

LAPORAN VULNERABILITY ASSESSMENT DAN PENETRATION TESTING (VAPT)

Nama Perusahaan Klien: PT Sev Corp

Nama Tim Penguji / Konsultan: Sevima auditor

Tanggal Pelaksanaan: 19 Juli 2025

Versi Dokumen: 1.0

Klasifikasi: CONFIDENTIAL

Daftar Isi

[Otomatis atau manual diisi saat finalisasi dokumen]

1. Executive Summary

Laporan ini merangkum hasil *Vulnerability Assessment dan Penetration Testing (VAPT)* yang dilakukan terhadap sistem yang ditentukan. Pengujian dilakukan untuk mengidentifikasi kerentanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab dan memberikan rekomendasi mitigasi.

2. Scope of Work

- Sistem/APLIKASI/IP yang diuji: Apocalypse
- Jenis pengujian: (Blackbox / Graybox / Whitebox): Black Box
- Lokasi pengujian: Ruang ujian SEVIMA
- Rentang waktu pengujian: 1 hari

3. Testing Methodology

Metodologi pengujian mengacu pada standar industri seperti OWASP, PTES, atau NIST SP 800-115, mencakup langkah-langkah berikut:

- Information Gathering

Team penguji mengumpulkan informasi sebanyak-banyaknya perihal IP address 192.168.99.9:8009 yang akan diuji beserta lampirannya. Data terbatas hanya diperoleh dari user.

- Threat Modeling

SQL Injection : Tidak adanya kerentanan

XSS (Cross Site Scripting): Ditemukan adanya kerentanan

Broken Acces Control: Tidak adanya kerentanan

- Vulnerability Analysis

Dengan menggunakan metode SQL Injection dengan memasukkan perintah

“ sqlmap -u http://192.168.99.9:8009 -dbs tidak terindikasi bahwa website tersebut rentan dengan SQL Injection seperti terlihat pada screen shoot dibawah ini

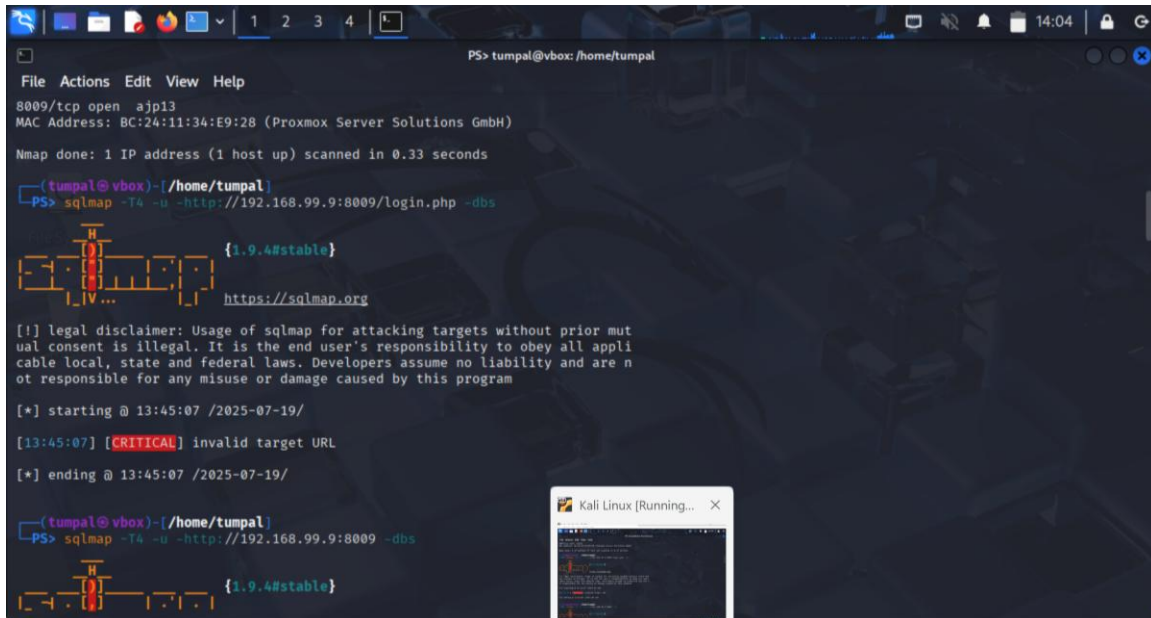
Penggunaan metode XXX dengan menambahkan `$<script>alert('DOM XSS')</script>`

