Ryan Hanif Dwihandoyo
CS Assignment Day 12

1. Scope (Cakupan)

Penilaian keamanan ini difokuskan secara eksklusif pada aplikasi web yang dapat diakses pada URL berikut:

URL: http://testphp.veulnweb.com

Aset lain di luar URL tersebut tidak termasuk dalam cakupan pengujian ini.

2. Methodology (Metodologi)

Proses asesmen keamanan dilakukan dengan mengikuti metodologi standar yang mencakup beberapa fase. Berikut adalah kronologi aktivitas berdasarkan waktu pengambilan bukti (screenshot):

10:37 WIB - Fase 1: Konfigurasi & Penyiapan

Peramban (Mozilla Firefox) dikonfigurasi untuk melewatkan semua lalu lintas melalui local proxy OWASP ZAP di 127.0.0.1:8080 untuk intersepsi dan analisis.

10:39 WIB - Fase 2: Information Gathering

Melakukan penelusuran manual awal pada aplikasi testphp.vulnweb.com untuk memetakan struktur situs dan mengidentifikasi fungsionalitas utama seperti fitur pencarian.

10:48 WIB - Fase 3: Vulnerability Scanning & Manual Testing

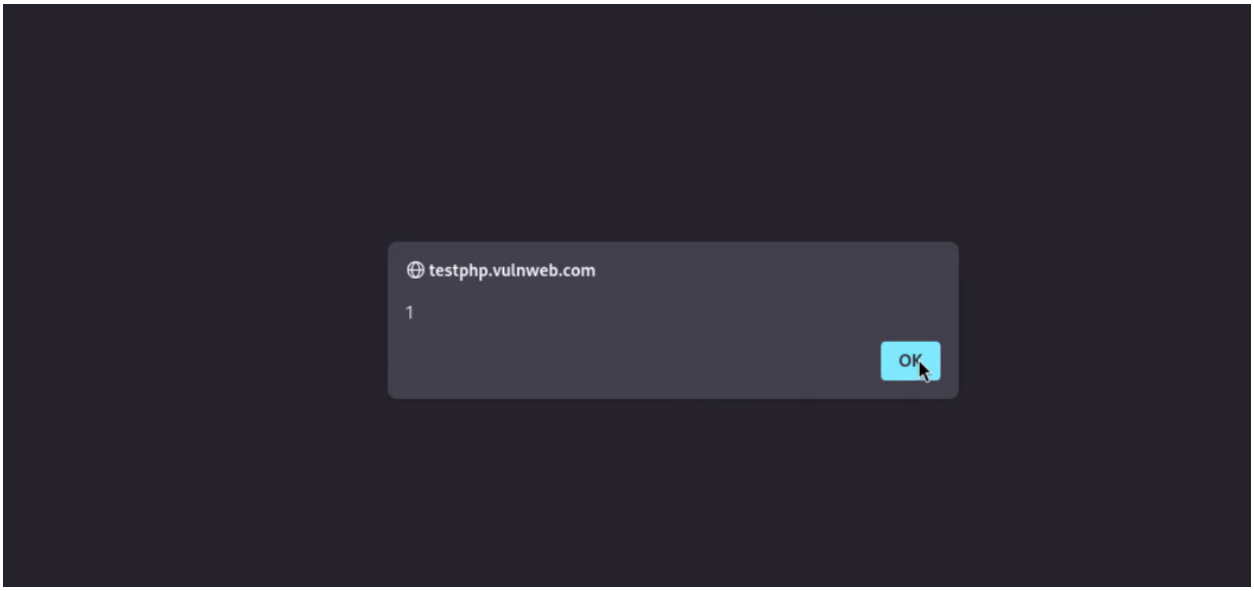
Fitur Active Scan pada OWASP ZAP diinisiasi untuk memindai kerentanan secara otomatis di seluruh situs. Selama pemindaian, dilakukan pengujian manual pada fungsionalitas pencarian untuk memverifikasi temuan.

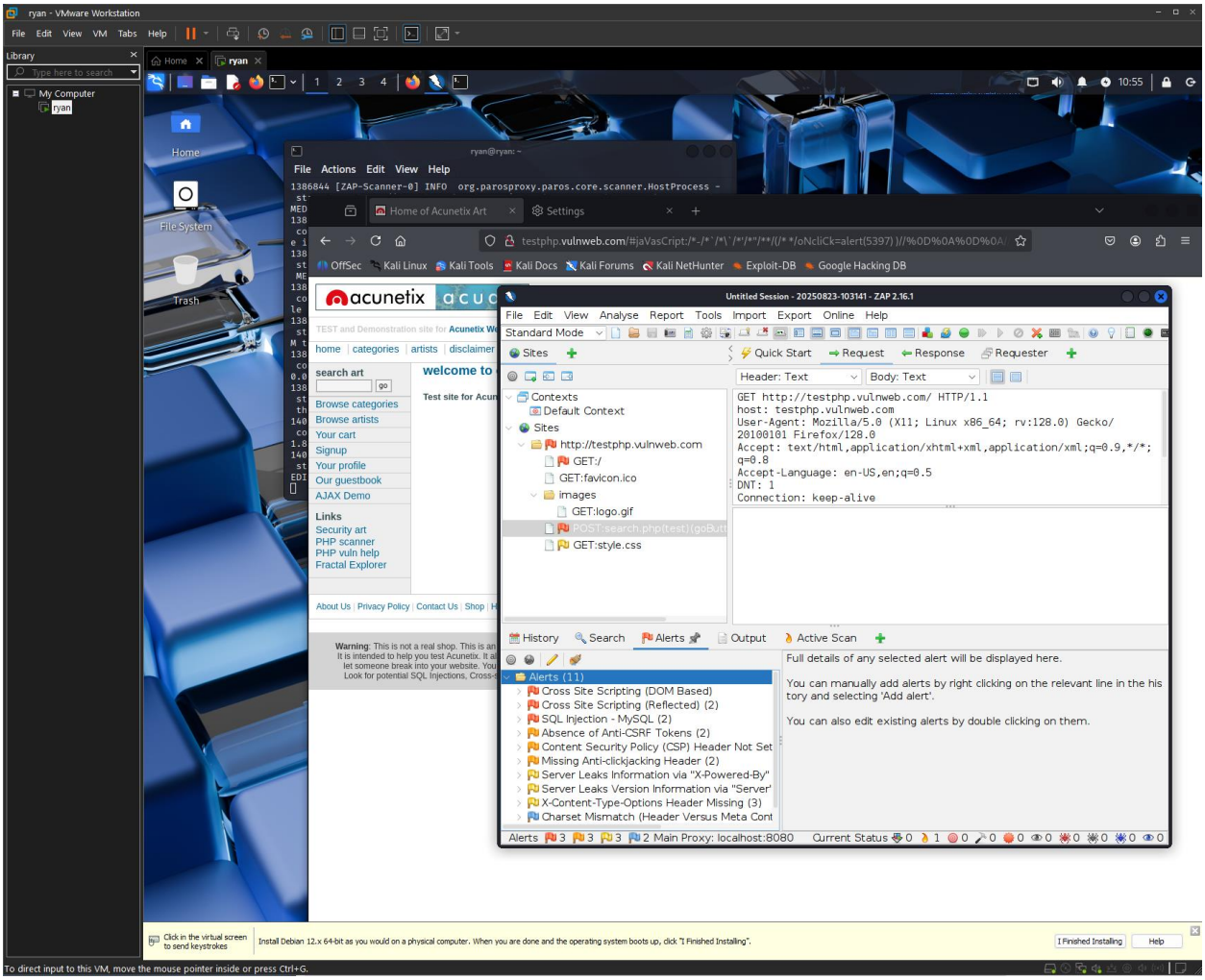
10:53 WIB - Fase 4: Exploitation & Verification

