LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1

Pertemuan 9 – *Web Footprinting*

DISUSUN OLEH

Nama	: Sofiyanatul Munawaroh
NIM	: 21/474781/SV/19035
Hari, Tanggal	: Selasa, 9 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

Pertemuan 9 – *Web Footprinting*

I. Tujuan

- Melakukan percobaan *data exposed.*
- Melakukan *basic command execution testing.*
- Melakukan *database reconnaissance.*

II. Latar Belakang

Dalam era digital saat ini, penggunaan internet semakin meluas dan penting dalam kehidupan sehari-hari. Banyak orang menggunakan internet untuk berkomunikasi, berbelanja, mencari informasi, dan berpartisipasi dalam aktivitas *online* lainnya. Namun, semakin banyaknya jejak digital yang ditinggalkan oleh pengguna di *web* meningkatkan risiko privasi dan keamanan.

Footprinting adalah proses mengumpulkan informasi sebanyak mungkin tentang jaringan target, untuk mengidentifikasi berbagai cara untuk menyusup ke dalam sistem jaringan organisasi. *Footprinting* adalah langkah pertama dari setiap serangan terhadap sistem informasi; penyerang mengumpulkan informasi sensitif yang tersedia untuk umum, yang digunakan untuk melakukan rekayasa sosial, serangan sistem dan jaringan, dll. yang menyebabkan kerugian finansial yang besar dan hilangnya reputasi bisnis.

Salah satu jenis *footprinting* yang akan digunakan pada praktikum ini adalah *Website Footprinting*. Teknik ini mengacu pada pemantauan dan analisis situs *web* organisasi target untuk mendapatkan informasi. Penyerang menggunakan informasi yang dikumpulkan untuk melakukan serangan jejak kaki dan rekayasa sosial lebih lanjut.

Web footprinting mengacu pada proses pengumpulan dan analisis jejak digital yang ditinggalkan oleh seseorang atau organisasi di *web*. Jejak digital ini dapat mencakup informasi pribadi, kegiatan *online*, interaksi sosial, dan preferensi pengguna. Melalui teknik-teknik seperti pencarian informasi, pengindeksan halaman *web*, pengumpulan data, dan analisis data, jejak digital ini dapat ditemukan dan dikaitkan untuk mengungkap informasi tentang individu atau organisasi tersebut.

Web footprinting memiliki implikasi yang luas dalam bidang privasi, keamanan, dan intelijen. Meskipun dapat membantu dalam penelusuran informasi yang diperlukan, juga dapat digunakan oleh pihak yang tidak bertanggung jawab untuk memanfaatkan informasi pribadi atau merusak reputasi seseorang atau organisasi.

III. Alat dan Bahan

- *Software Remote Desktop Connection*
- Kali Linux
- Laptop/PC
- Koneksi Internet

IV. Instruksi Kerja

A. Persiapan

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

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start mysql
[sudo] password for kali:

┌──(kali㉿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.

MariaDB [(none)]>
```

2. Jalankan perintah berikut:

```
use mysql;
ALTER USER 'root'@'localhost' IDENTIFIED BY '';
flush privileges;
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 privileges;
Query OK, 0 rows affected (0.001 sec)

MariaDB [mysql]> exit
Bye
```

3. *Restart* layanan MySQL.

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

B. Instal OWASP Mutillidae II

1. Sambungkan dengan DBMS.

```
┌──(kali㉿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.

