Rakamin | Kampus Merdeka INDONESIA JAYA

Homework Week 11

IT Security Fundamentals

ByteSquad
Gede Verel Aditya Setiabudi
Tarisha Zhafira
Muhammad Raditya Nur Aziz
Ida Bagus Putu Basma Yoga
Bunga Anggun Chintamy
Muhammad Abigail Anargya
Yusma Cantika Parhati
Ida Ayu Tri Sabina Putri
Egydia Alfariza Ramadhani
Atqiya Trianda Putra Anugrah

Mentor: Jhordy Wong Abuhasan

Anggota Kelompok

Ida Bagus Putu Basma Yoga

Product Manager

Rakamin Academy

Bunga Anggun Chintamy

UI/UX

Rakamin Academy

Ida Ayu Tri Sabina Putri

UI/UX

Rakamin Academy

Tarisha Zhafira

Front-End

Rakamin Academy

Egydia Alfariza Ramadhani

Front-End

Rakamin Academy

Atqiya Trianda Putra Anugrah

Backend

Rakamin Academy

Muhammad Raditya Nur Aziz

Backend

Rakamin Academy

Muhammad Abigail Anargya

Data Analyst

Rakamin Academy

Yusma Cantika Parhati

Data Analyst

Rakamin Academy

Gede Verel Aditya Setiabudi

Q/A

Rakamin Academy

Soal Homework - IT Security Fundamentals

Pilihan Homework Ke-2

Berdasarkan yang telah diajarkan tentang penggunaan **Nessus** sebagai salah satu **tools Vulnerability Assessment**, lakukan:

1. **Scan aplikasi** yang telah kalian buat pada **Final Project** kalian **secara berkelompok**.

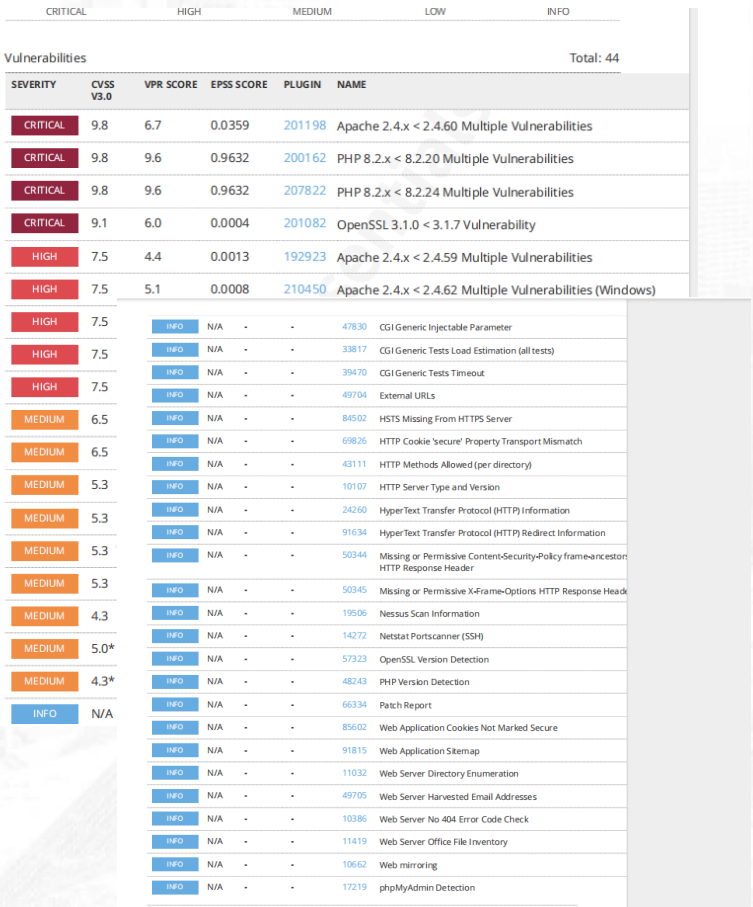
1. **Jelaskan temuan kalian** pada **dokumen tersebut**!

Link Homework - IT Security Fundamentals

Pilihan Homework Ke-2

Link Homework : https://drive.google.com/drive/folders/1hbXT3EZ71m-v_5Gi61sRppxf0RtIHWE4?usp=drive_link