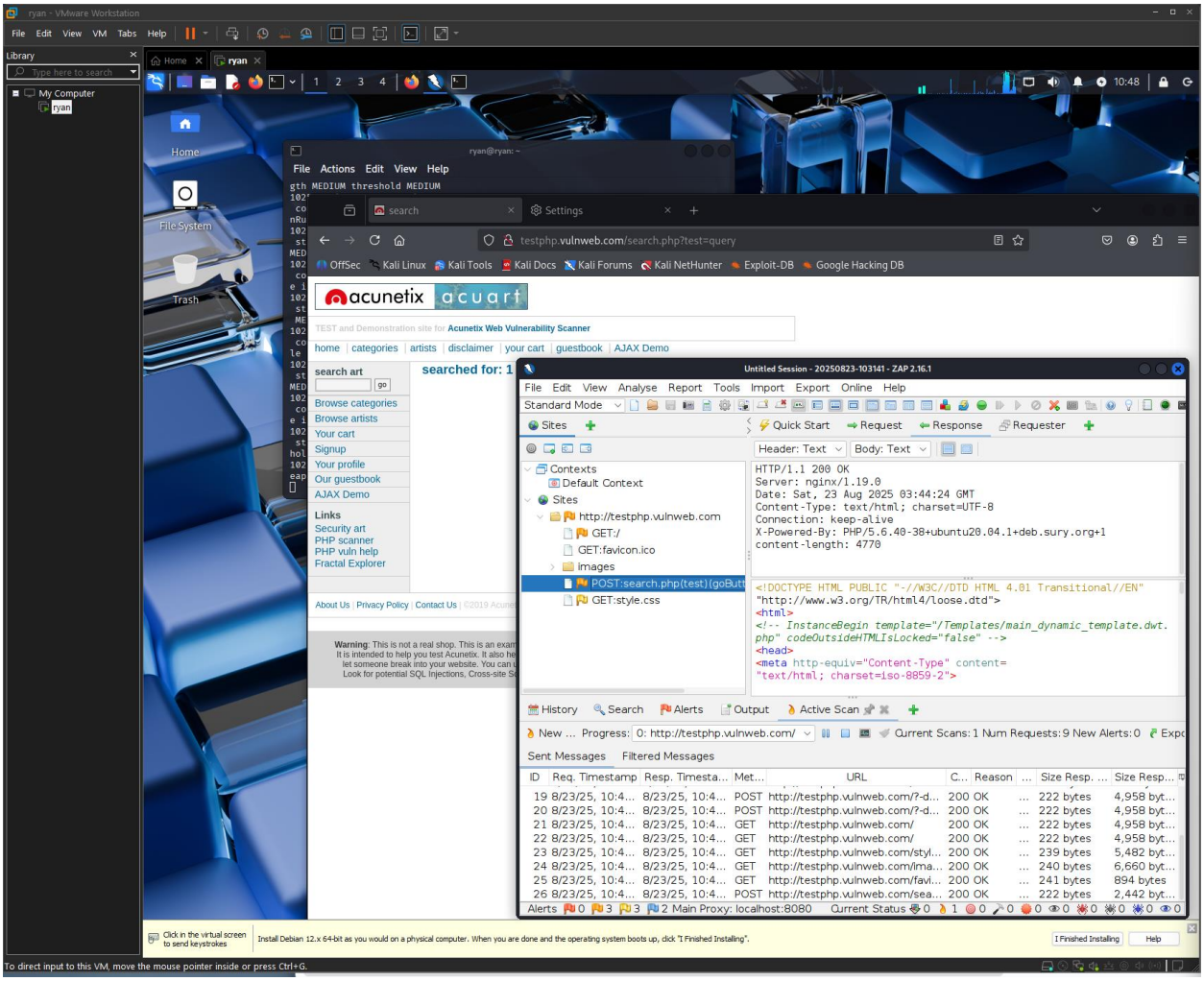
Kerentanan ***Cross-Site Scripting*** (XSS) yang teridentifikasi berhasil dieksploitasi secara manual untuk memvalidasi temuan dan membuktikan dampaknya.

10:55 WIB - Fase 5: Analisis & Pelaporan

Hasil akhir dari Active Scan dianalisis untuk mengidentifikasi semua kerentanan yang ditemukan.


testphp.vulnweb.com
1
OK


ryan - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
ryan
Home
File System
Trash
File Actions Edit View Help
1386844 [ZAP-Scanner-0] INFO org.parosproxy.paros.core.scanner.HostProcess -
Home of Acunetix Art
Settings
testphp.vulnweb.com/#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0D%0A/
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
acunetix
search art
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
Untitled Session - 20250823-103141 - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
http://testphp.vulnweb.com
GET:/
GET:favicon.ico
images
GET:logo.gif
POST:search.php(test)(goBut
GET:style.css
Header: Text
Body: Text
GET http://testphp.vulnweb.com/ HTTP/1.1
host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
DNT: 1
Connection: keep-alive
History
Search
Alerts
Output
Active Scan
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.
Alerts (11)
Cross Site Scripting (DOM Based)
Cross Site Scripting (Reflected) (2)
SQL Injection - MySQL (2)
Absence of Anti-CSRF Tokens (2)
Content Security Policy (CSP) Header Not Set
Missing Anti-clickjacking Header (2)
Server Leaks Information via "X-Powered-By"
Server Leaks Version Information via "Server"
X-Content-Type-Options Header Missing (3)
Charset Mismatch (Header Versus Meta Cont
Alerts 3 3 3 2 Main Proxy: localhost:8080 Current Status 0 1 0 0 0 0 0 0 0 0
Click in the virtual screen to send keystrokes
Install Debian 12.x 64-bit as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



3. Executive Summary (Ringkasan Eksekutif)

Sebuah pengujian keamanan (**VAPT**) telah dilakukan terhadap aplikasi web testphp.vulnweb.com untuk mengidentifikasi dan menilai potensi risiko keamanan. Hasil pengujian menemukan beberapa kerentanan dengan tingkat risiko Tinggi, termasuk SQL Injection yang dapat menyebabkan kebocoran data masif, dan Cross-Site Scripting (XSS) yang dapat digunakan untuk mengambil alih akun pengguna.

