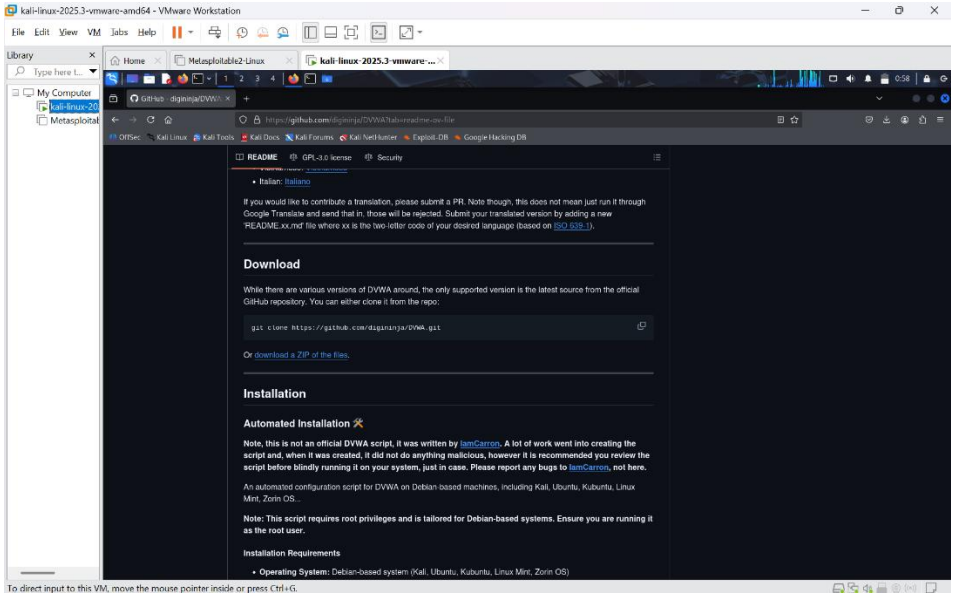
LAPORAN PRAKTIKUM
ADVANCED NETWORK SECURITY AND PROTOCOLS

DISUSUN OLEH

Nur Qamariah Yunus 105841104323 JK-A

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH MAKASSAR
2025

1. Download DVWA
   - Masuk ke VMware lalu jalankan kali linux.
   - Masuk ke firefox dan masukkan link github untuk mendownload DVWA.



   - Masuk ke terminal setelah file didownload. Lalu masuk sebagai ke folder downloads dan ekstrak file zip tersebut ke folder var/www/html.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo unzip -o DVWA-master.zip -d /var/www/html/
[sudo] password for kali:
Archive:  DVWA-master.zip
47bf4292134f454d6d6639ba2be543931b861ff1
   creating: /var/www/html/DVWA-master/
  inflating: /var/www/html/DVWA-master/.dockerignore
   creating: /var/www/html/DVWA-master/.github/
  inflating: /var/www/html/DVWA-master/.github/FUNDING.yml
   creating: /var/www/html/DVWA-master/.github/ISSUE_TEMPLATE/
  inflating: /var/www/html/DVWA-master/.github/ISSUE_TEMPLATE/bug-report---installation.md
  inflating: /var/www/html/DVWA-master/.github/ISSUE_TEMPLATE/bug-report---vulnerability.md
  inflating: /var/www/html/DVWA-master/.github/ISSUE_TEMPLATE/i-m-stuck.md
   creating: /var/www/html/DVWA-master/.github/workflows/
  inflating: /var/www/html/DVWA-master/.github/workflows/codeql-analysis.yml
  inflating: /var/www/html/DVWA-master/.github/workflows/docker-image.yml
  inflating: /var/www/html/DVWA-master/.github/workflows/pytest.yml
  inflating: /var/www/html/DVWA-master/.github/workflows/shiftleft-analysis.yml
  inflating: /var/www/html/DVWA-master/.github/workflows/vulnerable.yml
  inflating: /var/www/html/DVWA-master/CHANGELOG.md
```

   - Masuk sebagai root ke folder var/www/html lalu ubah nama folder ke DVWA