Scan Nessus



CRITICAL HIGH MEDIUM LOW INFO

Vulnerabilities Total: 44

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	0.0359	201198	Apache 2.4.x < 2.4.60 Multiple Vulnerabilities
CRITICAL	9.8	9.6	0.9632	200162	PHP 8.2.x < 8.2.20 Multiple Vulnerabilities
CRITICAL	9.8	9.6	0.9632	207822	PHP 8.2.x < 8.2.24 Multiple Vulnerabilities
CRITICAL	9.1	6.0	0.0004	201082	OpenSSL 3.1.0 < 3.1.7 Vulnerability
HIGH	7.5	4.4	0.0013	192923	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
HIGH	7.5	5.1	0.0008	210450	Apache 2.4.x < 2.4.62 Multiple Vulnerabilities (Windows)
HIGH	7.5				
HIGH	7.5				
HIGH	7.5				
MEDIUM	6.5				
MEDIUM	6.5				
MEDIUM	5.3				
MEDIUM	5.3				
MEDIUM	5.3				
MEDIUM	5.3				
MEDIUM	4.3				
MEDIUM	5.0*				
MEDIUM	4.3*				
INFO	N/A				

INFO	N/A	-	-	47830	CGI Generic Injectable Parameter
INFO	N/A	-	-	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	-	-	39470	CGI Generic Tests Timeout
INFO	N/A	-	-	49704	External URLs
INFO	N/A	-	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	-	69826	HTTP Cookie 'secure' Property Transport Mismatch
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	91634	HyperText Transfer Protocol (HTTP) Redirect Information
INFO	N/A	-	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	-	50345	Missing or Permissive X-Frame-Options HTTP Response Head
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	14272	Netstat Portscanner (SSH)
INFO	N/A	-	-	57323	OpenSSL Version Detection
INFO	N/A	-	-	48243	PHP Version Detection
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	85602	Web Application Cookies Not Marked Secure
INFO	N/A	-	-	91815	Web Application Sitemap
INFO	N/A	-	-	11032	Web Server Directory Enumeration
INFO	N/A	-	-	49705	Web Server Harvested Email Addresses
INFO	N/A	-	-	10386	Web Server No 404 Error Code Check
INFO	N/A	-	-	11419	Web Server Office File Inventory
INFO	N/A	-	-	10662	Web mirroring
INFO	N/A	-	-	17219	phpMyAdmin Detection

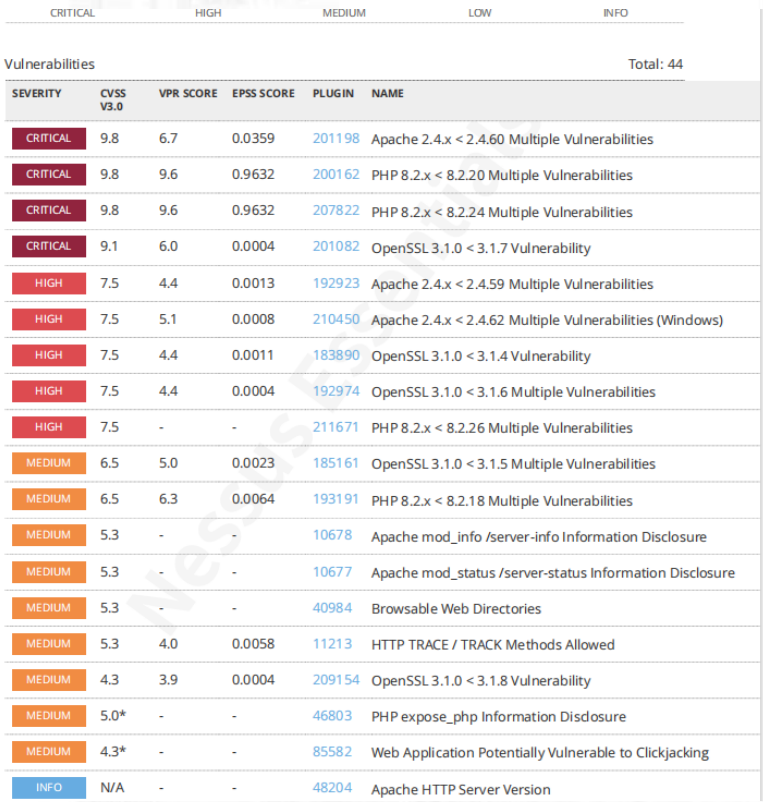
Distribusi Kerentanan

- Kritis: 4 kerentanan
- Tinggi: 5 kerentanan
- Menengah: 9 kerentanan
- Rendah: 0 kerentanan
- Informasi: 26 temuan Total: 44 temuan

Kerentanan Kritis (Prioritas Tertinggi)

1. Beberapa Kerentanan Apache 2.4.x (CVSS 9.8)
2. Beberapa Kerentanan PHP 8.2.x
    - Ditemukan dua masalah berbeda pada PHP versi < 8.2.20 dan < 8.2.24
    - Keduanya memiliki skor CVSS 9.8 dan skor EPSS tinggi (0.9632)
3. Kerentanan OpenSSL 3.1.0 (CVSS 9.1)