Terlihat bahwa IP address 192.168.99.9:8009 terindikasi rentan dengan XXX hal ini terlihat seperti pada scrren shoot dibawah ini

Dengan metode Broken Acces Control tidak ditemukan adanya kerentanan.

- Exploitation

SQL Injection



```
PS> tumpal@vbox: /home/tumpal
File Actions Edit View Help
8009/tcp open  ajp13
MAC Address: BC:24:11:34:E9:28 (Proxmox Server Solutions GmbH)
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds

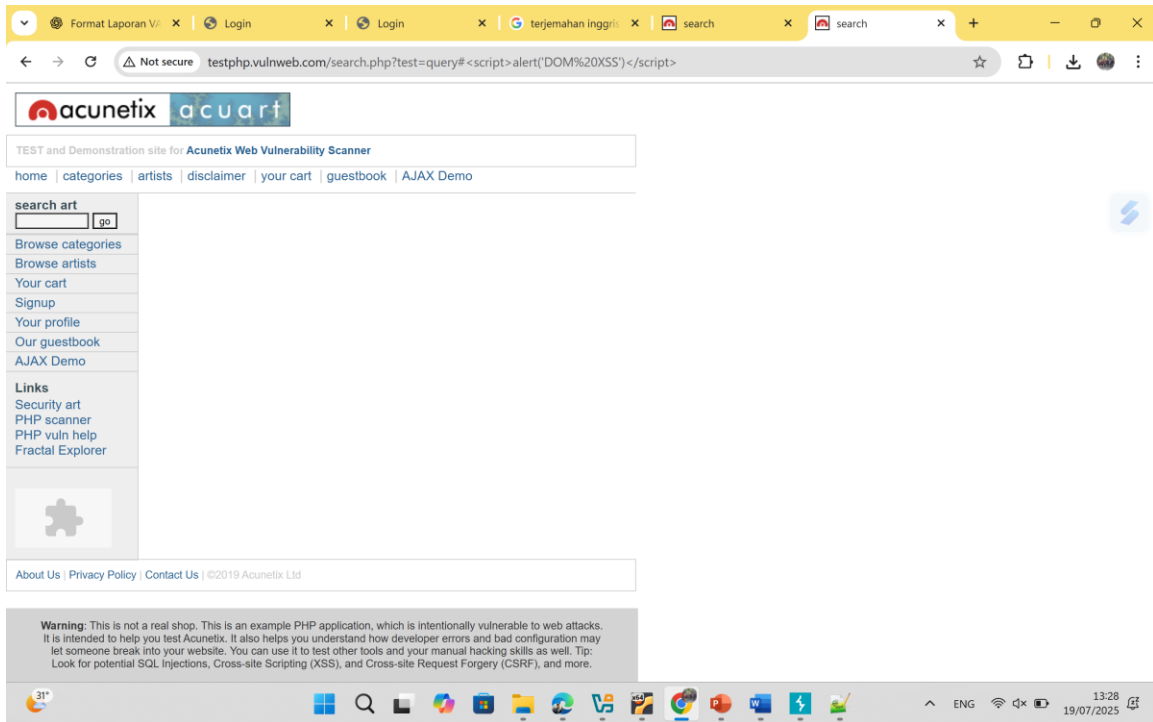
(tumpal@vbox)-[/home/tumpal]
PS> sqlmap -T4 -u http://192.168.99.9:8009/login.php -dbs

  H
  |
  |  {1.9.4#stable}
