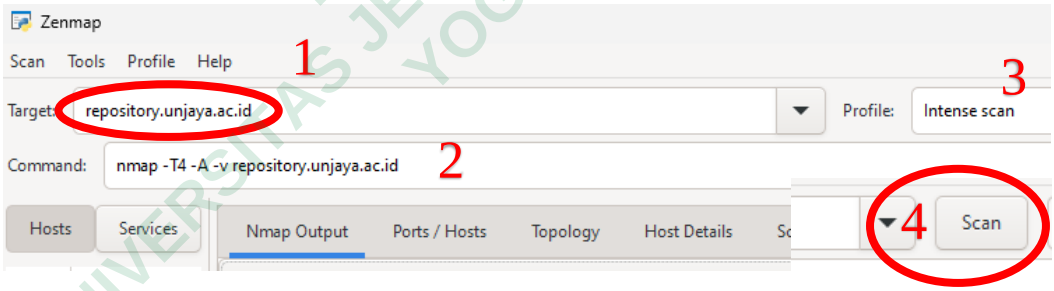
Peningkatan Keamanan	
SSL/TLS	Situs ini bukan HTTPS.
SPF	Tampaknya host ini tidak memiliki catatan SPF. Mungkin ada catatan SPF di domain unjaya.ac.id.

Peningkatan Keamanan	
DMARC	Host ini tidak memiliki catatan DMARC. Mungkin ada catatan DMARC di situs laporan untuk unjaya.ac.id. Disarankan untuk memeriksa laporan situs.
Web *Tracker*	Tidak ada *tracker* web yang teridentifikasi

Tabel 4.6 menunjukan hasil pindai *website* Netcraft terhadap SSL/TLS, SPF, DMARC, dan Web *Tracker*, pada halaman *website Repository* Unjaya. Laporan ini mengindikasikan beberapa kelemahan dalam konfigurasi email keamanan *domain* unjaya.ac.id, yaitu tidak adanya catatan SPF dan DMARC, yang penting untuk mencegah penyalahgunaan email dari *domain* tersebut. Selain itu, tidak ada Web *Tracker* yang teridentifikasi di web tersebut.

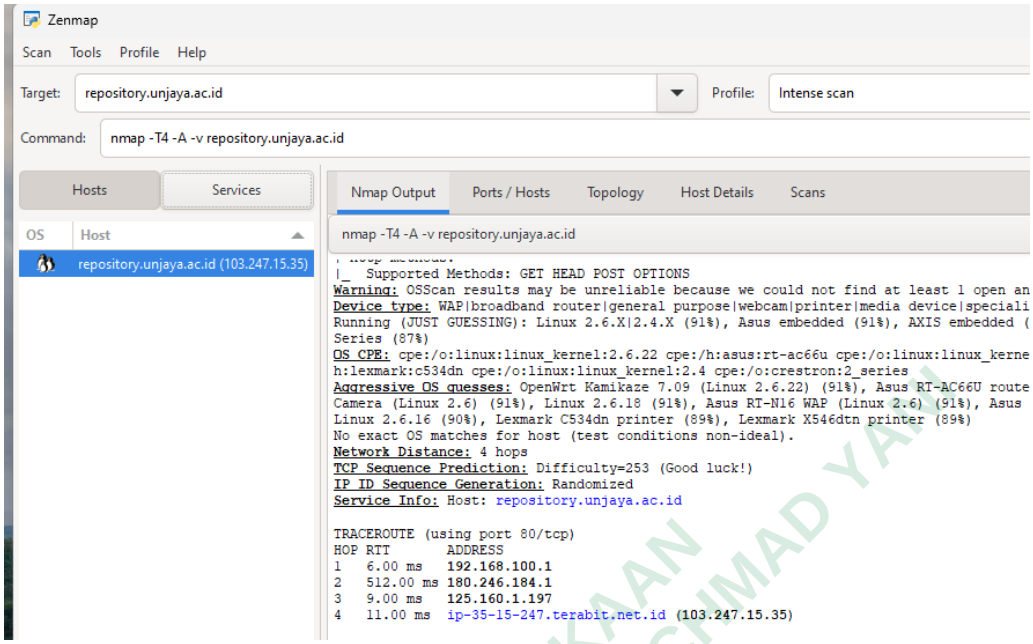
4.4.2 *Scanning Network*

Scanning network dilakukan untuk mengumpulkan informasi dari website *Repository* Unjaya menggunakan aplikasi Nmap. Dengan tahapan seperti gambar di bawah



Gambar 4.5 Nmap *setting*

Setting sebelum melakukan *scanning* menggunakan Nmap ditunjukan pada Gambar 4.5 setelah *Scan Button* diklik tunggu sampe proses selesai. Waktu yang dibutuhkan untuk melakukan proses scanning ini 5-10 menit.