Scan Nessus



CRITICAL HIGH MEDIUM LOW INFO

Vulnerabilities Total: 44

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	0.0359	201198	Apache 2.4.x < 2.4.60 Multiple Vulnerabilities
CRITICAL	9.8	9.6	0.9632	200162	PHP 8.2.x < 8.2.20 Multiple Vulnerabilities
CRITICAL	9.8	9.6	0.9632	207822	PHP 8.2.x < 8.2.24 Multiple Vulnerabilities
CRITICAL	9.1	6.0	0.0004	201082	OpenSSL 3.1.0 < 3.1.7 Vulnerability
HIGH	7.5	4.4	0.0013	192923	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
HIGH	7.5	5.1	0.0008	210450	Apache 2.4.x < 2.4.62 Multiple Vulnerabilities (Windows)
HIGH	7.5	4.4	0.0011	183890	OpenSSL 3.1.0 < 3.1.4 Vulnerability
HIGH	7.5	4.4	0.0004	192974	OpenSSL 3.1.0 < 3.1.6 Multiple Vulnerabilities
HIGH	7.5	-	-	211671	PHP 8.2.x < 8.2.26 Multiple Vulnerabilities
MEDIUM	6.5	5.0	0.0023	185161	OpenSSL 3.1.0 < 3.1.5 Multiple Vulnerabilities
MEDIUM	6.5	6.3	0.0064	193191	PHP 8.2.x < 8.2.18 Multiple Vulnerabilities
MEDIUM	5.3	-	-	10678	Apache mod_info /server-info Information Disclosure
MEDIUM	5.3	-	-	10677	Apache mod_status /server-status Information Disclosure
MEDIUM	5.3	-	-	40984	Browsable Web Directories
MEDIUM	5.3	4.0	0.0058	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	4.3	3.9	0.0004	209154	OpenSSL 3.1.0 < 3.1.8 Vulnerability
MEDIUM	5.0*	-	-	46803	PHP expose_php Information Disclosure
MEDIUM	4.3*	-	-	85582	Web Application Potentially Vulnerable to Clickjacking
INFO	N/A	-	-	48204	Apache HTTP Server Version

Risiko Tinggi

1. Beberapa kerentanan Apache (versi < 2.4.59 dan < 2.4.62)
2. Beberapa kerentanan OpenSSL di versi 3.1.0
3. Kerentanan PHP 8.2.x (versi < 8.2.26)

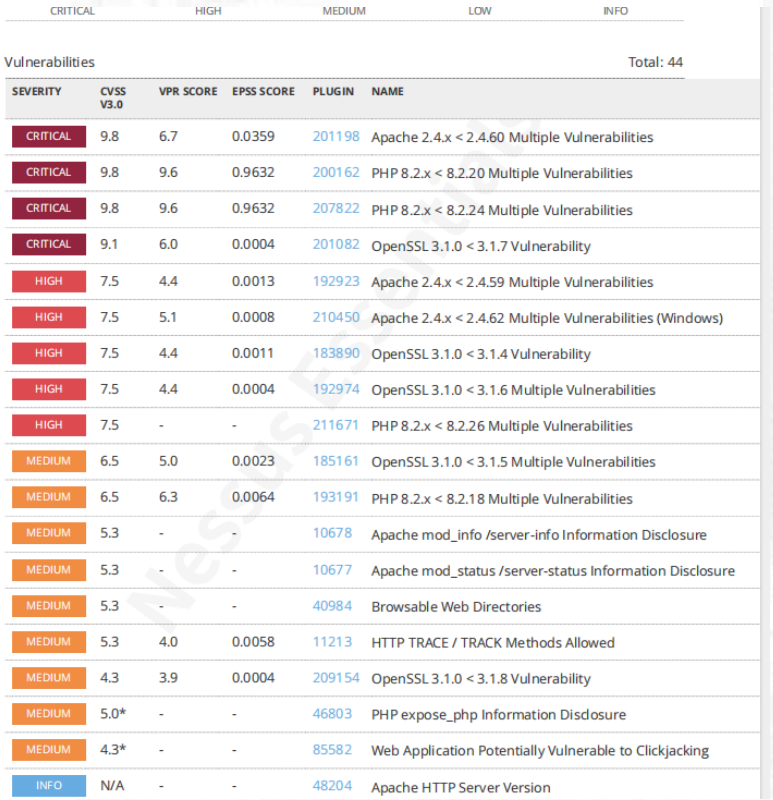
Risiko Menengah yang Penting

1. Masalah Kebocoran Informasi:
   - Terekspos nya Apache mod_info
   - Terekspos nya Apache mod_status
   - Kebocoran informasi PHP expose_php
2. Masalah Konfigurasi Keamanan:
   - Direktori web yang dapat dijelajahi
   - Metode HTTP TRACE/TRACK diperbolehkan
   - Potensi kerentanan clickjacking