  |  https://sqlmap.org
  |  [!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
  |  ual consent is illegal. It is the end user's responsibility to obey all appli
  |  cable local, state and federal laws. Developers assume no liability and are n
  |  ot responsible for any misuse or damage caused by this program
  |
  |  [*] starting @ 13:45:07 /2025-07-19/
  |
  |  [13:45:07] [CRITICAL] invalid target URL
  |
  |  [*] ending @ 13:45:07 /2025-07-19/

(tumpal@vbox)-[/home/tumpal]
PS> sqlmap -T4 -u http://192.168.99.9:8009 -dbs

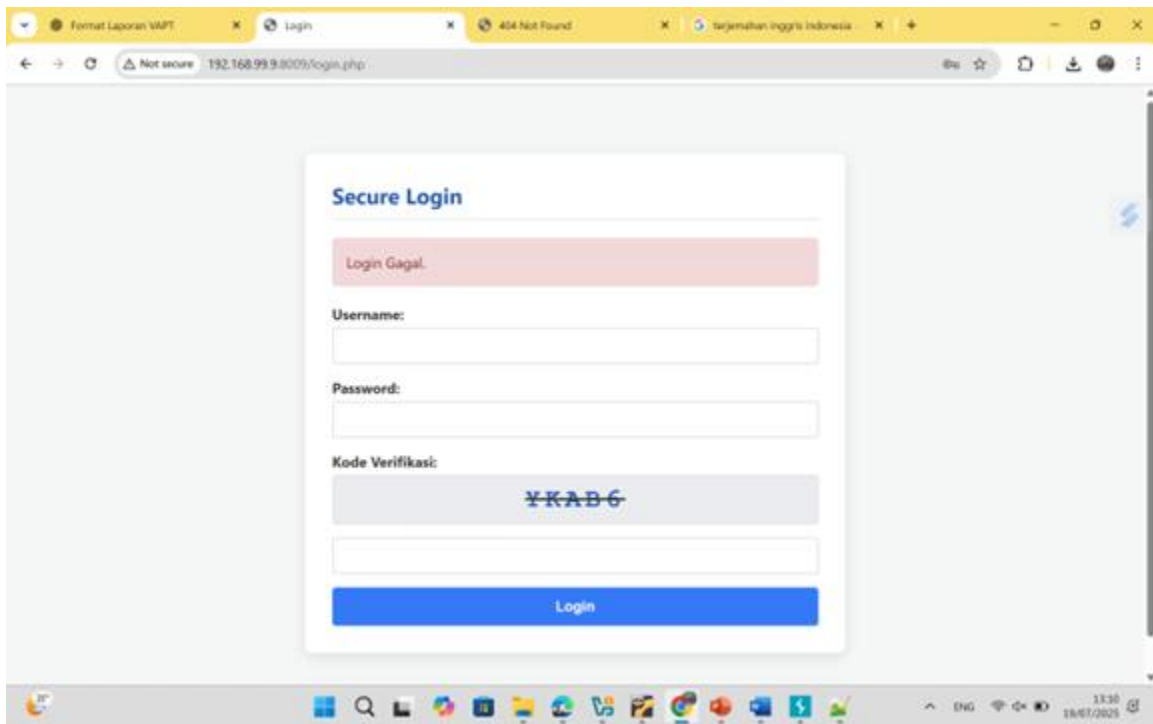
  H
  |
  |  {1.9.4#stable}
```