Gambar 4.6 Hasil *Scanning* Nmap

Hasil *scanning* dari Nmap ditampilkan oleh Gambar 4.6, informasi yang didapatkan adalah sebagai berikut:

Tabel 4.7 Hasil *Scanning* Nmap

Temuan	Keterangan
Host	*repository.unjaya.ac.id*
IP	103.247.15.35
Waktu pindai	535.36 s
Jarak jaringan	4 lompatan (*hops*) 192.168.100.1 (6.00 ms) 180.2466.184.1 (512.00 ms) 125.160.1.197 (9.00 ms) IP-35-15-247.terabit.net.id (103.247.15.35) (11.00 ms)
Open port	80/tcp (HTTP) menjalankan Apache httpd 2.4.52 (Ubuntu)
	443/tcp (HTTPS) menjalankan Apache httpd 2.4.52
http-robots.txt	1 entri yang tidak diperbolehkan (/cgi/)
Favicon	MD5 tidak dikenal (CCB8412F6C6957CBF1AD01BEE1F32A45)
Title	*Welcome to Repository Unjaya - Repository Unjaya*

Temuan	Keterangan
Port Lain	997 *port* tcp terfilter (*no-response*), 1 *port* tcp terfilter (*admin-prohibited)*

Tabel 4.7 menunjukan hasil scanning yang didapatkan dari tools Nmap, diantaranya ditemukan port terbuka pada port 80/tcp (HTTP) dan port 443/tcp (HTTPS).

Tabel 4.8 *Port* 80/tcp

Temuan	Keterangan
Generator HTTP	Eprints 3.4.4
Title	*Welcome to Repository Unjaya - Repository Unjaya*
Header Server HTTP	Apache/2.4.52 (Ubuntu)
Metode HTTP yang didukung	*GET, HEAD, POST, OPTIONS*

Tabel 4.8 menunjukan bahwa dari *port* terbuka 80/tcp (HTTP), diperoleh juga informasi terkait *generator* HTTP, *title*, *header server* HTTP, dan metode HTTP yang didukung dari *website repository.unjaya.ac.id.*

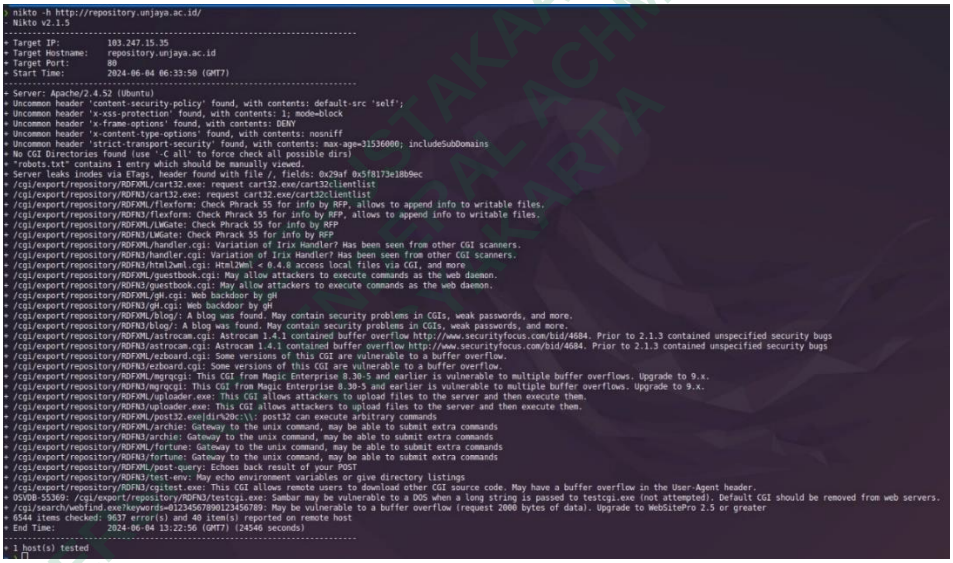
Tabel 4.9 *Port* 443/tcp

Temuan	Keterangan
Subject	*commonName=repository.unjaya.ac.id*
Subject Alternative Name	*DNS.unjaya.ac.id*
Issuer	*commonName=R10/organizationName=Let's Encrypt/countryName=US*
Tipe Kunci Publik	rsa, 2048 bit
Algoritma Tanda Tangan	*sha256WithRSAEncryption*
Validitas	dari 2024-06-10 sampai 2024-09-08
MD5	9299:a81a:2f88:f814:b91a:f0f8:49a1:8eed
SHA-1	47d1:cc6b:d091:a34c:ab5c:16e2:82d1:b0f4:6207

Tabel 4.9 menunjukan bahwa dari *port* terbuka 443/tcp dapat diperoleh informasi terkait *subject*, *subject alternative name*, *issuer*, tipe kunci publik, algoritma tanda tangan, validitas, MD5 dan SHA-1.

4.4.3 *Scanning Vulnerability*

Tahap *scanning vulnerability* menggunakan *tools* Nikto *Scanner*. Berbeda dengan *tools* lain yang dapat berjalan di Windows OS, Nikto *Scanner* memerlukan aplikasi tambahan untuk dapat berjalan di Windows OS. Dalam penelitian ini peneliti menggunakan Oracle VM Virtual Manager sebagai aplikasi penghubung antara Nikto Scanner dan Windows OS.