Ditemukan juga beberapa miskonfigurasi keamanan tingkat Sedang dan Rendah yang secara kolektif melemahkan postur keamanan aplikasi. Risiko bisnis utama dari temuan ini adalah potensi kebocoran data sensitif, kerugian reputasi, dan gangguan operasional.

Rekomendasi utama adalah agar tim pengembang segera memprioritaskan perbaikan untuk kerentanan berisiko tinggi dan menerapkan praktik pengkodean yang aman serta pengerasan konfigurasi server.

4. Tools (Peralatan yang Digunakan)

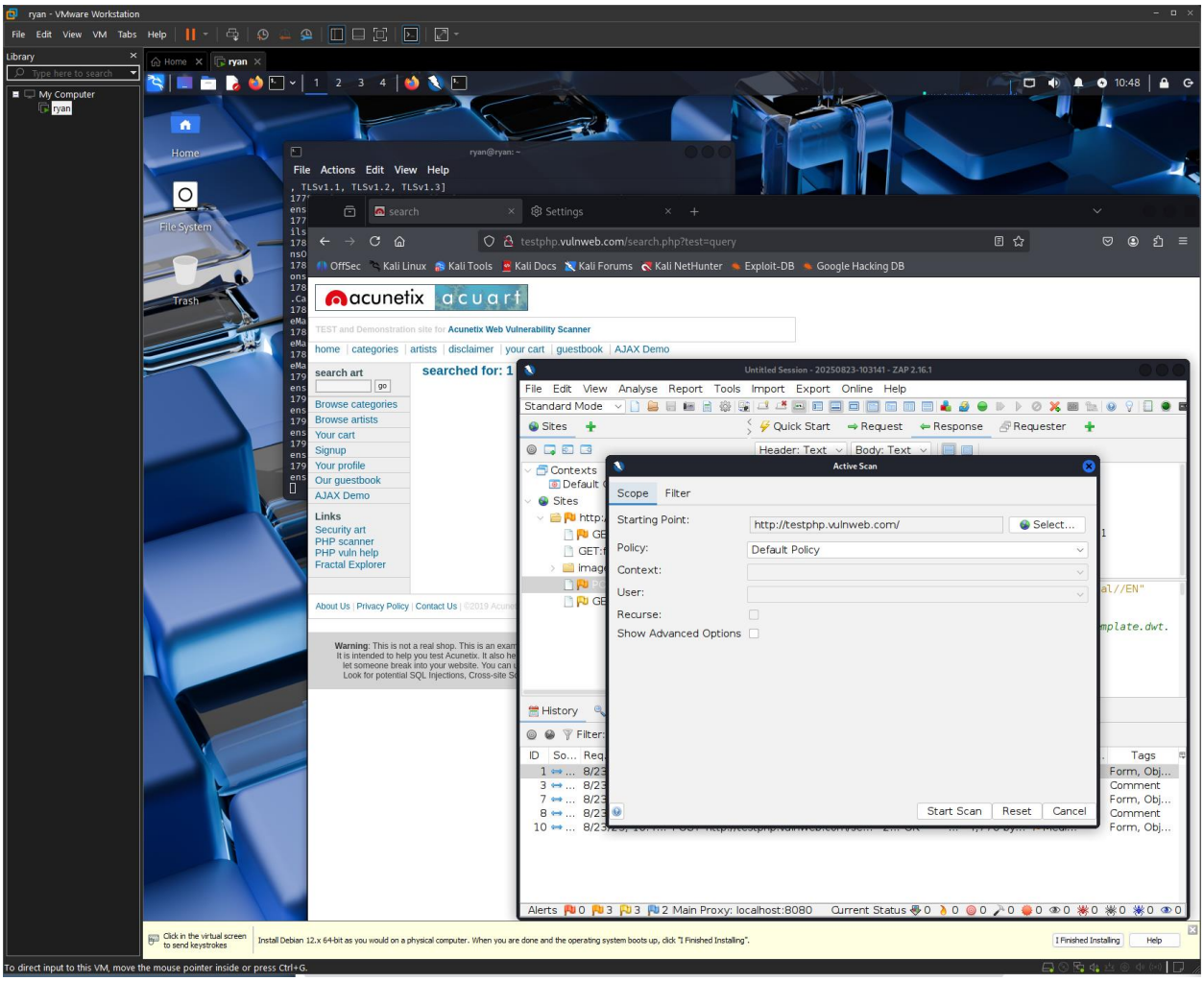
- OWASP Zed Attack Proxy (ZAP)