Masalah Konfigurasi Utama

1. Header Keamanan yang Hilang:
   - HSTS belum diimplementasikan
   - Content-Security-Policy hilang atau terlalu permisif
   - X-Frame-Options hilang atau terlalu permisif
2. Keamanan Cookie:
   - Konfigurasi cookie tidak aman
   - Ketidaksesuaian keamanan transport

Scan Nessus



CRITICAL HIGH MEDIUM LOW INFO

Vulnerabilities Total: 44

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	0.0359	201198	Apache 2.4.x < 2.4.60 Multiple Vulnerabilities
CRITICAL	9.8	9.6	0.9632	200162	PHP 8.2.x < 8.2.20 Multiple Vulnerabilities
CRITICAL	9.8	9.6	0.9632	207822	PHP 8.2.x < 8.2.24 Multiple Vulnerabilities
CRITICAL	9.1	6.0	0.0004	201082	OpenSSL 3.1.0 < 3.1.7 Vulnerability
HIGH	7.5	4.4	0.0013	192923	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
HIGH	7.5	5.1	0.0008	210450	Apache 2.4.x < 2.4.62 Multiple Vulnerabilities (Windows)
HIGH	7.5	4.4	0.0011	183890	OpenSSL 3.1.0 < 3.1.4 Vulnerability
HIGH	7.5	4.4	0.0004	192974	OpenSSL 3.1.0 < 3.1.6 Multiple Vulnerabilities
HIGH	7.5	-	-	211671	PHP 8.2.x < 8.2.26 Multiple Vulnerabilities
MEDIUM	6.5	5.0	0.0023	185161	OpenSSL 3.1.0 < 3.1.5 Multiple Vulnerabilities
MEDIUM	6.5	6.3	0.0064	193191	PHP 8.2.x < 8.2.18 Multiple Vulnerabilities
MEDIUM	5.3	-	-	10678	Apache mod_info /server-info Information Disclosure
MEDIUM	5.3	-	-	10677	Apache mod_status /server-status Information Disclosure
MEDIUM	5.3	-	-	40984	Browsable Web Directories
MEDIUM	5.3	4.0	0.0058	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	4.3	3.9	0.0004	209154	OpenSSL 3.1.0 < 3.1.8 Vulnerability
MEDIUM	5.0*	-	-	46803	PHP expose_php Information Disclosure
MEDIUM	4.3*	-	-	85582	Web Application Potentially Vulnerable to Clickjacking
INFO	N/A	-	-	48204	Apache HTTP Server Version

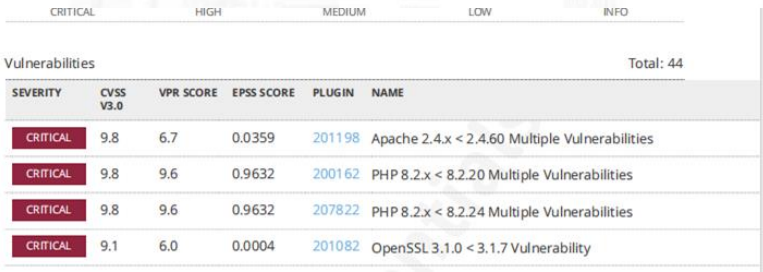
Rekomendasi Tindakan Prioritas

- Perbarui PHP ke versi 8.2.24 atau lebih baru
- Perbarui Apache ke versi 2.4.62 atau lebih baru
- Perbarui OpenSSL ke versi 3.1.8
- Nonaktifkan modul Apache yang tidak perlu (mod_info, mod_status)
- Terapkan header keamanan (HSTS, CSP, X-Frame-Options)
- Amankan konfigurasi cookie
- Nonaktifkan metode HTTP TRACE/TRACK
- Tinjau dan batasi direktori yang dapat dijelajahi
- Terapkan penanganan error 404 yang tepat

Dampak Potensial jika Tidak Ditangani

1. Kerentanan Kritis:
   - Potensi serangan remote code execution
   - Kebocoran data sensitif
   - Peretasan sistem
2. Risiko Tinggi:
   - Serangan man-in-the-middle
   - Pencurian sesi pengguna
   - Manipulasi data aplikasi
3. Risiko Menengah:
   - Pengumpulan informasi oleh penyerang
   - Serangan social engineering
   - Penurunan performa sistem

Scan Nessus Detail



CRITICAL | HIGH | MEDIUM | LOW | INFO

Vulnerabilities — Total: 44

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	0.0359	201198	Apache 2.4.x < 2.4.60 Multiple Vulnerabilities
CRITICAL	9.8	9.6	0.9632	200162	PHP 8.2.x < 8.2.20 Multiple Vulnerabilities
CRITICAL	9.8	9.6	0.9632	207822	PHP 8.2.x < 8.2.24 Multiple Vulnerabilities
CRITICAL	9.1	6.0	0.0004	201082	OpenSSL 3.1.0 < 3.1.7 Vulnerability

Kerentanan Kritis (Prioritas Tertinggi)