Gambar 4.7 Hasil Nikto *Scanner*

Gambar 4.7 menunjukkan hasil pemindaian keamanan menggunakan Nikto v2.1.5 pada server dengan IP 103.247.15.35 dan nama *host repository.unjaya.ac.id*. Berikut adalah informasi lain yang didapatkan Nikto Scanner terkait server, port target, tanggal pemindaian

Tabel 4.10 Hasil Nikto *Scanner*

Temuan	Keterangan
Server	Apache/2.4.52 (Ubuntu)
Port Target	80

Temuan	Keterangan
Tanggal Pemindaian	2024-06-04 06:33:50 (GMT)
Jumlah Direktori CGI yang ditemukan	0
Jumlah pengecekan item	9637
Jumlah kerentanan yang ditemukan	40

Tabel 4.10 Berikut adalah informasi lain yang didapatkan Nikto *Scanner* terkait server, *port* target, tanggal pemindaian, jumlah direktori CGI yang ditemukan, jumlah pengecekan item, jumlah kerentanan yang ditemukan.

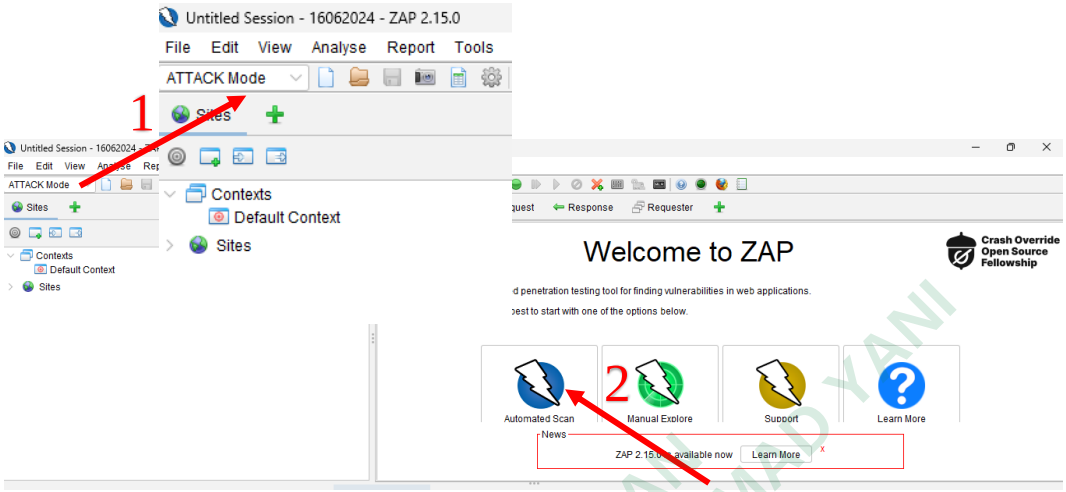
Tabel 4.11 Detil Kerentanan

No	Kategori	Kelas	Keterangan
1	Header yang tidak umum	*content-security-policy*	*default-src 'self'*
		x-xss-protection	1; *mode=block*
		x-frame-options	DENY
		x-content-type-options	nosniff
		strict-transport-security	*max-age=31536000; includeSubDomains*
2	File atau direktori yang tidak ditemukan (404)	-	*/cgi-bin/*
3	Informasi server yang dapat diakses:	-	ETag dengan hash file tertentu yang menunjukkan informasi potensial tentang file yang dipindai.
4	Kerentanan dalam berbagai file CGI	*/cgi/export/repository/RDFXML/cart32.exe*	memungkinkan penyerang menambahkan informasi ke file yang dapat ditulis.
		/cgi/export/repository/RDFXML/flexform	memungkinkan penyerang menambahkan informasi ke file yang dapat ditulis.
		/cgi/export/repository/RDFXML/LGGuestbook	dapat dieksploitasi untuk menjalankan perintah sebagai daemon web.