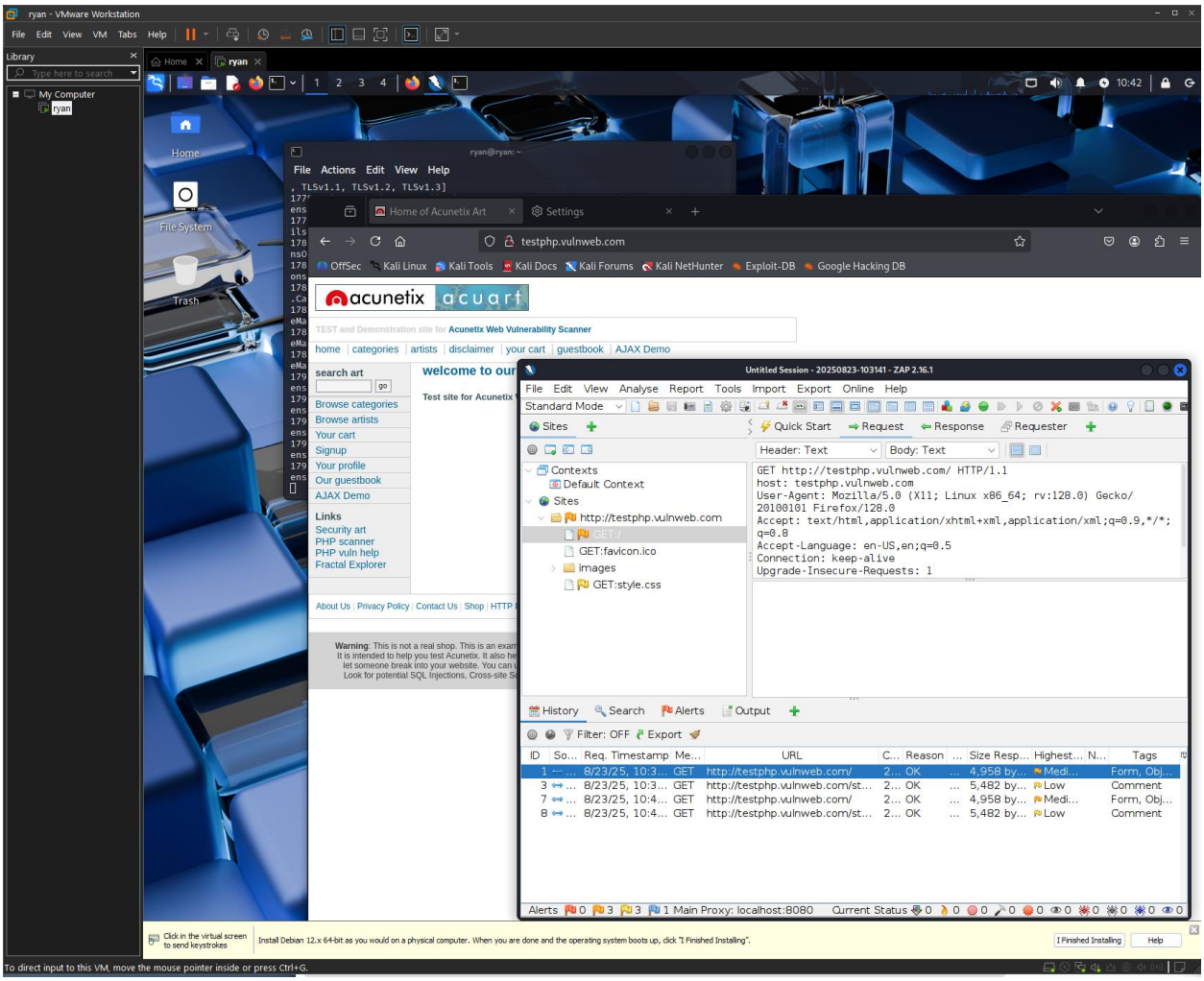
- Mozilla Firefox

- Kali Linux

- VMware Workstation

- CVSS Calculator





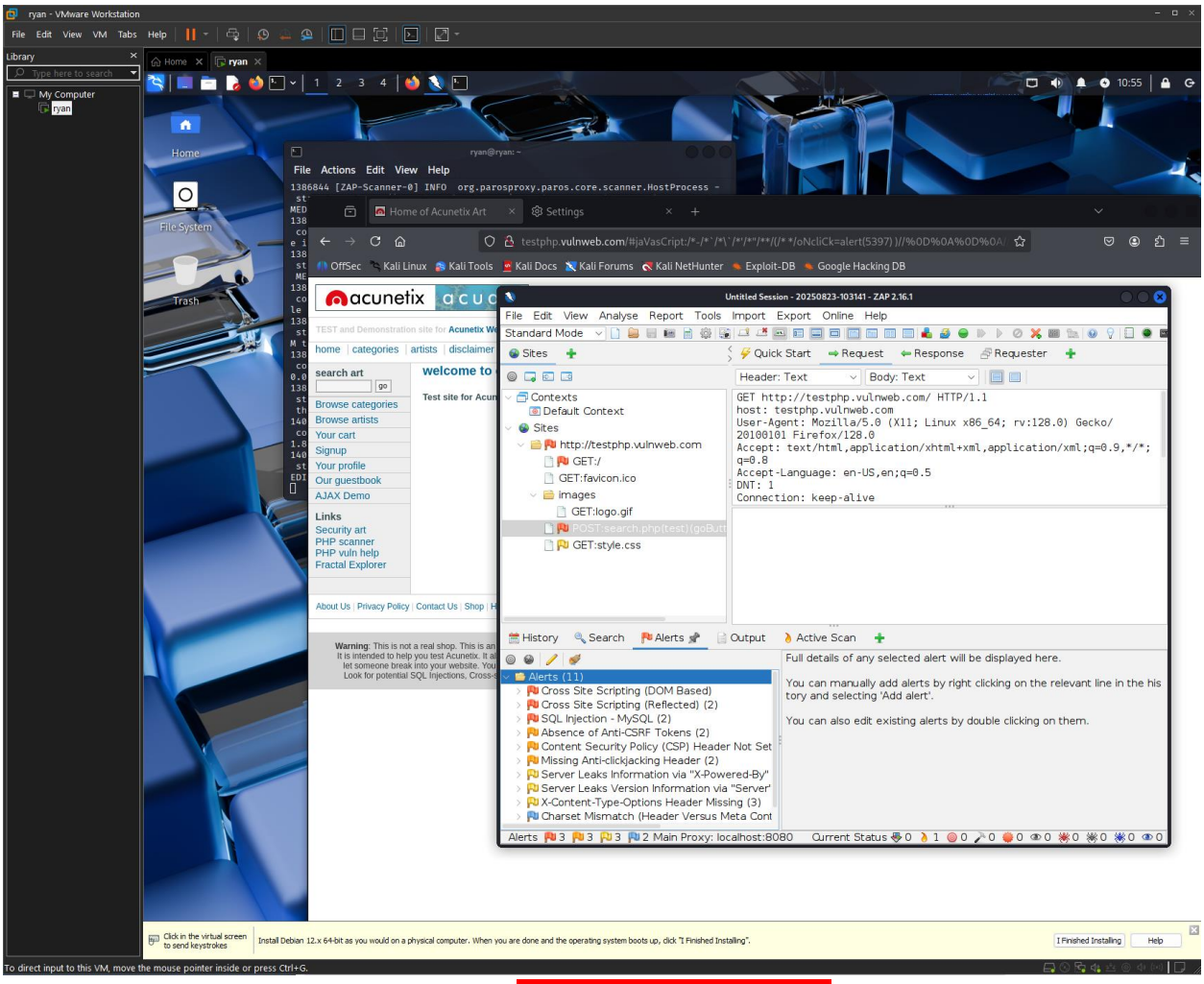
5. Technical Findings (Temuan Teknis)

5.1. SQL Injection (MySQL)

Tingkat Risiko: TINGGI

Deskripsi Kerentanan: Aplikasi ini rentan terhadap serangan SQL Injection. Parameter pada fungsionalitas pencarian tidak melakukan sanitasi input dengan benar, sehingga memungkinkan penyerang untuk menyisipkan perintah SQL berbahaya pada database backend.

Evidence / Proof-of-Concept: Hasil akhir pemindaian OWASP ZAP



secara jelas mencantumkan temuan "SQL Injection - MySQL".

Risk (Skor CVSS & Analisis):

CVSS 3.1 Score (Estimasi): 9.8 (Kritis)

Impact: Tinggi. Dapat menyebabkan kompromi total terhadap kerahasiaan, integritas, dan ketersediaan data.