1. **Apache 2.4.x (CVSS 9.8)**
   - **Deskripsi**: Versi Apache HTTP Server yang terinstal adalah 2.4.58, yang rentan terhadap beberapa kelemahan seperti:
     - Null pointer dereference menyebabkan crash server. (CVE-2024-36387)
     - SSRF memungkinkan kebocoran NTLM hash. (CVE-2024-38472)
     - Kerentanan bypass autentikasi melalui mod_proxy. (CVE-2024-38473)
2. **PHP 8.2.x**
   - **Deskripsi**: Versi PHP yang terinstal adalah 8.2.12, rentan terhadap eksploitasi termasuk:
     - Eksekusi kode arbitrer akibat misinterpretasi karakter di command line. (CVE-2024-4577)
     - Validasi URL yang salah memungkinkan URL palsu. (CVE-2024-5458)
3. **OpenSSL 3.1.0 (CVSS 9.1)**
   - **Deskripsi**: Versi OpenSSL 3.1.3 mengalami:
     - Buffer overread menyebabkan potensi kebocoran data hingga 255 byte. (CVE-2024-5535)

Scan Nessus Detail

HIGH	7.5	4.4	0.0013	192923	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
HIGH	7.5	5.1	0.0008	210450	Apache 2.4.x < 2.4.62 Multiple Vulnerabilities (Windows)
HIGH	7.5	4.4	0.0011	183890	OpenSSL 3.1.0 < 3.1.4 Vulnerability
HIGH	7.5	4.4	0.0004	192974	OpenSSL 3.1.0 < 3.1.6 Multiple Vulnerabilities
HIGH	7.5	-	-	211671	PHP 8.2.x < 8.2.26 Multiple Vulnerabilities

Risiko Tinggi

1. **Apache < 2.4.59 dan < 2.4.62**
   - **Deskripsi**: Kerentanan pada versi Apache yang lebih rendah termasuk:
     - Splitting respon HTTP untuk manipulasi desinkronisasi. (CVE-2024-24795)
     - SSRF melalui NTLM hash di mod_rewrite. (CVE-2024-40898)
2. **OpenSSL 3.1.0 (Berbagai Kerentanan)**
   - **Deskripsi**: Masalah unbounded memory growth dan use-after-free pada TLS. (CVE-2024-2511, CVE-2024-4741)
3. **PHP 8.2.x (versi < 8.2.26)**
   - **Deskripsi**: Kelemahan pada validasi URL dan potensi eksekusi kode arbitrer.

Scan Nessus Detail

MEDIUM	6.5	5.0	0.0023	185161	OpenSSL 3.1.0 < 3.1.5 Multiple Vulnerabilities
MEDIUM	6.5	6.3	0.0064	193191	PHP 8.2.x < 8.2.18 Multiple Vulnerabilities
MEDIUM	5.3	-	-	10678	Apache mod_info /server-info Information Disclosure
MEDIUM	5.3	-	-	10677	Apache mod_status /server-status Information Disclosure
MEDIUM	5.3	-	-	40984	Browsable Web Directories
MEDIUM	5.3	4.0	0.0058	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	4.3	3.9	0.0004	209154	OpenSSL 3.1.0 < 3.1.8 Vulnerability
MEDIUM	5.0*	-	-	46803	PHP expose_php Information Disclosure
MEDIUM	4.3*	-	-	85582	Web Application Potentially Vulnerable to Clickjacking

Risiko Menengah yang Penting

1. **Kebocoran Informasi**
   - Modul Apache seperti `mod_info` dan `mod_status` terekspos.
   - Fitur PHP `expose_php` diaktifkan.
2. **Masalah Konfigurasi Keamanan**
   - Direktori web dapat dijelajahi.
   - HTTP TRACE/TRACK diaktifkan.
   - Potensi clickjacking akibat header keamanan hilang.