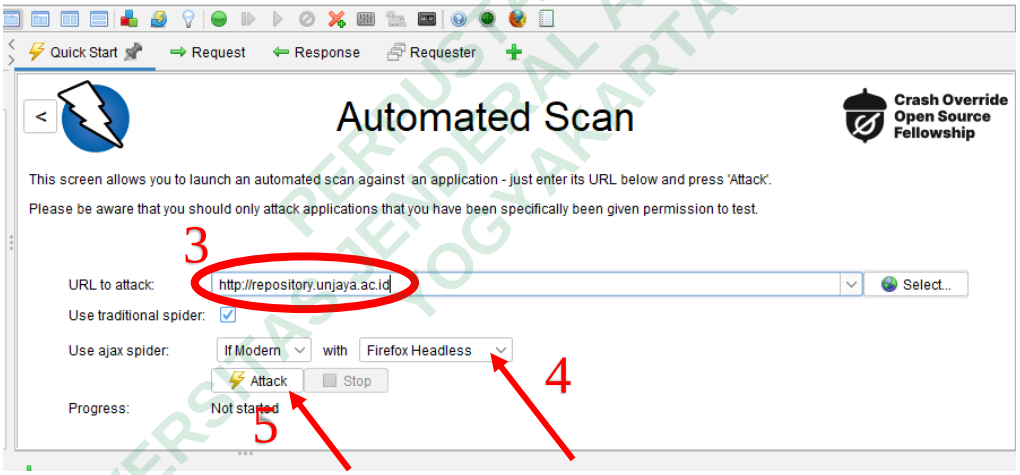
No	Kategori	Kelas	Keterangan
		5/cgi/export/repository6/RDFXML/nph-test-cgi	dapat dieksploitasi untuk menjalankan perintah sebagai daemon web
		/cgi/export/repository/RDFXML/ezboard.cgi	beberapa versi dari CGI ini rentan terhadap buffer overflow.
		/cgi/export/repository/RDFXML/upload.py	memungkinkan penyerang untuk mengunggah file ke server dan menjalankannya
		/cgi/export/repository/RDFXML/uploader.exe	memungkinkan penyerang untuk mengunggah file ke server dan menjalankannya.
5	Beberapa program berbasis UNIX yang ditemukan rentan	*archie*	dapat menjalankan perintah tambahan
		phf	dapat menjalankan perintah tambahan.
		test-env	memungkinkan pembacaan variabel environment atau memberikan listing direktori.
6	Kerentanan OSVDB	OSVDB-596	CGI htsearch memungkinkan unduhan kode sumber HTDig. Rentan terhadap buffer overflow.
		OSVDB-569	CGI /cgi/export/proxy/nph-test-cgi rentan terhadap buffer overflow. Harus dihapus dari server web.

Tabel 4.11 menunjukan detil kerentanan yang ditemukan oleh Nikto s*canner* seperti penemuan kerentanan pada Header yang tidak umum, file atau direktori yang tidak ditemukan (404), Informasi server yang dapat diakses, kerentanan dalam berbagai file CGI, beberapa program berbasis UNIX yang ditemukan rentan, kerentanan OSVDB.

4.4.4 *Penetration Testing*



Gambar 4.8 *Setting* OWASP ZAP 1

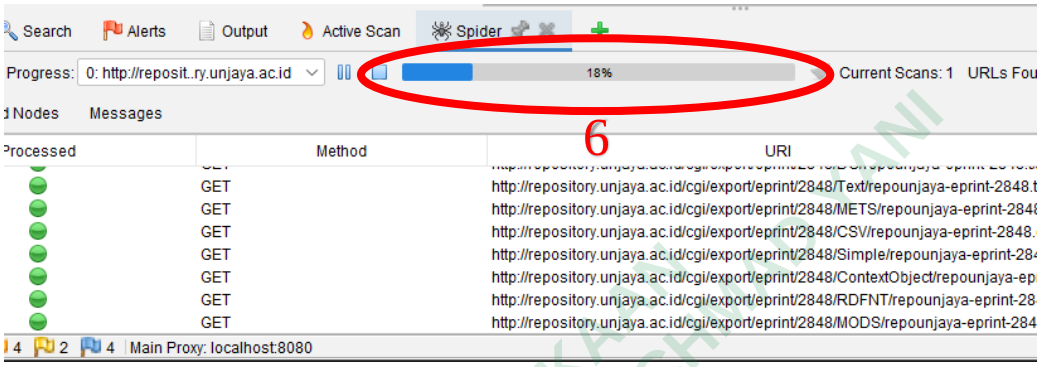


Gambar 4.9 *Setting* OWASP ZAP 2

Untuk memenuhi kebutuhan data dalam penelitian ini maka sebelum melakukan proses *scanning network* menggunakan OWASP ZAP, *setting* aplikasi OWASP ZAP harus diatur seperti Gambar 4.8 dan Gambar 4.9.

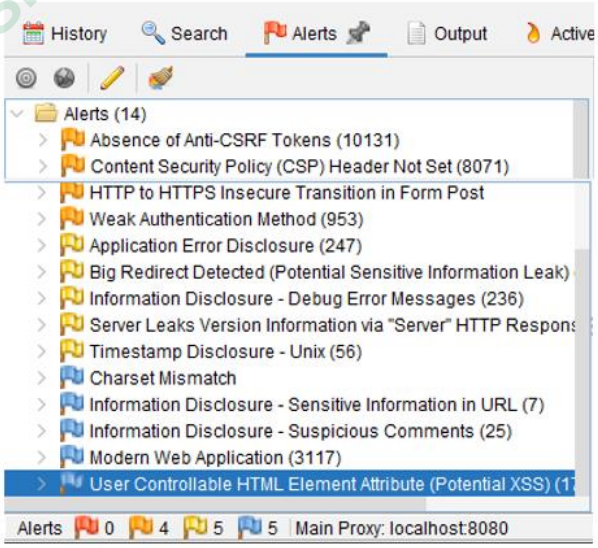
1. Mengubah standart mode menjadi *attack mode*
2. Memilih pemindaian otomatis (*automated scan*)
3. Memasukan alamat URL target yang akan diteliti yaitu *http://repository.unjaya.ac.id*

4. Memastikan *use ajax spidernya* terpasang pada pilihan *firefox headless*
5. Setelah keempat langkah diatas sudah dipastikan benar, langkah selanjutnya adalah melakukan serangan (*attack*).