Impact (Dampak Teknis & Bisnis):

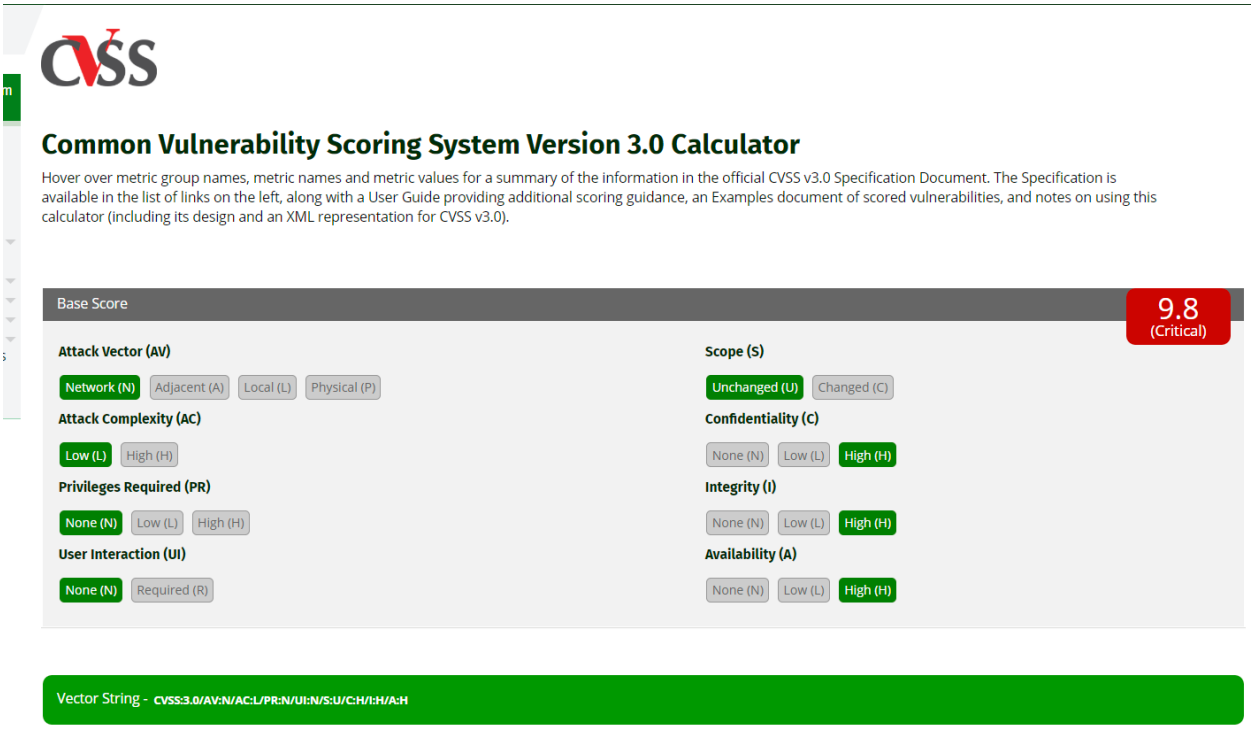
Teknis: Penyerang dapat membaca, memodifikasi, atau menghapus data dari database, bahkan berpotensi mengambil alih server.

Bisnis: Kebocoran data pelanggan, kerugian finansial, dan kerusakan reputasi parah.

Rekomendasi Mitigasi:

Gunakan Parameterized Queries (Prepared Statements): Terapkan prepared statements pada semua query database untuk memisahkan kode SQL dari data input pengguna.

Input Validation: Terapkan validasi server-side yang ketat untuk semua input pengguna.



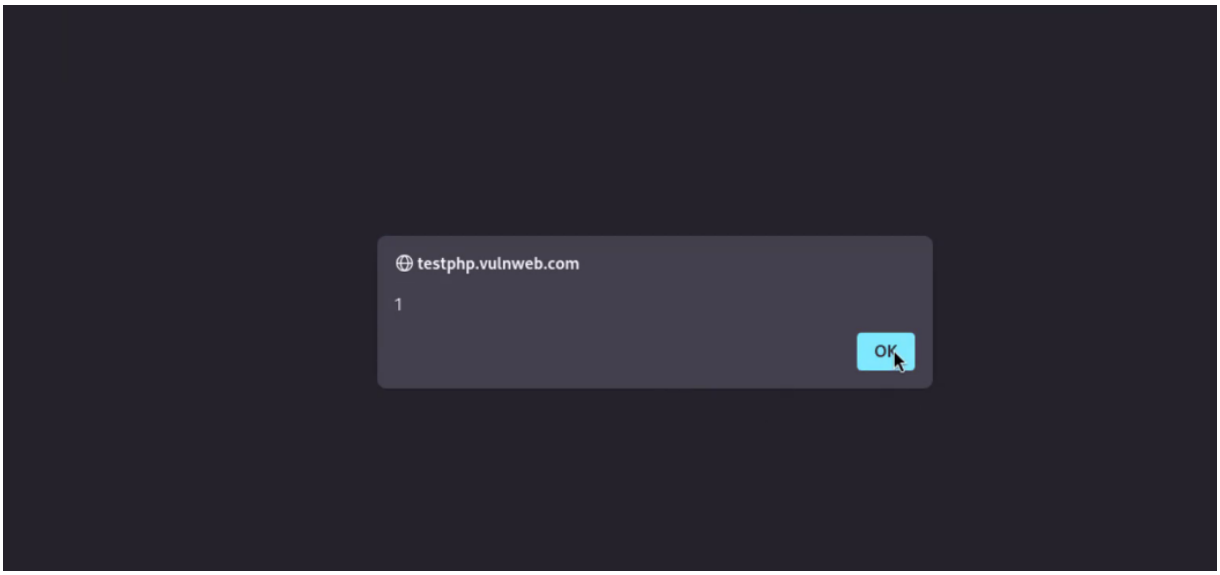
5.2. Cross-Site Scripting (XSS) - Reflected