```
┌──(root㉿kali)-[/var/www/html]
└─# mv DVWA-master DVWA

┌──(root㉿kali)-[/var/www/html]
└─# dir
DVWA  index.html  index.nginx-debian.html
```

- Buat file config DVWA

```
┌──(root㉿kali)-[/var/www/html/DVWA]
└─# dir
about.php      config        Dockerfile  external     index.php
CHANGELOG.md   COPYING.txt   docs        favicon.ico  instructions.php
compose.yml    database      dvwa        hackable     login.php

┌──(root㉿kali)-[/var/www/html/DVWA]
└─# cd config

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# dir
config.inc.php.dist

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# cp config.inc.php.dist config.inc.php
```

- Beri akses ke direktori DVWA

```
┌──(root㉿kali)-[/var/www/html]
└─# sudo chmod -R 777 /var/www/html/DVWA
```

- Pastikan mysql serive di mulai

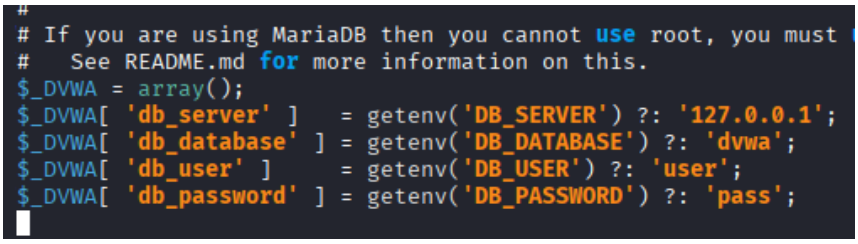
```
┌──(root㉿kali)-[/var/www/html]
└─# service mysql start
```

- Login ke mysql, buat database baru baru “dvwa” dan user user@127.0.0.1 dengan password “pass”

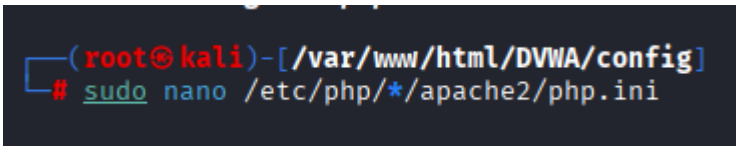
```
┌──(root㉿kali)-[/var/www/html]
└─# mysql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 11.8.5-MariaDB-3 from Debian -- Please help get to 10k stars at https://github.com/MariaDB/Server

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;
ERROR 1007 (HY000): Can't create database 'dvwa'; database exists
MariaDB [(none)]> CREATE USER 'user'@'127.0.0.1' IDENTIFIED BY 'pass';
ERROR 1396 (HY000): Operation CREATE USER failed for 'user'@'127.0.0.1'
MariaDB [(none)]> GRANT ALL PRIVILEGES ON dvwa.* TO 'user'@'127.0.0.1';
Query OK, 0 rows affected (0.005 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]>
MariaDB [(none)]> CREATE USER 'user'@'localhost' IDENTIFIED BY 'pass';
Query OK, 0 rows affected (0.004 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON dvwa.* TO 'user'@'localhost';
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]>
MariaDB [(none)]> EXIT;
Bye
```

- Masuk ke file config untuk mengedit detail isinya.

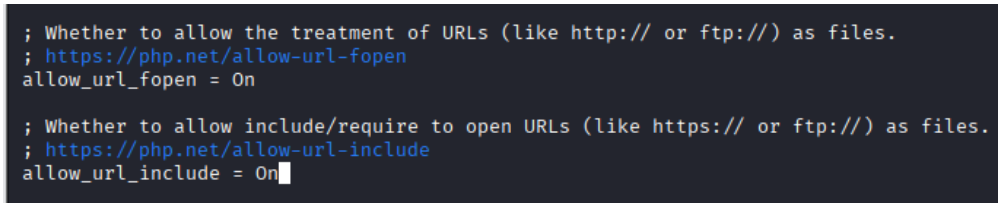
- Sesuaikan detailnya isinya seperti ini



- Edit file php.ini apache

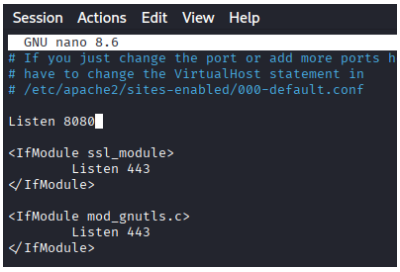


- Editi isinya seperti ini



- Ubah port di ports.conf

- Ubah 80 menjadi 8080



- Ubah port di virtualhost