XSS DOM

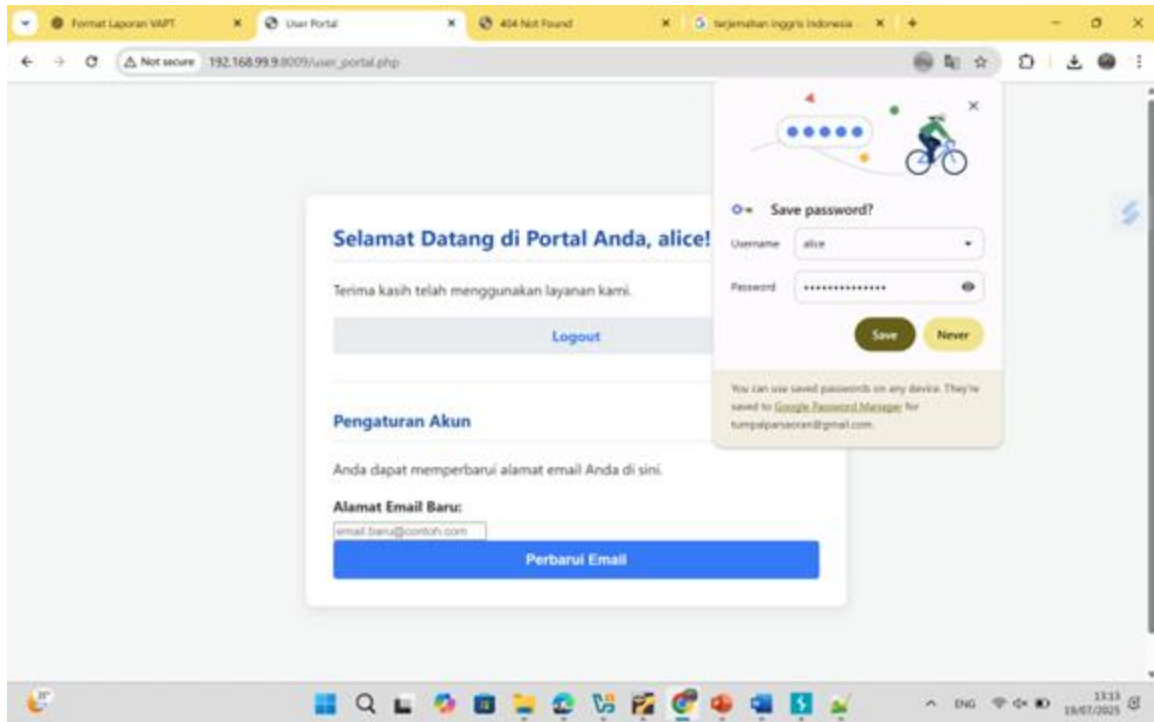


Broken Acces Control

Contoh input salah menghasilkan



Contoh Input benar



- Post-Exploitation

SQL Injection : Tidak perlu dilakukan pencegahan

XSS : Perlu dilakukan tindakan mitigasi agar alamat IP adder tersebut aman. Langkah pencegahannya sbb: 1. Menggunakan `htmlspecialchars()` di PHP 2. Hanya izinkan karakter tertentu (huruf, angka) 3. Cegah skrip tak dikenal dijalankan di http