MariaDB [(none)]>
```

2. Buat *database* mutillidae.

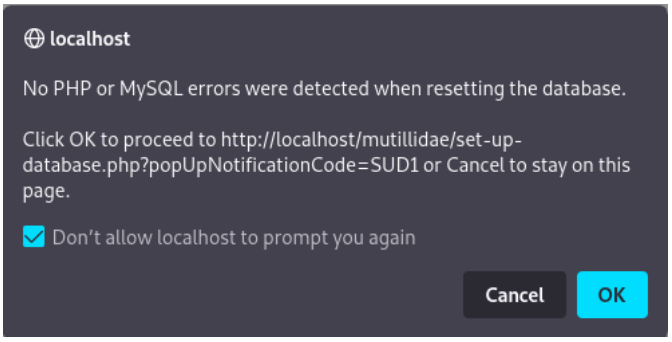
```
MariaDB [(none)]> CREATE DATABASE mutillidae;
ERROR 1007 (HY000): Can't create database 'mutillidae'; database exists
```

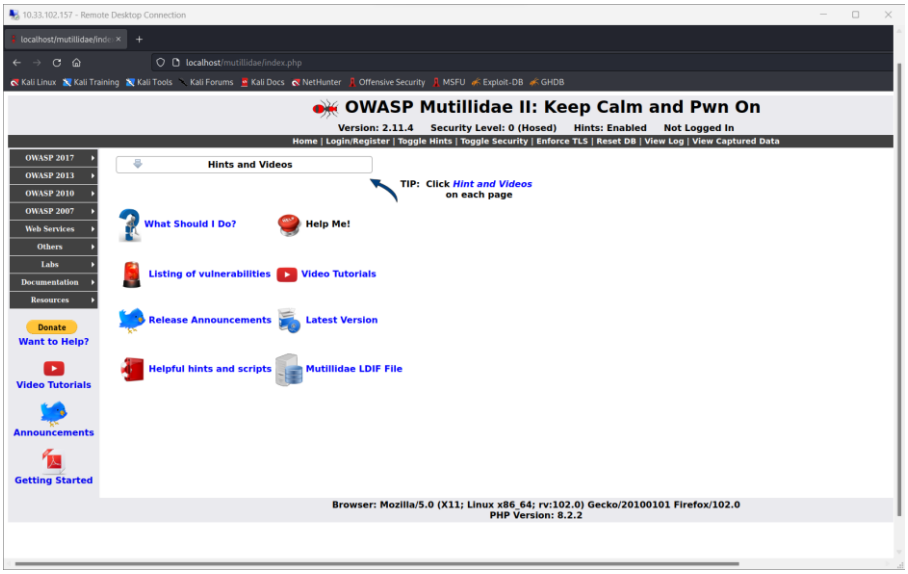
3. Karena *database* mutillidae telah tersedia, maka jalankan perintah berikut.