```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# sudo nano /etc/apache2/sites-available/000-default.conf
```

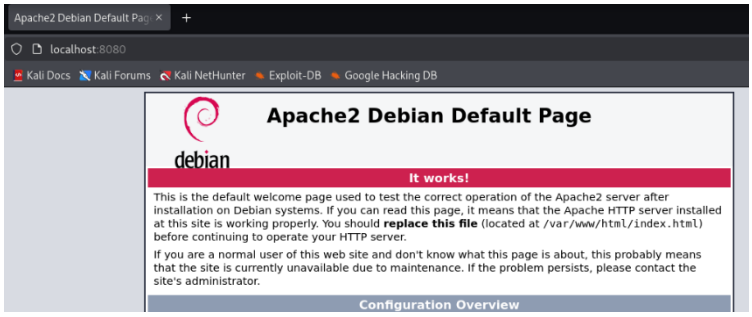
```
Session   Actions   Edit   View   Help
  GNU nano 8.6
<VirtualHost *:8080>
        # The ServerName directive sets the request
        # the server uses to identify itself. This i
        # redirection URLs. In the context of virtua
        # specifies what hostname must appear in the
        # match this virtual host. For the default v
        # value is not decisive as it is used as a l
        # However, you must set it for any further v
        #ServerName www.example.com
```

- Restart apache lalu cek status

```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# sudo systemctl restart apache2


┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# sudo systemctl status apache2 --no-pager

● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Tue 2025-12-30 01:43:55 EST; 14s ago
 Invocation: ceb60c2041bf483ab012252a6067a10c
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 30830 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 30846 (apache2)
      Tasks: 6 (limit: 2197)
     Memory: 23.4M (peak: 23.6M)
        CPU: 224ms
     CGroup: /system.slice/apache2.service
             ├─30846 /usr/sbin/apache2 -k start
             ├─30857 /usr/sbin/apache2 -k start
             ├─30858 /usr/sbin/apache2 -k start
             ├─30859 /usr/sbin/apache2 -k start
             ├─30860 /usr/sbin/apache2 -k start
             └─30861 /usr/sbin/apache2 -k start

Dec 30 01:43:54 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Dec 30 01:43:55 kali apachectl[30845]: AH00558: apache2: Could not reliably determine the ser
Dec 30 01:43:55 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
```

- Tes port apakah sudah berjalan (sudah berjalan).

```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# ss -ltnp | grep apache2

LISTEN 0      511                *:8080             *:*    users:(("apache2",pid=30861,fd=4),("apache2",pid=30860,fd=4),("apache2",pid=30859,fd=4),("apache2",pid=30858,fd
,pid=30846,fd=4))
```



2. Praktikum hping3

- Catat ip target

```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:c9:03:10 brd ff:ff:ff:ff:ff:ff
    inet 10.34.219.18/24 brd 10.34.219.255 scope global dynamic eth0
       valid_lft 3598sec preferred_lft 3598sec
    inet6 2404:c0:4451:b208:ca6d:c0ff:e743:8505/64 scope global dynamic noprefixroute
       valid_lft 6997sec preferred_lft 6997sec
    inet6 fe80::83b8:9209:ede2:51a2/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- Catat ip attacker (kali yg telah dipasangi apache dan DVWA)

```
┌──(root㉿kali)-[/home/kali]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
    inet 10.34.219.40/24 brd 10.34.219.255 scope global dynamic noprefixroute eth0
       valid_lft 3223sec preferred_lft 3223sec
    inet6 2404:c0:4010:7bfd:7f7c:5beb:bf7d:b447/64 scope global dynamic noprefixroute
       valid_lft 6321sec preferred_lft 6321sec
    inet6 2404:c0:4451:b208:8a6f:65d8:256b:7d47/64 scope global dynamic noprefixroute
       valid_lft 7015sec preferred_lft 7015sec
    inet6 fe80::393c:aea1:81f:e5cf/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- Ping ip target dari sisi attacker