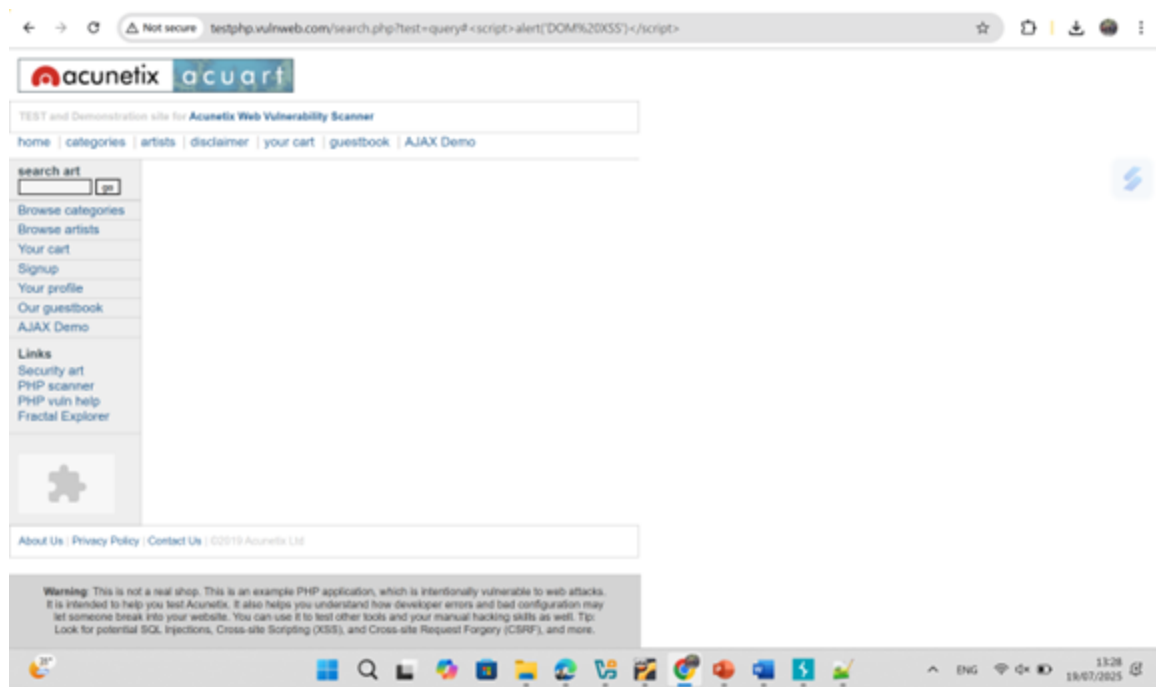
Broken Acces Control: Tidak perlu dilakukan pencegahan

- Reporting

Dari ketiga celah keamanan umum di aplikasi ternyata Alamat Web 192.168.99.9:8009 rentan dengan XSS

4. Findings

Contoh Format Temuan:



Judul Temuan: IP address 192.168.99.9:8009 rentan dengan ancaman XSS

Indikasi: ancaman ini dapat terjadi Ketika input berbahaya disimpan di server/database lalu ditampilkan Kembali kepada pengguna lain tanpa disaring

Deskripsi: Ancaman XSS

Dampak: Dampak dari serangan ini adalah

1. Pencurian data: Penyerang dapat menggunakan XSS untuk mencuri data sensitif, seperti cookie, token autentikasi, atau informasi pribadi lainnya.
2. Pengambilalihan akun: Penyerang dapat menggunakan XSS untuk mengambil alih akun pengguna, sehingga mereka dapat melakukan tindakan yang tidak diinginkan atas nama pengguna.
3. Penyebaran malware: Penyerang dapat menggunakan XSS untuk menyebarkan malware, seperti virus atau Trojan, ke komputer pengguna.
4. Phishing: Penyerang dapat menggunakan XSS untuk melakukan phishing, yaitu mencuri informasi login atau data sensitif lainnya dengan cara menipu pengguna.

5. Kerusakan reputasi: Serangan XSS dapat merusak reputasi situs web atau perusahaan, sehingga pengguna kehilangan kepercayaan pada situs web tersebut.

6. Kehilangan data: Serangan XSS dapat menyebabkan kehilangan data sensitif, seperti data keuangan atau informasi pribadi lainnya.