```
sudo systemctl start php8.2-fpm.service
sudo systemctl start apache2.service
sudo systemctl start mysql
```

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

┌──(kali㉿kali)-[~]
└─$ sudo systemctl start apache2.service

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

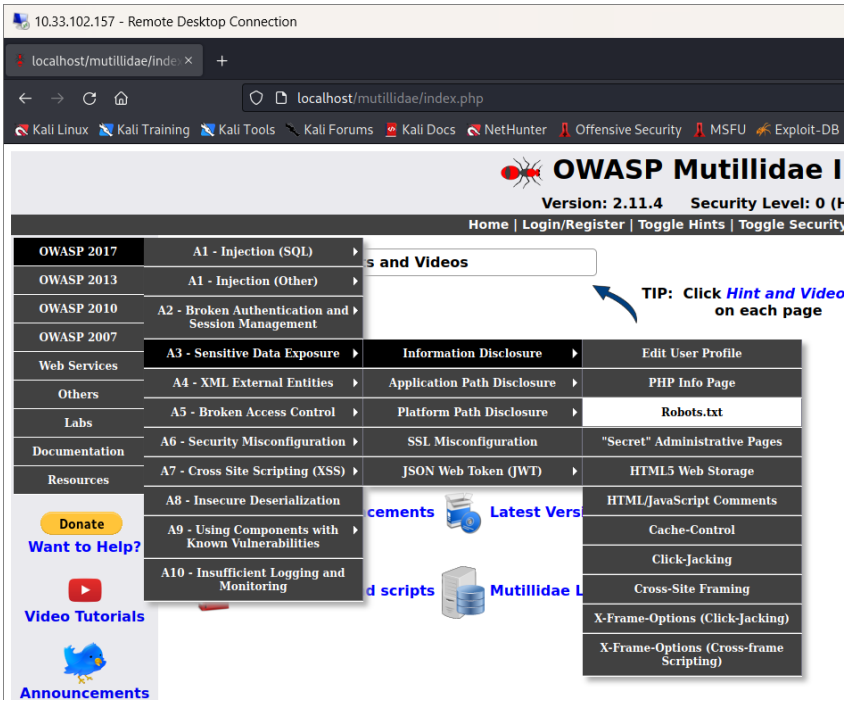