```
┌──(root㉿kali)-[/home/kali]
└─# ping -c 4 10.34.219.18
PING 10.34.219.18 (10.34.219.18) 56(84) bytes of data.
64 bytes from 10.34.219.18: icmp_seq=1 ttl=64 time=4.53 ms
64 bytes from 10.34.219.18: icmp_seq=2 ttl=64 time=1.27 ms
64 bytes from 10.34.219.18: icmp_seq=3 ttl=64 time=1.30 ms
64 bytes from 10.34.219.18: icmp_seq=4 ttl=64 time=1.00 ms

── 10.34.219.18 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 1.000/2.027/4.534/1.452 ms
```

- Jalankan serangan hping3 dari sisi attacker

```
┌──(root㉿kali)-[/home/kali]
└─# sudo hping3 -S --flood -p 8080 10.34.219.18
HPING 10.34.219.18 (eth0 10.34.219.18): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

- Cek di sisi target apakah ada serangan atau tidak

```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# netstat -ant | grep 8080
tcp6       0      0 :::8080                 :::*                    LISTEN
tcp6       0      0 10.34.219.18:8080       10.34.219.40:40603      SYN_RECV
tcp6       0      0 10.34.219.18:8080       10.34.219.40:40603      SYN_RECV
```

- Blokir ip penyerang dengan iptables

```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# sudo iptables -A INPUT -s 10.34.219.40 -j DROP
```

- Lakukan pengecekan ulang (ip penyerang sudah tidak muncul)

```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# netstat -ant | grep 8080
tcp6       0      0 :::8080                 :::*                    LISTEN
```

3. Praktikum slowloris
   - Install slowhttptest di vm attacker

```
┌──(root㉿kali)-[/home/kali]
└─# sudo apt update && sudo apt install slowhttptest
Get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.9 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.5 MB]
Fetched 73.5 MB in 1min 1s (1,198 kB/s)
1467 packages can be upgraded. Run 'apt list --upgradable' to see them.
Installing:
  slowhttptest

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1467
  Download size: 31.6 kB
  Space needed: 91.1 kB / 63.4 GB available

Get:1 http://http.kali.org/kali kali-rolling/main amd64 slowhttptest amd64 1.9.0-1+b1 [31.6 kB]
Fetched 31.6 kB in 1s (24.2 kB/s)
Selecting previously unselected package slowhttptest.
(Reading database ... 417248 files and directories currently installed.)
Preparing to unpack .../slowhttptest_1.9.0-1+b1_amd64.deb ...
Unpacking slowhttptest (1.9.0-1+b1) ...
Setting up slowhttptest (1.9.0-1+b1) ...
Processing triggers for kali-menu (2025.3.2) ...
Processing triggers for man-db (2.13.1-1) ...
```

   - Lakukan serangan ke vm target

```
┌──(root㉿kali)-[/home/kali]
└─# slowhttptest -c 1000 -H -u http://10.34.219.18:8080
```

```
Session  Actions  Edit  View  Help
Tue Dec 30 02:36:31 2025:
        slowhttptest version 1.9.0
 - https://github.com/shekyan/slowhttptest -
test type:                        SLOW HEADERS
number of connections:            1000
URL:                              http://10.34.219.18:8080/
verb:                             GET
cookie:
Content-Length header value:      4096
follow up data max size:          68
interval between follow up data:  10 seconds
connections per seconds:          50
probe connection timeout:         5 seconds
test duration:                    240 seconds
using proxy:                      no proxy

Tue Dec 30 02:36:31 2025:
slow HTTP test status on 0th second:

initializing:         0
pending:              1
connected:            0
error:                0
closed:               0
service available:    YES
```