Gambar 4.10 Proses *Scanning*

Setelah langkah pada Gambar 4.10 dilakukan, perlu menunggu beberapa waktu untuk mendapatkan seluruh hasil *scanning* dari OWASP ZAP, dalam pemindaian kali ini waktu yang dibutuhkan oleh peneliti kurang lebih 2-3 jam (pukul 11 – 13). Lamanya waktu pemindaian dapat berbeda-beda dalam proses *scanning* tergantung kecepatan jaringan, spesifikasi perangkat komputer, dan waktu sibuk lalu lintas *website* target.



Gambar 4.11 Hasil OWASP ZAP

Dari hasil pemindaian menggunakan OWASP ZAP menemukan 14 *alerts* sebagaimana ditunjukan pada Gambar 4.12. Hasil tersebut menunjukan bahwa *website Repository* Unjaya *Absence of Anti-CSRF Tokens, Content Security policy* (CSP) *Header Not Set*, HTTP to HTTPS Insecure *Transition in form Post*, *Weak Authentications Method, Application Error Disclosure, Big Redirect Detected* (*Potential Sensitive Information Leak*), *Information Disclosure-Debug Error Messages, Server Leaks Version Information Via "server*" HTTP *Respons, Timestamp Disclosure,Charset Mismatch, Information Disclosure - Sensitive Information in* URL, *Information Disclosure – suspicious comments, mmodern web application, danUser Controllable* HTML *Element Attribute (*XSS*).*

Tabel 4.12 Temuan Data

Temuan	Sumber	Keterangan
Timestamp Disclosure	OWASP ZAP	Informasi *timestamp* terungkap dalam respon HTTP
HTTP to *HTTPS Insecure Transition*	OWASP ZAP	Transisi dari HTTP ke HTTPS tidak aman ditemukan
Absence of Anti-CSRF *Tokens*	OWASP ZAP	Token Anti-CSRF tidak ada
Content Security Policy Header Not Set	OWASP ZAP	*Header Content Security Policy* (CSP) tidak diatur
User Controllable HTML *Element Attribute (*XSS*)*	OWASP ZAP	Elemen HTML yang dikontrol pengguna berpotensi XSS ditemukan
Weak Authentication Method	OWASP ZAP	Metode autentikasi yang lemah ditemukan
Information Disclosure - Sensitive Information in URL	OWASP ZAP	Informasi sensitif ditemukan dalam URL
Information Disclosure - Debug Error Messages	OWASP ZAP	Pesan kesalahan debug yang mengungkapkan informasi sensitif
Application Error Disclosure	OWASP ZAP	Informasi kesalahan aplikasi terungkap
Server Leaks Version Information via	OWASP ZAP	Informasi versi server ditemukan melalui respon HTTP

Temuan	Sumber	Keterangan
"Server" HTTP *Response*		
Server Leaks Version Information	Nikto *Scanner*	Ditemukan versi server yang sedang digunakan (Apache 2.4.52)
Uncommon header 'content-security-policy' found	Nikto *Scanner*	Header CSP tidak umum ditemukan
Uncommon header 'x-xss-protection' found	Nikto *Scanner*	Header X-XSS-Protection ditemukan
CGI *Directories Found*	Nikto *Scanner*	Direktori CGI ditemukan
Potential vulnerabilities in multiple CGI *scripts*	Nikto *Scanner*	Potensi kerentanan dalam beberapa skrip CGI ditemukan
Buffer Overflow vulnerabilities	Nikto *Scanner*	Beberapa kerentanan *buffer overflow* dalam skrip CGI ditemukan
Open Ports (80/tcp, 443/tcp)	Nmap	*Port* 80 (HTTP) dan 443 (HTTPS) terbuka
EPrints 3.4.4	Nmap	EPrints 3.4.4 terdeteksi sebagai generator HTTP
SSL *Certificate Details*	Nmap	Informasi sertifikat SSL terdeteksi
OS *Detection*	Nmap	Deteksi OS: Linux 2.6.X atau 2.4.X
Traceroute Results	Nmap	Hasil *traceroute* untuk *repository.unjaya.ac.id*
HTTP *Methods Supported*	Nmap	Metode HTTP yang didukung (*Get*, *Head*, *Post*, *Options*)

Dari informasi-informasi yang diperoleh dari tahapan *scanning network* mengggunakan Nmap, tahap *scanning vulnerability* menggunakan Nikto *Scanner*, dan *penetration testing* menggunakan OWASP ZAP maka data yang akan digunakan dalam penilaian RAV tercantum dalam Tabel 4.12 .

4.5 PENILAIAN RAV DAN STAR

Untuk melakukan penilaian *Risk Asessment Value* perlu menentukan nilai dari *operational security*, *loss control* kelas *interactive* dan *process*, serta *controls*. Sedangkan untuk *Security Testing Audit Report* merupakan ringkasan proses dan hasil dari penelitian ini.