Tingkat Risiko: TINGGI

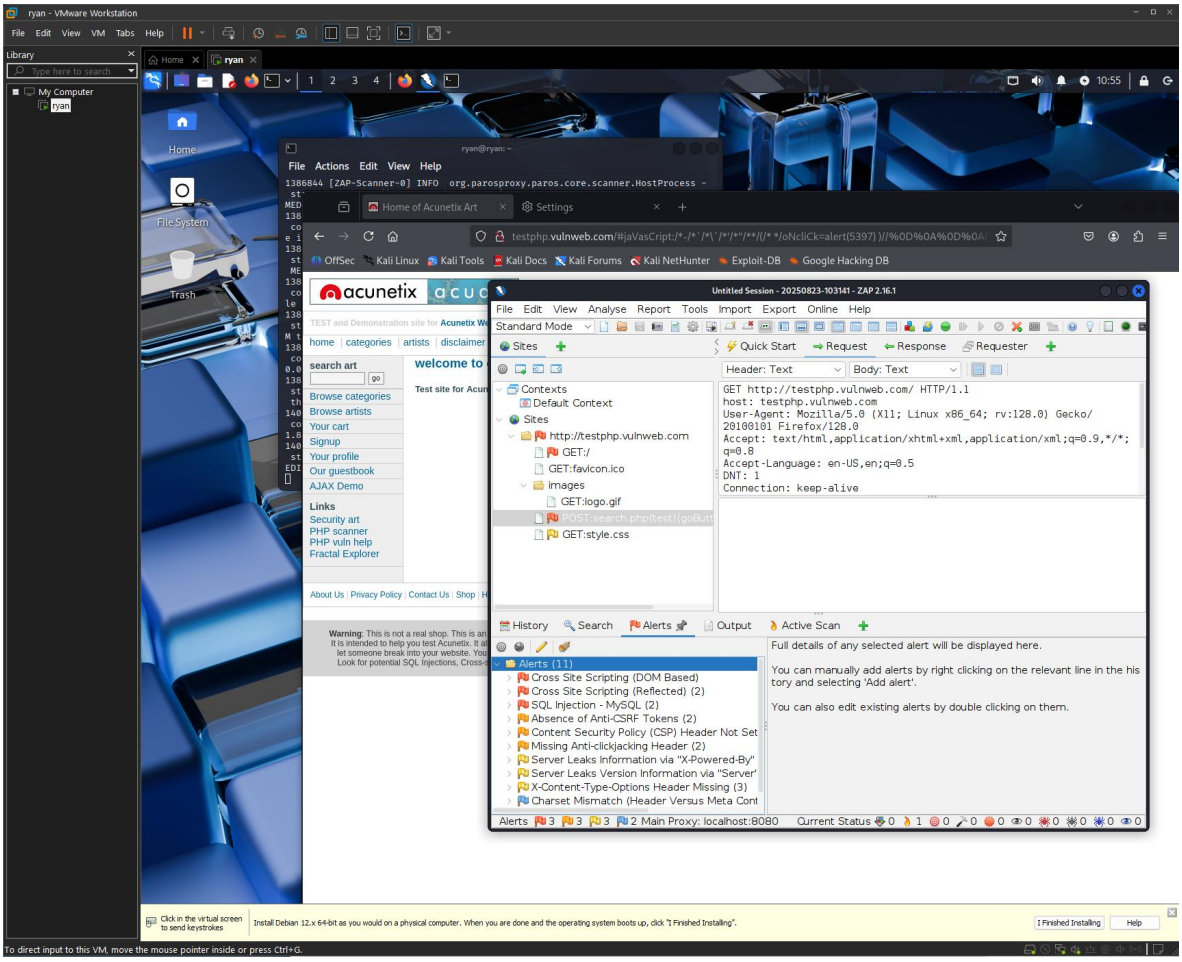
Deskripsi Kerentanan: Aplikasi rentan terhadap serangan Reflected Cross-Site Scripting. Input dari pengguna pada fungsionalitas pencarian ditampilkan kembali di halaman tanpa proses output encoding yang memadai.

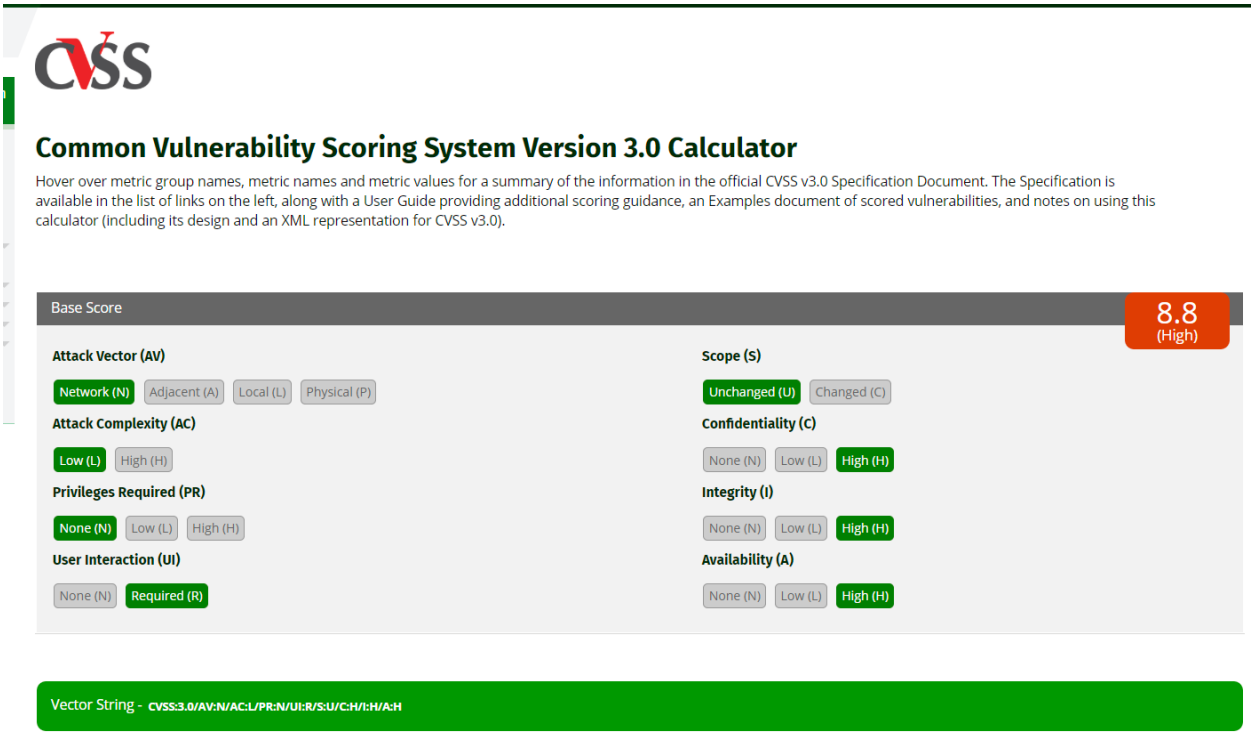
Evidence / Proof-of-Concept:

Serangan berhasil dieksekusi, yang dibuktikan dengan munculnya kotak dialog "1". Bukti ini terekam pukul 10:53:42 WIB



Temuan ini juga dikonfirmasi oleh ringkasan hasil pemindai ZAP pada pukul 10:55:18 WIB





Risk (Skor CVSS & Analisis):

CVSS 3.1 Score (Estimasi): 8.8 (Tinggi)

Impact: Tinggi. Dapat digunakan untuk mencuri cookie sesi, melakukan tindakan atas nama pengguna, atau merusak konten halaman.