Scan Nessus Detail

CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 44

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	0.0359	201198	Apache 2.4.x < 2.4.60 Multiple Vulnerabilities
CRITICAL	9.8	9.6	0.9632	200162	PHP 8.2.x < 8.2.20 Multiple Vulnerabilities
CRITICAL	9.8	9.6	0.9632	207822	PHP 8.2.x < 8.2.24 Multiple Vulnerabilities
CRITICAL	9.1	6.0	0.0004	201082	OpenSSL 3.1.0 < 3.1.7 Vulnerability
HIGH	7.5	4.4	0.0013	192923	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
HIGH	7.5	5.1	0.0008	210450	Apache 2.4.x < 2.4.62 Multiple Vulnerabilities (Windows)
HIGH	7.5	4.4	0.0011	183890	OpenSSL 3.1.0 < 3.1.4 Vulnerability
HIGH	7.5	4.4	0.0004	192974	OpenSSL 3.1.0 < 3.1.6 Multiple Vulnerabilities
HIGH	7.5	-	-	211671	PHP 8.2.x < 8.2.26 Multiple Vulnerabilities
MEDIUM	6.5	5.0	0.0023	185161	OpenSSL 3.1.0 < 3.1.5 Multiple Vulnerabilities
MEDIUM	6.5	6.3	0.0064	193191	PHP 8.2.x < 8.2.18 Multiple Vulnerabilities
MEDIUM	5.3	-	-	10678	Apache mod_info /server-info Information Disclosure
MEDIUM	5.3	-	-	10677	Apache mod_status /server-status Information Disclosure
MEDIUM	5.3	-	-	40984	Browsable Web Directories
MEDIUM	5.3	4.0	0.0058	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	4.3	3.9	0.0004	209154	OpenSSL 3.1.0 < 3.1.8 Vulnerability
MEDIUM	5.0*	-	-	46803	PHP expose_php Information Disclosure
MEDIUM	4.3*	-	-	85582	Web Application Potentially Vulnerable to Clickjacking
INFO	N/A	-	-	48204	Apache HTTP Server Version

Masalah Konfigurasi Utama

1. **Header Keamanan yang Hilang**
   - Header seperti HSTS, Content-Security-Policy, dan X-Frame-Options tidak diterapkan.
2. **Keamanan Cookie**
   - Konfigurasi cookie tidak aman, memungkinkan pencurian sesi..
3. **Keamanan Transport**
   - Ketidaksesuaian pada implementasi HTTPS menyebabkan penurunan keamanan.

Scan Aplikasi ZAP

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	4
Informational	3

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	2
Missing Anti-clickjacking Header	Medium	1
Cookie No HttpOnly Flag	Low	1
Cross-Domain JavaScript Source File Inclusion	Low	3
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	2
X-Content-Type-Options Header Missing	Low	2
Information Disclosure - Suspicious Comments	Informational	2
Modern Web Application	Informational	1
Session Management Response Identified	Informational	5

1. Summary of Alerts

Ringkasan hasil temuan kerentanan berdasarkan tingkat risiko menggunakan ZAP:

- **High (Tinggi)**: **0 alert**
  - Tidak ditemukan kerentanan dengan tingkat risiko tinggi.
- **Medium (Sedang)**: **2 alert**
  - Terdapat dua kerentanan dengan tingkat risiko sedang, yaitu:
    - *Content Security Policy (CSP) Header Not Set* (2 instance).
    - *Missing Anti-clickjacking Header* (1 instance).
- **Low (Rendah)**: **4 alert**
  - Ada empat kerentanan risiko rendah, meliputi:
    - Cookie tanpa *HttpOnly flag*.
    - Cross-Domain JavaScript Source File Inclusion (3 instance).
    - Server Leaks Information via *X-Powered-By HTTP Header* (2 instance).
    - *X-Content-Type-Options Header Missing* (2 instance).
- **Informational (Informasi)**: **3 alert**
  - Temuan ini memberikan informasi tambahan terkait potensi risiko atau kondisi aplikasi:
    - *Suspicious Comments* dalam kode (2 instance).
    - Indikasi aplikasi modern (*Modern Web Application*).
    - *Session Management Token* terdeteksi (5 instance).

Scan Aplikasi ZAP

Medium	Content Security Policy (CSP) Header Not Set
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:8000/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	2
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

2. Tingkat Resiko - Medium

Kerentanan yang memiliki risiko moderat dan berpotensi membahayakan aplikasi, tetapi biasanya membutuhkan kondisi tertentu untuk dieksploitasi oleh penyerang.

a. Content Security Policy (CSP) Header Not Set

- **Deskripsi**: Header Content-Security-Policy (CSP) tidak diatur, sehingga aplikasi rentan terhadap serangan ***Cross-Site Scripting (XSS)*** dan ***data injection***. CSP adalah sebuah layer untuk mendeteksi dan mengurangi serangan seperi ***XSS*** dan *data* ***injection***.
- **Solusi**: Tambahkan header **Content-Security-Policy** di server untuk membatasi sumber konten yang diizinkan.
- **Instance**: 2 instance ditemukan. Dua halaman atau respons HTTP yang tidak memiliki header *Content-Security-Policy*.
- **CWE Id**: 693 (*Improper Control of Content Generation*). ***Common Weakness Enumeration (CWE)*** yang mengacu pada kelemahan dalam pengendalian atau pengaturan konten yang dihasilkan oleh aplikasi untuk membuka serangan ***Cross-Site Scripting (XSS)***, ***Injection Attack, dan Clickjacking.***

Scan Aplikasi ZAP

Medium	Missing Anti-clickjacking Header
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	
Other Info	
Instances	1
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