4.5.1 *Risk Assesment Value*

1. *Operational Security*

Tabel 4.13 Nilai dan Temuan Kategori *Operational Security*

Metrik	Temuan	Nilai
Visibility	*Server Leaks Version Information*	3
	Uncommon header 'content-security-policy' found	
	Uncommon header 'x-xss-protection' found	
Access	*Server Leaks Version Information via "Server"* HTTP *Response*	3
	HTTP *Methods Supported*	
	Open Ports (80/tcp, 443/tcp)	
	CGI *Directories Found*	
	Potential vulnerabilities in multiple CGI *scripts*	
Trust	SSL *Certificate Details*	1

Tabel 4.13 menunjukan bahwa pada penilaian kategori *Oprational Security website repository.unjaya.ac.id* mempunyai 3 nilai untuk *visibility* dan *access* dan 1 nilai untuk *trust*.

2. *Loss Controls*

a. Interactive

Tabel 4.14 Nilai dan Temuan Kategori *Loss Control* Kelas *Interactive*

Metrik	Temuan	Nilai
Authentication	Weak Authentication Method	1
Identification	*Information Disclosure - Sensitive Information in URL*	2
	OS Detection	
Resilience	HTTP *to* HTTPS *Insecure Transition*	2
	Absence of Anti-CSRF Tokens	
Subjugation	*User Controllable* HTML *Element Attribute* (XSS)	1
Continuity	*Application Error Disclosure*	1

Tabel 4.14 menunjukan bahwa kategori *loss control* kelas *interactive authentication, subjugation,* dan *continuity* mempunyai nilai 1, sedangkan *recsilience* dan *identification* mempunyai nilai 2.

b. Process

Tabel 4.15 Nilai dan Temuan Kategori *Loss Control* Kelas *Process*

Metrik	Keterangan	Nilai
Non-repudiation	Tidak ada informasi spesifik mengenai *non-repudiantion*	0
Confidentiality	*Information Disclosure- Sensitive Information in URL*	2
	SSL Certificate Details	
Privacy	*Content Security Policy Header Not Set*	2
	Information Disclosure - Sensitive Information in URL	
Integrity	*Weak Authentication Method*	3
	Buffer Overflow vulnerabilities	

Metrik	Keterangan	Nilai
	EPrints 3.4.4	
Alarm	*Server Leaks Version Information via "Server"* HTTP *Response*	2
	Uncommon header 'content-security-policy' found	

Tabel 4.15 menunjukan bahwa kategori *loss control* kelas process *Non-repudention* tidak memiliki nilai/0, 2 nilai untuk *confidentiality*, *privacy* dan *alarm*, dan 3 nilai untuk *integrity*.