Impact (Dampak Teknis & Bisnis):

Teknis: Pencurian cookie dan pengambilalihan sesi (session hijacking), phishing kredensial, dan defacement situs web.

Bisnis: Kompromi akun pengguna, penipuan, dan rusaknya kepercayaan pelanggan.

Rekomendasi Mitigasi:

Context-Aware Output Encoding: Terapkan encoding pada semua data yang berasal dari pengguna sebelum menampilkannya di halaman.

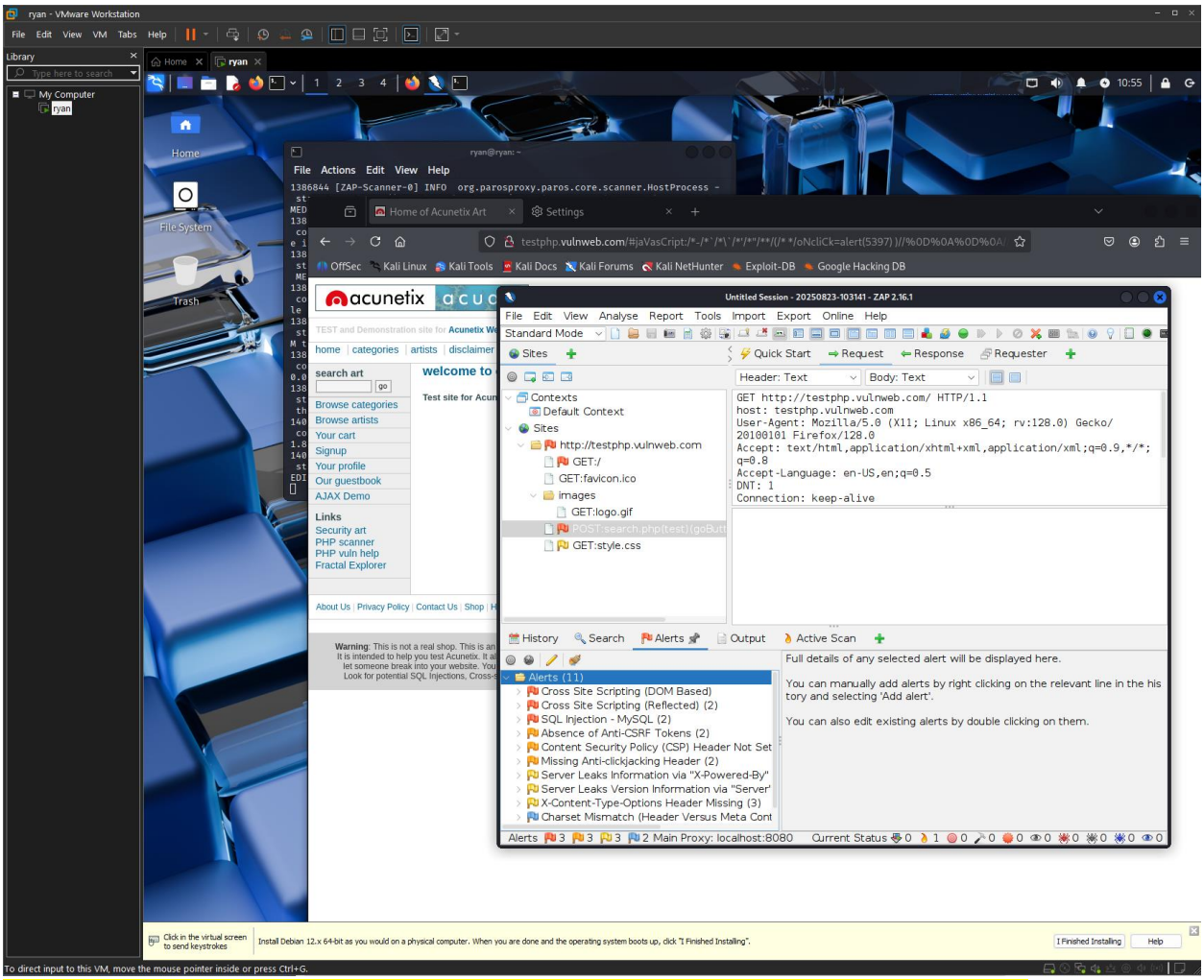
Implementasi **Content Security Policy** (CSP): Gunakan HTTP response header Content-Security-Policy untuk memitigasi dampak serangan XSS.

5.3. Keamanan Header HTTP yang Tidak Memadai

Tingkat Risiko: SEDANG

Deskripsi Kerentanan: Server web tidak mengirimkan beberapa header HTTP keamanan penting, seperti Content-Security-Policy, X-Frame-Options, dan X-Content-Type-Options.

Evidence / Proof-of-Concept: Hasil pemindaian OWASP ZAP



mencantumkan beberapa peringatan terkait header keamanan yang hilang.

Impact (Dampak Teknis & Bisnis): Melemahkan lapisan pertahanan aplikasi (defense-in-depth) dan membuatnya lebih rentan terhadap serangan seperti clickjacking dan XSS.

Rekomendasi Mitigasi: Konfigurasikan server web untuk selalu menyertakan header berikut:

- Content-Security-Policy: default-src 'self'