2. Tingkat Resiko - Medium

Kerentanan yang memiliki risiko moderat dan berpotensi membahayakan aplikasi, tetapi biasanya membutuhkan kondisi tertentu untuk dieksploitasi oleh penyerang.

b. Missing Anti-clickjacking Header

- **Deskripsi**: Halaman tidak dilindungi dari serangan ***Clickjacking***, jenis serangan di mana penyerang menipu pengguna untuk mengklik sesuatu di sebuah situs web yang berbeda dari apa yang mereka kira. Header seperti “**X-Frame-Options”** atau **“frame-ancestors”** tidak disetel.
- **Solusi**: Tambahkan header “**X-Frame-Options”** dengan nilai “**DENY”** atau “**SAMEORIGIN.”**
- **Instance**: 2 instance ditemukan. Dua halaman atau respons HTTP yang tidak memiliki header *Content-Security-Policy*.
- **CWE Id**: 693 (*Improper Control of Content Generation*). ***Common Weakness Enumeration (CWE)*** yang mengacu pada kelemahan dalam pengendalian atau pengaturan konten yang dihasilkan oleh aplikasi untuk membuka serangan ***Cross-Site Scripting (XSS)***, ***Injection Attack, dan Clickjacking.***

Scan Aplikasi ZAP

Low	Cookie No HttpOnly Flag

Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
Instances	1
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

Low	Cross-Domain JavaScript Source File Inclusion
Description	The page includes one or more script files from a third-party domain.
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	<script type="module" src="http://[::1]:5173/@vite/client"></script>
Other Info	
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	<script type="module" src="http://[::1]:5173/resources/js/app.jsx"></script>
Other Info	
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	<script type="module" src="http://[::1]:5173/resources/js/Pages/LandingPage.jsx"></script>
Other Info	
Instances	3
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017

3. Tingkat Resiko - Low

Kerentanan dengan dampak kecil yang sulit atau membutuhkan usaha besar untuk dieksploitasi. Risiko ini biasanya tidak langsung membahayakan aplikasi.

a. Cookie No HttpOnly Flag

- **Deskripsi**: Cookie diatur tanpa menggunakan **HttpOnly flag**. **HttpOnly flag** adalah atribut keamanan yang ditambahkan pada **cookie** untuk **mencegah akses** terhadap **cookie** tersebut oleh skrip di sisi klien, seperti JavaScript. Oleh karena itu, **Cookie** dapat diakses oleh **JavaScript**, meningkatkan **risiko *session hijacking*** jika ada skrip berbahaya.
- **Solusi**: Tambahkan atribut **HttpOnly** pada cookie.
- **Instance**: 1 instance ditemukan.

b. Cross-Domain JavaScript Source File Inclusion

- **Deskripsi**: **Skrip JavaScript** dimuat dari **sumber domain** yang **berbeda**, meningkatkan **risiko manipulasi** jika domain tersebut tidak terpercaya.
- **Solusi**: Pastikan hanya memuat skrip dari domain terpercaya.
- **Instance**: 3 instance ditemukan.

Scan Aplikasi ZAP

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

Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.3.11
Other Info	
URL	http://127.0.0.1:8000/sitemap.xml
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.3.11
Other Info	
Instances	2
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	https://owasp.org/www-project-we Web_Application_Security_Testin Fingerprint_Web_Application_Fra https://www.troyhunt.com/2012/02
CWE Id	200
WASC Id	13
Plugin Id	10037

Low	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://127.0.0.1:8000/robots.txt
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	2
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

3. Tingkat Resiko - Low

Kerentanan dengan dampak kecil yang sulit atau membutuhkan usaha besar untuk dieksploitasi. Risiko ini biasanya tidak langsung membahayakan aplikasi.

c. Server Leaks Information via "X-Powered-By" HTTP Response Header

- **Deskripsi**: Header **X-Powered-By** menunjukkan **informasi teknologi server**, seperti **versi PHP**, yang dapat dimanfaatkan oleh penyerang.
- **Solusi**: Hapus header **X-Powered-By** di konfigurasi server.
- **Instance**: 2 instance ditemukan.

d. X-Content-Type-Options Header Missing

- **Deskripsi**: Header ***X-Content-Type-Options*** tidak diatur, memungkinkan ***MIME-sniffing*** oleh browser yang dapat menyebabkan interpretasi konten yang tidak aman.
- **Solusi**: Tambahkan **header X-Content-Type-Options** dengan **nilai nosniff.**
- **Instance**: 2 instance ditemukan.