4. Untuk menginisialisasi *database*, akses tautan: http://localhost/mutillidae/set-up-database.php



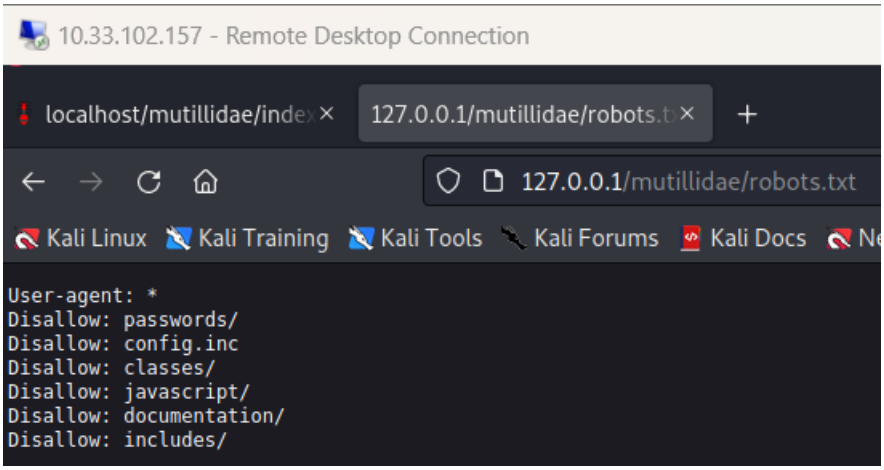


C. Praktik *Data Exposed* dengan *Robot File*

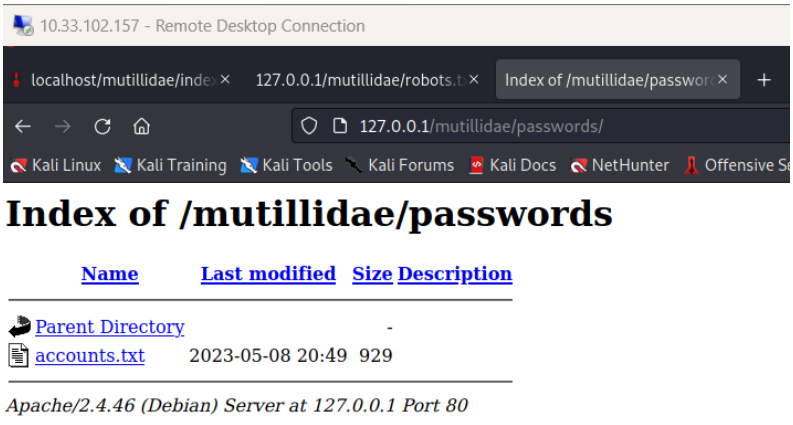
1. Buka jendela multilidae.
2. Pilih menu OWASP 2017 > *sensitive data exposure* > *information disclosure* > *Robots.txt.*