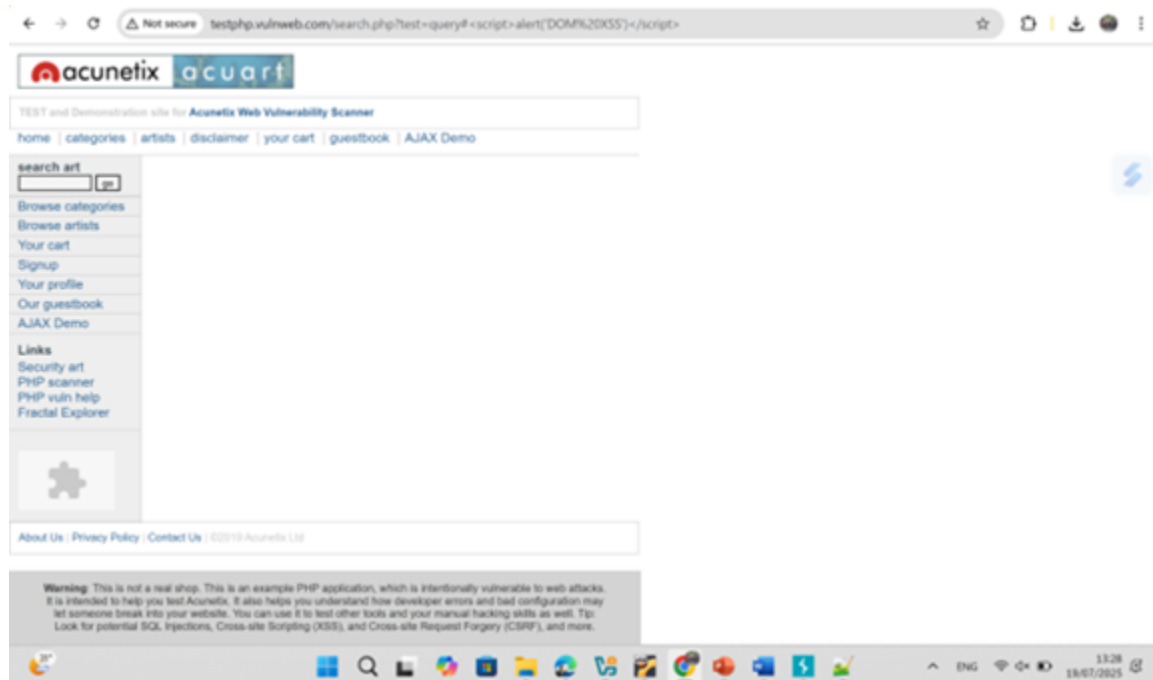
7. Penggunaan tidak sah: Penyerang dapat menggunakan XSS untuk melakukan tindakan tidak sah, seperti mengirimkan spam atau melakukan serangan DDoS.

Rekomendasi:

Dampak XSS dapat dicegah dengan melakukan beberapa langkah keamanan, seperti:

- Menggunakan validasi input yang ketat
- Menggunakan encoding output yang tepat
- Menggunakan Content Security Policy (CSP)
- Menggunakan HTTPS
- Melakukan pengujian keamanan secara teratur

Bukti:

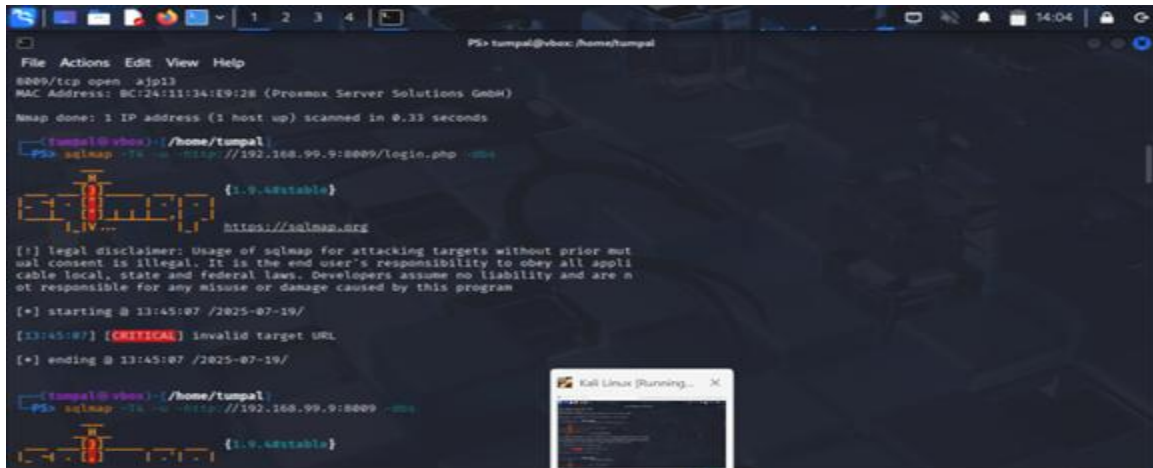


7. Appendices

- Tools yang digunakan Kali linux SQL Injection, acunetix acuart

- Bukti teknis

SQL Injection



```
PS> tumpal@vbox: /home/tumpal
File Actions Edit View Help
8080/tcp open  ajp13
MAC Address: 0C:12:41:11:34:E9:28 (Proxmox Server Solutions GmbH)
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds

[tumpal@vbox:~/home/tumpal]
PS> sqlmap -u http://192.168.99.9:8080/login.php --sqlmap

[1.9.4stable]
https://sqlmap.org

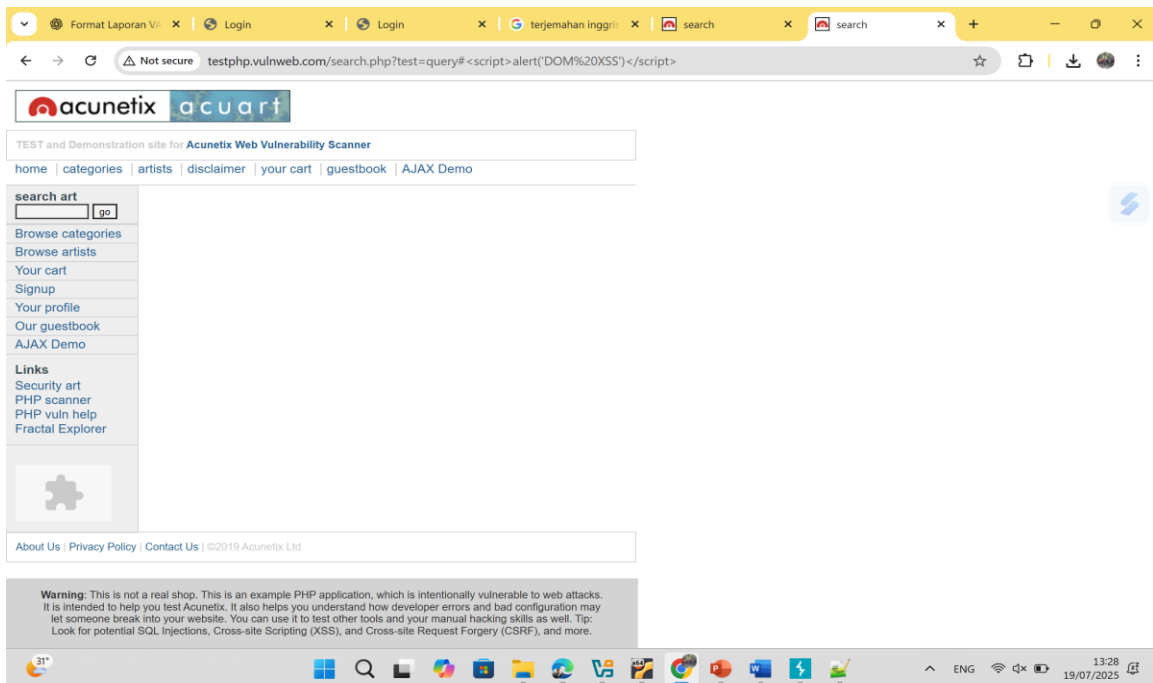
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applica-
ble local, state and federal laws. Developers assume no liability and are n-
ot responsible for any misuse or damage caused by this program

[+] starting @ 13:45:07 /2025-07-19/
[13:45:07] [CRITICAL] invalid target URL
[+] ending @ 13:45:07 /2025-07-19/

[tumpal@vbox:~/home/tumpal]
PS> sqlmap -u http://192.168.99.9:8080 --sqlmap

[1.9.4stable]
```

XSS



Broken Acces Control