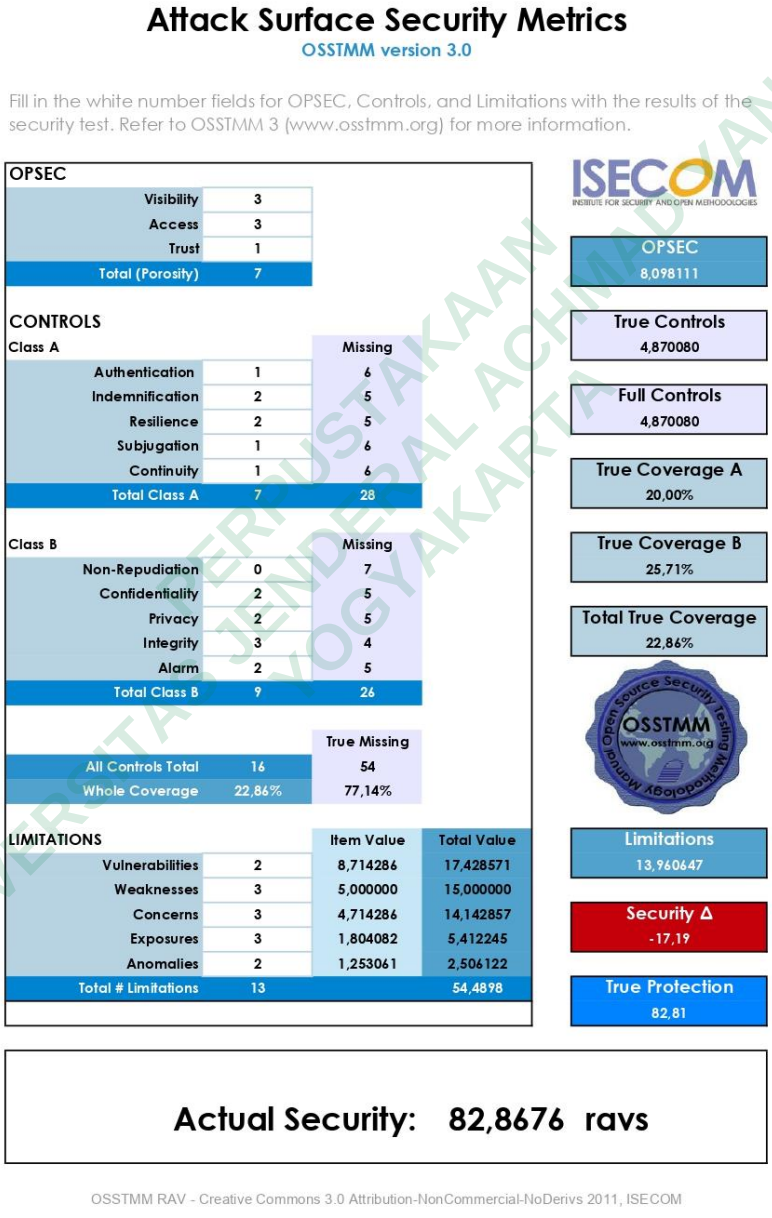
3. *Limitations*

Tabel 4.16 Nilai dan Temuan Kategori *Limitations*

Metrik	Keterangan	Nilai
Vulnerabilities	*Buffer Overflow vulnerabilities*	2
	Potential vulnerabilities in multiple CGI *scripts*	
Weaknesses	*Weak Authentication Method*	3
	CGI *Directories Found*	
	Potential vulnerabilities in multiple CGI *scripts*	
Concerns	*Server Leaks Version Information via "Server"* HTTP *Response*	3
	Weak Authentication Method	
	Buffer Overflow vulnerabilities	
Exposures	*Information Disclosure - Debug Error Messages*	3
	Server Leaks Version Information	
	Weak Authentication Method	
Anomalies	*Uncommon header 'content-security-policy' found*	2
	Uncommon header 'x-xss-protection' found	

Tabel 4.16 menunjukan bahwa kategori *limitations* memiliki nilai 2 untuk *vulnerability* dan *anomalies.* Sedangkan untuk *weaknesses*, *concerns*, dan e*xposures* mempunyai nilai 3.

4. *RAV Score*



Attack Surface Security Metrics

OSSTMM version 3.0

Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.

OPSEC		
Visibility	3	
Access	3	
Trust	1	
Total (Porosity)	7	

CONTROLS		
Class A		Missing
Authentication	1	6
Indemnification	2	5
Resilience	2	5
Subjugation	1	6
Continuity	1	6
Total Class A	7	28
Class B		Missing
Non-Repudiation	0	7
Confidentiality	2	5
Privacy	2	5
Integrity	3	4
Alarm	2	5
Total Class B	9	26
		True Missing
All Controls Total	16	54
Whole Coverage	22,86%	77,14%

LIMITATIONS		Item Value	Total Value
Vulnerabilities	2	8,714286	17,428571
Weaknesses	3	5,000000	15,000000
Concerns	3	4,714286	14,142857
Exposures	3	1,804082	5,412245
Anomalies	2	1,253061	2,506122
Total # Limitations	13		54,4898

ISECOM

INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC	8,098111
True Controls	4,870080
Full Controls	4,870080
True Coverage A	20,00%
True Coverage B	25,71%
Total True Coverage	22,86%
Limitations	13,960647
Security Δ	-17,19
True Protection	82,81

OSSTMM Open Source Security Testing Methodology Manual www.osstmm.org

Actual Security: 82,8676 ravs

OSSTMM RAV - Creative Commons 3.0 Attribution-NonCommercial-NoDerivs 2011, ISECOM

Gambar 4.12 Hasil *RAV Score Website Repository* Unjaya

Gambar 4.12 menunjukan hasil *RAV Score* dari *website Repository* Unjaya sebesar **82,8676 ravs** dan kekurangan security sebesar **17.19 ravs**

4.5.2 *Security Testing Audit Report*

Setelah melakukan penelitian pada tahap wawancara bersama narasumber Bapak Sigid Nugroho Adhi, S.Kom.,M.Eng pada tanggal 29/05/2024, *reconnaissance/information gathering* pada tanggal 02/06/2024 menggunakan Netcraft, *scanning network* pada tanggal 02/06/2024 menggunakan Nmap, *scanning vulnerability* pada tanggal 04/06/2024 menggunakan Nikto *Scanner*, dan *penetration testing* pada tanggal 22/06/2024 OWASP ZAP, serta melakukan perhitungan sesuai standar *Open Source Security Testhing Methodology Manual* maka analisis kerentanan pada *domain repository.unjaya.ac.id* menghasilkan *RAV score* sebesar 82,8676 *ravs*. *Website repository.unjaya.ac.id* termasuk kedalam kategori *website* dengan keamanan kurang karena memerlukan 17,19 *ravs* untuk mencapai kategori *website* dengan keamanan sempurna. Penilaian keamanan pada *repository.unjaya.ac.id* mengungkapkan beberapa kerentanan dan keterbatasan, sebagaimana ditunjukkan oleh kerentanan pada *operational security, loss control invitation* dan *process*, serta *limitations*.