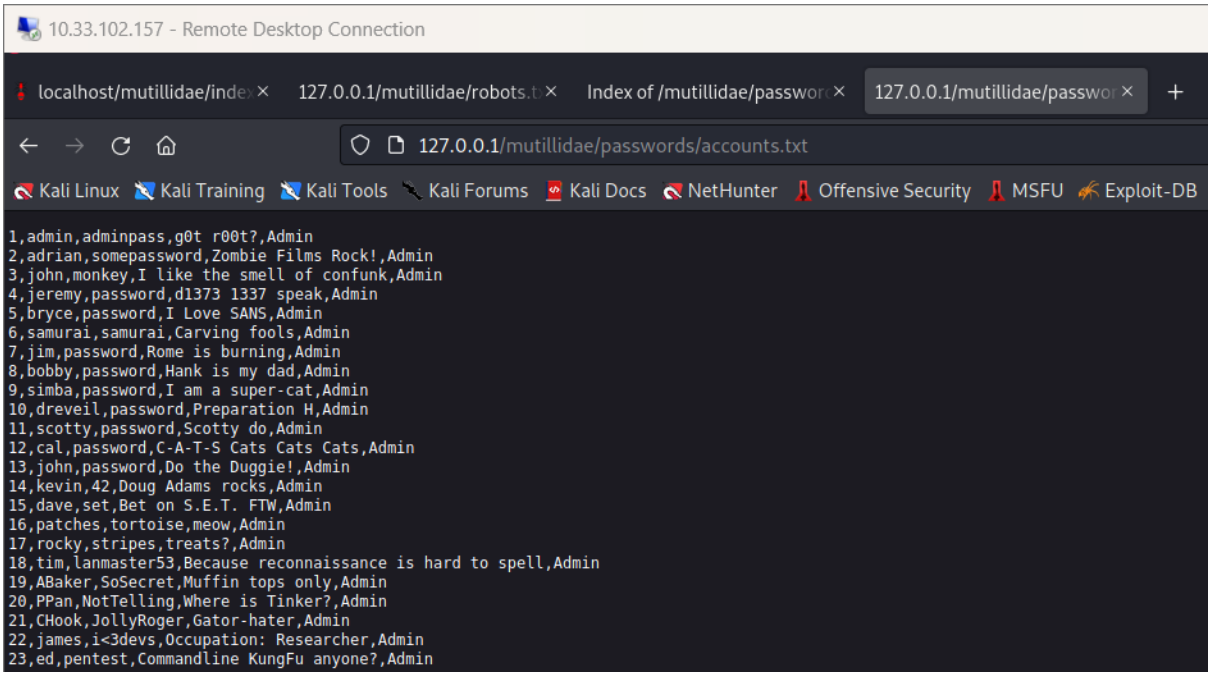
3. Akses Robots.txt melalui *browser*.



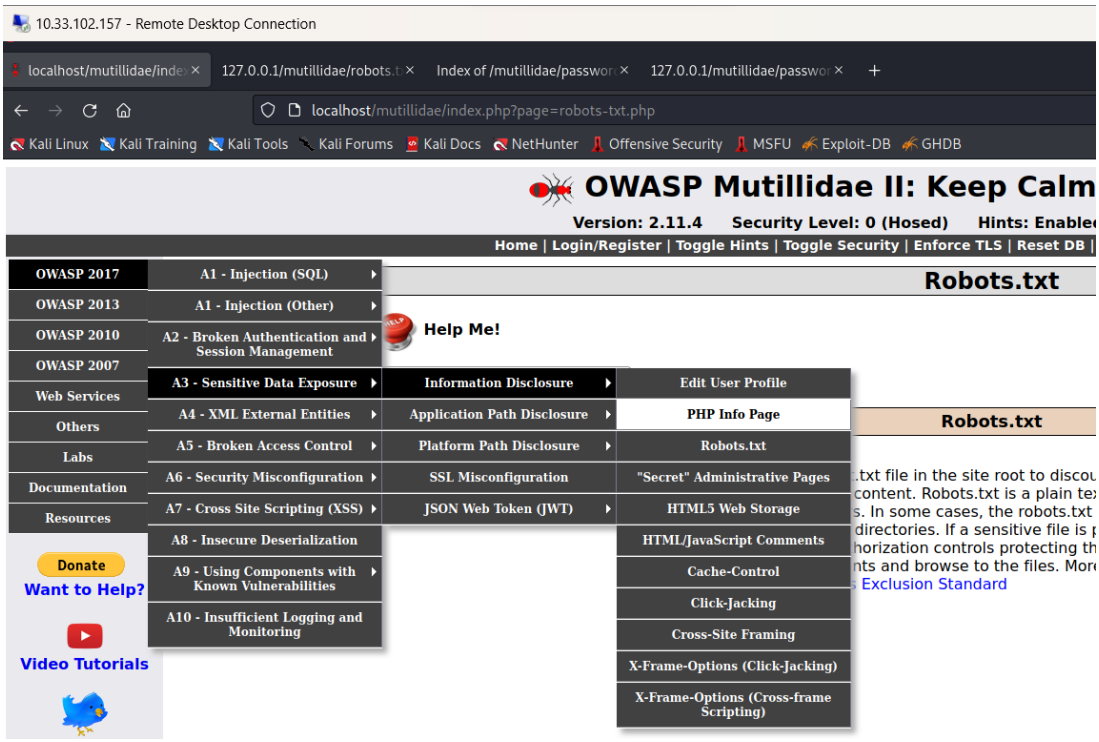
4. Buka folder *passwords.*

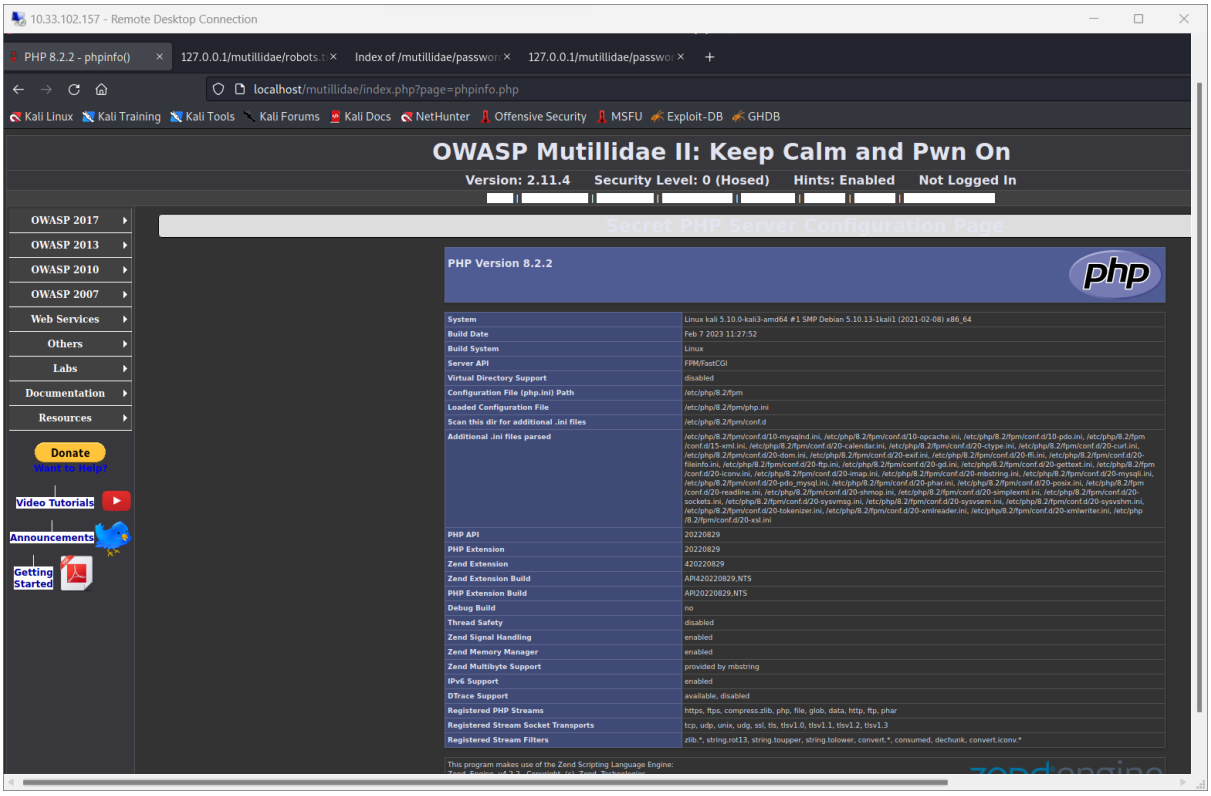


5. Buka file *accounts.txt.*



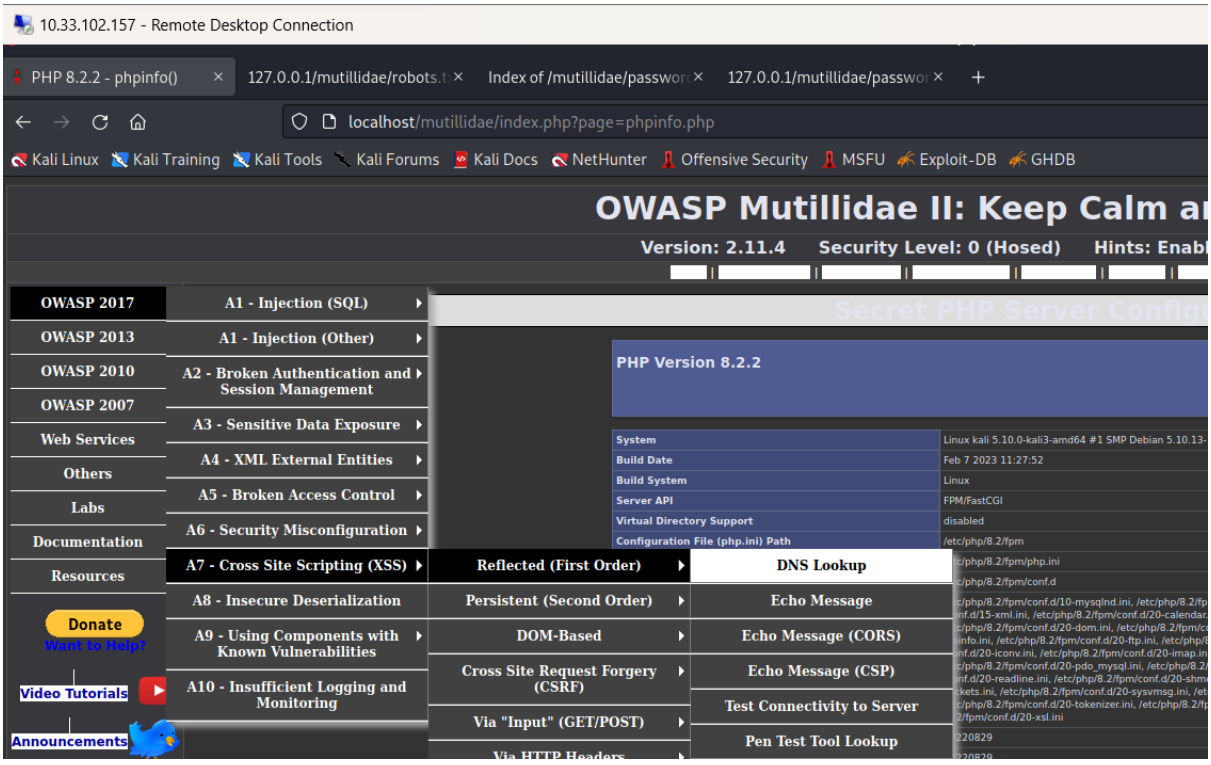