- Pantau serangan di vmtarget

```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# netstat -ant | grep 8080
tcp6     512      0 :::8080                 :::*                    LISTEN
tcp6     277      0 10.34.219.18:8080       10.34.219.40:50926      ESTABLISHED
tcp6     255      0 10.34.219.18:8080       10.34.219.40:52420      ESTABLISHED
tcp6     273      0 10.34.219.18:8080       10.34.219.40:51100      ESTABLISHED
tcp6       0      0 10.34.219.18:8080       10.34.219.40:47668      ESTABLISHED
tcp6     286      0 10.34.219.18:8080       10.34.219.40:51590      ESTABLISHED
tcp6     238      0 10.34.219.18:8080       10.34.219.40:54146      ESTABLISHED
tcp6     238      0 10.34.219.18:8080       10.34.219.40:53920      ESTABLISHED
tcp6     246      0 10.34.219.18:8080       10.34.219.40:51708      ESTABLISHED
tcp6     238      0 10.34.219.18:8080       10.34.219.40:54648      ESTABLISHED
tcp6     238      0 10.34.219.18:8080       10.34.219.40:50092      ESTABLISHED
tcp6     276      0 10.34.219.18:8080       10.34.219.40:53822      ESTABLISHED
tcp6     238      0 10.34.219.18:8080       10.34.219.40:54612      ESTABLISHED
tcp6     262      0 10.34.219.18:8080       10.34.219.40:51196      ESTABLISHED
tcp6     268      0 10.34.219.18:8080       10.34.219.40:53222      ESTABLISHED
tcp6     238      0 10.34.219.18:8080       10.34.219.40:54650      ESTABLISHED
tcp6     238      0 10.34.219.18:8080       10.34.219.40:54156      ESTABLISHED
tcp6     259      0 10.34.219.18:8080       10.34.219.40:51114      ESTABLISHED
tcp6     267      0 10.34.219.18:8080       10.34.219.40:50934      ESTABLISHED
tcp6       0      0 10.34.219.18:8080       10.34.219.40:47362      ESTABLISHED
tcp6     238      0 10.34.219.18:8080       10.34.219.40:49764      ESTABLISHED
tcp6     276      0 10.34.219.18:8080       10.34.219.40:52372      ESTABLISHED
tcp6     257      0 10.34.219.18:8080       10.34.219.40:51408      ESTABLISHED
tcp6       0      0 10.34.219.18:8080       10.34.219.40:47664      ESTABLISHED
tcp6     238      0 10.34.219.18:8080       10.34.219.40:50132      ESTABLISHED
tcp6     270      0 10.34.219.18:8080       10.34.219.40:51404      ESTABLISHED
tcp6     238      0 10.34.219.18:8080       10.34.219.40:49842      ESTABLISHED
tcp6     287      0 10.34.219.18:8080       10.34.219.40:51254      ESTABLISHED
tcp6     285      0 10.34.219.18:8080       10.34.219.40:51280      ESTABLISHED
tcp6     261      0 10.34.219.18:8080       10.34.219.40:53684      ESTABLISHED
tcp6     283      0 10.34.219.18:8080       10.34.219.40:51454      ESTABLISHED
tcp6     292      0 10.34.219.18:8080       10.34.219.40:52904      ESTABLISHED
tcp6     238      0 10.34.219.18:8080       10.34.219.40:54586      ESTABLISHED
```

- Blokir ip penyerang di vm client menggunakan iptables

```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# sudo iptables -A INPUT -s 10.34.219.40 -j DROP
```

- Lakukan pengecekan ulang (sudah tidak ada banjir ip yang berarti ip penyerang berhasil di blokir)

```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# netstat -ant | grep 8080
tcp6       0      0 :::8080                 :::*                    LISTEN
```