4.6 LAPORAN

Pada tahap terakhir dari semua proses penelitian terhadap *website repository.unjaya.ac.id* menggunakan metode *Open Source Security Testhing Methodology Manual*, Tabel 4.17 merupakan kesimpulan penulis tentang hasil penelian ini bahwa keempat alat yang digunakan yaitu Netcraft, Nmap, Nikto *Scanner* dan OWASP ZAP berhasil menemukan celah/kerentanan pada *website Repository* Unjaya. Bila terlambat ditangani maka kerentanan-kerentanan ini berpotensi menimbulkan;

Tabel 4.17 Potensi Kerentanan pada *Website Repository* Unjaya

Kerentanan	Potensi
Timestamp Disclosure	Penyerang dapat menggunakan informasi timestamp untuk melakukan serangan timing attack atau menilai

Kerentanan	Potensi
	versi perangkat lunak yang digunakan untuk mencari kerentanan yang sesuai.
HTTP to HTTPS *Insecure Transition*	Pengguna mungkin terekspos pada serangan *man-in-the-middle* (MITM) selama transisi dari HTTP ke HTTPS, yang dapat mengakibatkan pengungkapan informasi sensitif.
Absence of Anti-CSRF *Tokens*	Rentan terhadap serangan *Cross-Site Request Forgery* (CSRF), di mana penyerang dapat membuat pengguna yang tidak curiga melakukan tindakan yang tidak diinginkan di aplikasi web.
Content Security Policy Header Not Set	Rentan terhadap serangan *Cross-Site Scripting* (XSS) karena tidak ada kebijakan yang mengontrol sumber daya yang dapat dimuat oleh browser.
User Controllable HTML *Element Attribute (*XSS*)*	Penyerang dapat menyisipkan skrip berbahaya yang dieksekusi oleh browser pengguna, mencuri informasi sensitif atau mengubah konten situs.
Weak Authentication Method	Aplikasi mudah disusupi oleh penyerang yang menggunakan metode autentikasi lemah, memungkinkan akses tidak sah ke sistem dan data sensitif.
Information Disclosure - Sensitive Information in URL	Informasi sensitif yang ditampilkan di URL dapat diakses oleh pihak ketiga melalui log server, cache browser, atau alat monitoring jaringan
Information Disclosure - Debug Error Messages	Pesan error debug dapat memberikan informasi rinci tentang sistem dan konfigurasi kepada penyerang, memfasilitasi eksploitasi lebih lanjut.

Kerentanan	Potensi
Application Error Disclosure	Pengungkapan pesan error aplikasi dapat membantu penyerang dalam melakukan serangan yang lebih canggih dengan memanfaatkan informasi yang diberikan.
Server Leaks Version Information via "Server" HTTP *Response*	Penyerang dapat menggunakan informasi versi server untuk mencari dan mengeksploitasi kerentanan yang diketahui terkait versi tersebut.
Server Leaks Version Information	Memberikan informasi rinci tentang versi perangkat lunak yang digunakan kepada penyerang, yang dapat digunakan untuk merancang serangan spesifik.
Uncommon header 'content-security-policy' found	Penyerang dapat mencoba menembus kebijakan yang tidak umum dan mungkin tidak sepenuhnya dikonfigurasi dengan benar.
Uncommon header 'x-xss-protection' found	Kebijakan yang tidak lazim atau salah konfigurasi dapat menciptakan celah bagi serangan XSS.
CGI *Directories Found*	Direktori CGI dapat mengandung skrip yang rentan yang bisa dieksploitasi oleh penyerang untuk mendapatkan akses tidak sah atau menjalankan perintah berbahaya.
Potential vulnerabilities in multiple CGI *scripts*	Skrip CGI yang rentan dapat menjadi titik masuk bagi penyerang untuk menyusupi sistem dan mencuri data atau merusak sistem.
Buffer Overflow vulnerabilities	Penyerang dapat mengeksploitasi kerentanan *buffer overflow* untuk menjalankan kode berbahaya, yang dapat mengakibatkan kerusakan sistem atau akses tidak sah.

Kerentanan	Potensi
Open Ports (80/tcp, 443/tcp)	*Port* yang terbuka dapat digunakan oleh penyerang untuk melakukan pengintaian atau melancarkan serangan tertentu seperti DDoS atau serangan eksploitasi layanan.
EPrints 3.4.4	Versi perangkat lunak yang diketahui dan tidak diperbarui dapat mengandung kerentanan yang bisa dieksploitasi oleh penyerang.
SSL *Certificate Details*	Sertifikat SSL yang tidak valid atau salah konfigurasi dapat menyebabkan ketidakpercayaan pengguna dan rentan terhadap serangan MITM
OS *Detection*	Informasi sistem operasi yang terdeteksi dapat digunakan oleh penyerang untuk menargetkan serangan spesifik terhadap OS tersebut.
Traceroute Results	Informasi jalur jaringan yang terungkap dapat membantu penyerang dalam merencanakan serangan jaringan yang lebih efektif.
HTTP *Methods Supported*	Metode HTTP yang tidak aman atau tidak diperlukan seperti PUT atau DELETE dapat memberikan celah bagi penyerang untuk memodifikasi atau menghapus data.

Berdasarkan Tabel 4.17 potensi-potensi yang dapat ditimbulkan oleh celah keamanan website Repository Unjaya sudah sepantasnya untuk mendapatkan perhatian khusus dari pihak pengelola untuk meminimalisir terjadinya serangan dari pihak-pihak yang tidak bertanggung jawab.