Scan Aplikasi ZAP

Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "<script type="module" > import RefreshRuntime from 'http://[::1]:5173/@react-refresh' RefreshRuntime.injectIntoGlobalHoo", see evidence field for the suspicious comment /snippet.
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "<script type="text/javascript">const Ziggy={"url":"http:\/\/127.0.0.1:8000","port":8000,"defaults":{},"routes":{"sanctum.csrf-co", see evidence field for the suspicious comment /snippet.
Instances	2
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10027

Informational	Modern Web Application
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	http://127.0.0.1:8000/
Method	GET
Attack	

4. Tingkat Resiko - Information

Temuan ini memberikan informasi tambahan tentang kondisi aplikasi yang tidak berbahaya secara langsung tetapi bisa menjadi indikasi potensi risiko.

a. Suspicious Comments

- **Deskripsi**: Ditemukan komentar mencurigakan dalam kode yang dapat memberikan petunjuk kepada penyerang.
- **Solusi**: Hapus komentar yang tidak perlu.
- **Instance**: 2 instance ditemukan.

b. Modern Web Application

- **Deskripsi**: Aplikasi teridentifikasi sebagai aplikasi modern berdasarkan pola skrip dan penggunaan Ajax.
- **Solusi**: Tidak ada langkah perbaikan, hanya informasi.

Scan Aplikasi ZAP

Informational	Session Management Response Identified
Description	The given response has been identified as containing a session management token. The 'Other
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	eyJpdiI6IjAvNGUvT285UHhsVUdNMXI1eUIzc2c9PSIsInZhbHVlIjoiMitWM3ViK3o4OFVtQms1Z
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	eyJpdiI6IlJFWVFQa1A2bFpDYStiZUY4VGVMQ1E9PSIsInZhbHVlIjoiaFhyYUZBL1ZkUmtZeHQ 3D
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	eyJpdiI6InZYd2VxVTVYOUVFV0VKY3c0SFlHRGc9PSIsInZhbHVlIjoiaS9QYmx0cFJScytUbnM
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	eyJpdiI6InZYd2VxVTVYOUVFV0VKY3c0SFlHRGc9PSIsInZhbHVlIjoiaS9QYmx0cFJScytUbnM
Other Info	cookie:laravel_session
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	eyJpdiI6IjFzNHBUYlgzbHlzelJzaHdyMmxJV2c9PSIsInZhbHVlIjoiUG8rd3cvUm4vN2hueWFhMF 3D
Other Info	cookie:XSRF-TOKEN
Instances	5
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id
CWE Id	
WASC Id	

Plugin Id	10112

4. Tingkat Resiko - Information

Temuan ini memberikan informasi tambahan tentang kondisi aplikasi yang tidak berbahaya secara langsung tetapi bisa menjadi indikasi potensi risiko.

c. Session Management Response Identified

- **Deskripsi**: Token ***Session Management*** terdeteksi dalam respons. ***Session Management*** proses pengelolaan sesi pengguna dalam aplikasi, terutama aplikasi berbasis web.
- **Solusi**: Hapus komentar yang tidak perlu.
- **Instance**: 2 instance ditemukan.

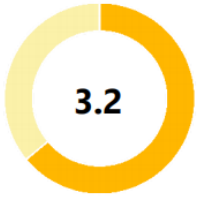
Scan SmartScanner

Target: **http://127.0.0.1:8443/**

Date: **Sun Nov 24 2024**

Found Issues: **30**

scan **finished** within **1' 32"** after **704** requests.



Risk

Issue Severity

Executive Summary

SmartScanner conducted a scan on 127.0.0.1:8443 to find security weaknesses and vulnerabilities. The scan took 1 minute and 32 seconds. After performing 704 requests, SmartScanner found 30 issues in which 6 of them have medium severity. The overall security risk of 127.0.0.1:8443 is 3.2 out of 5. To reduce the security risk, please fix the found issues as soon as possible. Technical details, as well as remediation of results, can be found in the following. *

* DISCLAIMER: This report is only limited to the results of SmartScanner findings.

Temuan Utama:

1. **Masalah dengan Keparahan Sedang:**
   - Cookie sesi tidak memiliki flag Secure.
   - Tidak ada pengalihan otomatis dari HTTP ke HTTPS.
   - HTTPS belum diimplementasikan.
2. **Masalah dengan Keparahan Rendah:**
   - Atribut *Subresource Integrity* (SRI) untuk sumber daya eksternal hilang.
   - Header keamanan yang hilang:
     - *Content-Security-Policy* (CSP).
     - *X-Frame-Options*.
   - Cookie tidak memiliki flag HttpOnly.
3. **Masalah Informasi:**
   - Sumber daya tidak direferensikan dan header seperti `X-Content-Type-Options` yang hilang.

Perbandingan Aplikasi

Nessus : Hasil scan lebih lengkap dan menyeluruh, Tetapi scan lumayan lama dan terkadang berat di pc

ZAP : memiliki waktu scan yang cepat, dan report paling mudah untuk dibaca juga dipahami, tetapi tidak selengkap nessus

SmartScanner : Waktu scan tercepat hanya 30 detik namun hasil tidak selengkap aplikasi lain

Thank you!

Raih Mimpi #TanpaBatas