- X-Frame-Options: DENY

- X-Content-Type-Options: nosniff

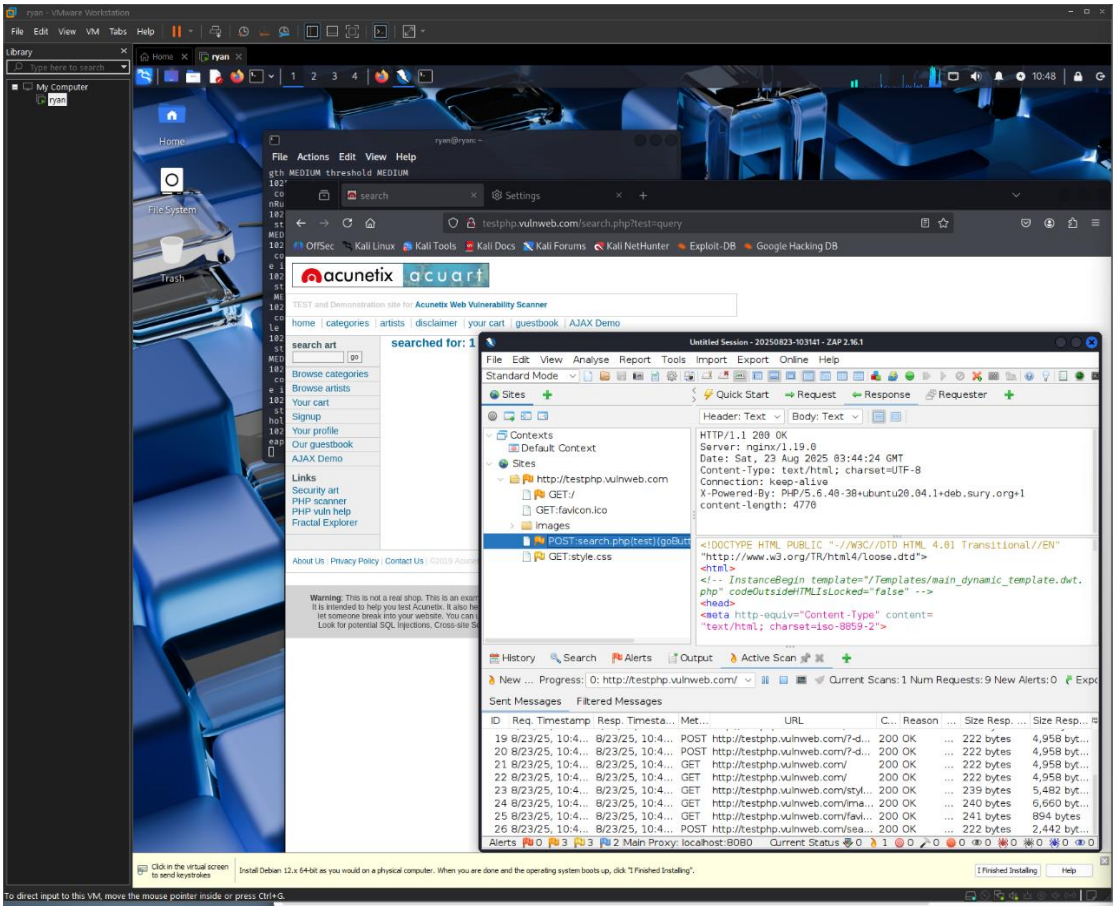
5.4. Information Leakage via Server Headers

Tingkat Risiko: RENDAH

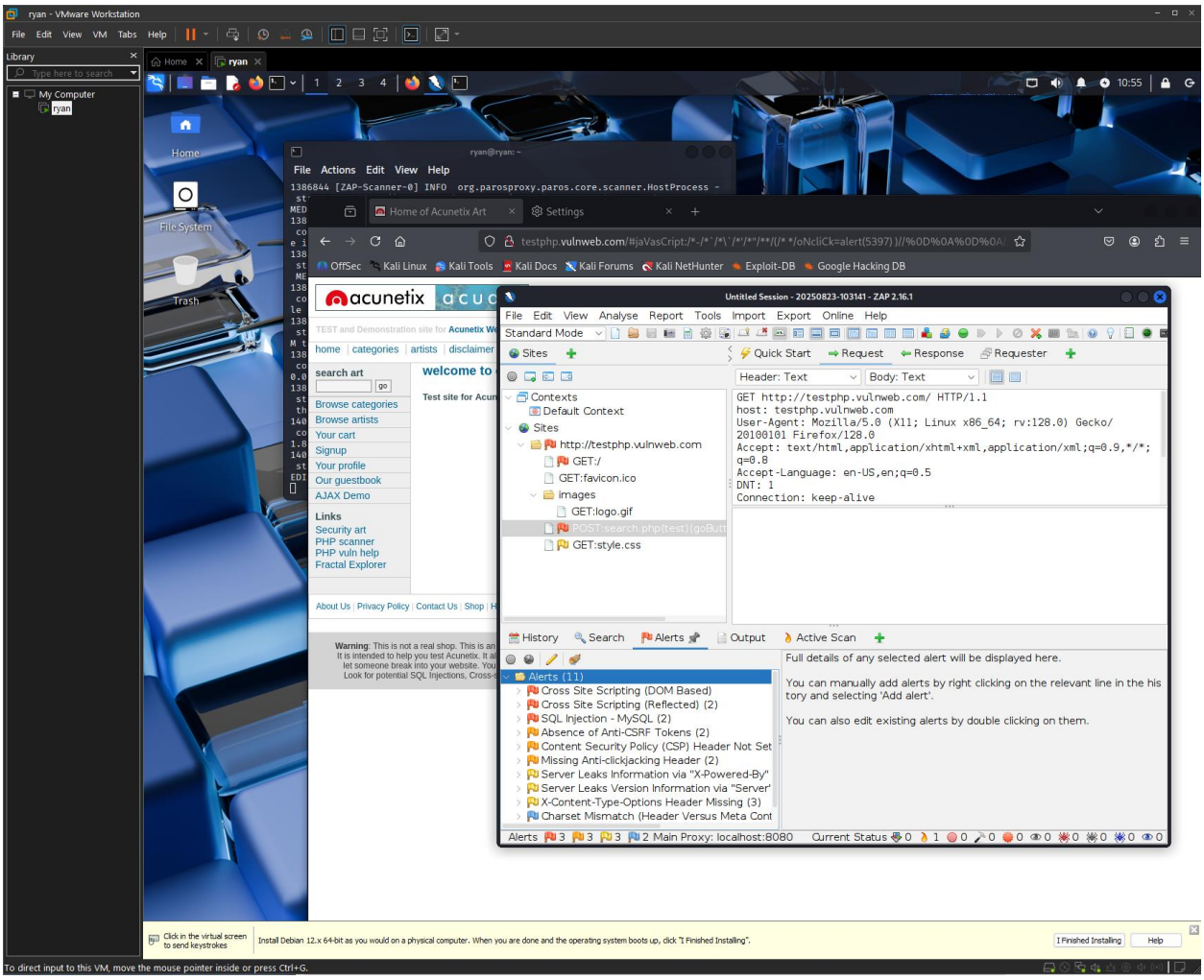
Deskripsi Kerentanan: Server web membocorkan informasi versi perangkat lunak yang digunakan melalui HTTP response headers (Server: nginx/1.19.3 dan X-Powered-By).

Evidence / Proof-of-Concept:

Header Server: nginx/1.19.3 teridentifikasi pada lalu lintas yang diintersepsi pada pukul 10:48:43 WIB



Temuan ini juga diringkas dalam hasil akhir ZAP pada pukul 10:55:18 WIB



Impact (Dampak Teknis & Bisnis): Membantu penyerang dalam fase pengintaian. Jika versi perangkat lunak yang digunakan memiliki kerentanan publik, penyerang dapat langsung menargetkannya.

Rekomendasi Mitigasi:

- Untuk Nginx: Tambahkan server_tokens off; di file konfigurasi nginx.conf.

- Untuk PHP: Ubah nilai expose_php = Off di file php.ini.