6. Untuk mengecek data *sensitive* ter-*expose* buka owsp 2017 > *Sensitive Data Exposure* > *Information Disclosure* > *php info page.*



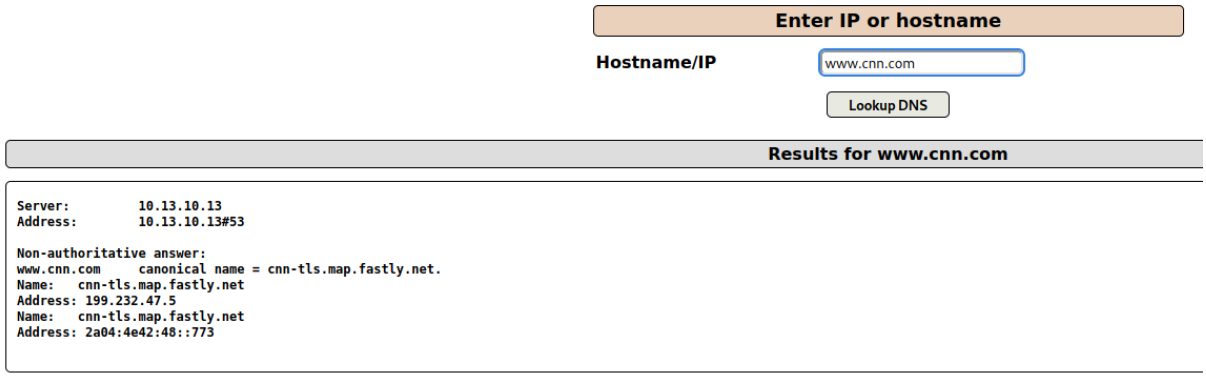


D. ***Basic Command Executing Testing***

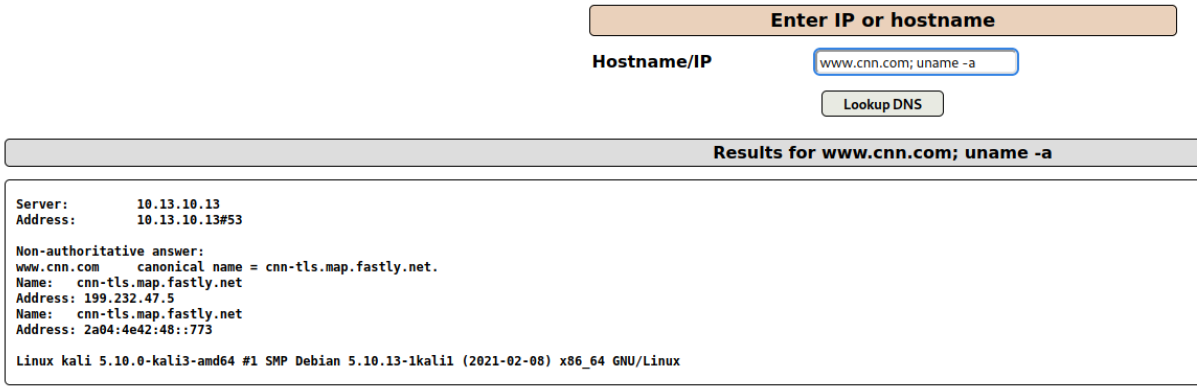
1. Akses OWASP Top 10 > A7 – *Cross Site Scripting* (XSS) > *Reflected* (*First Order*) > DNS *Lookup*.



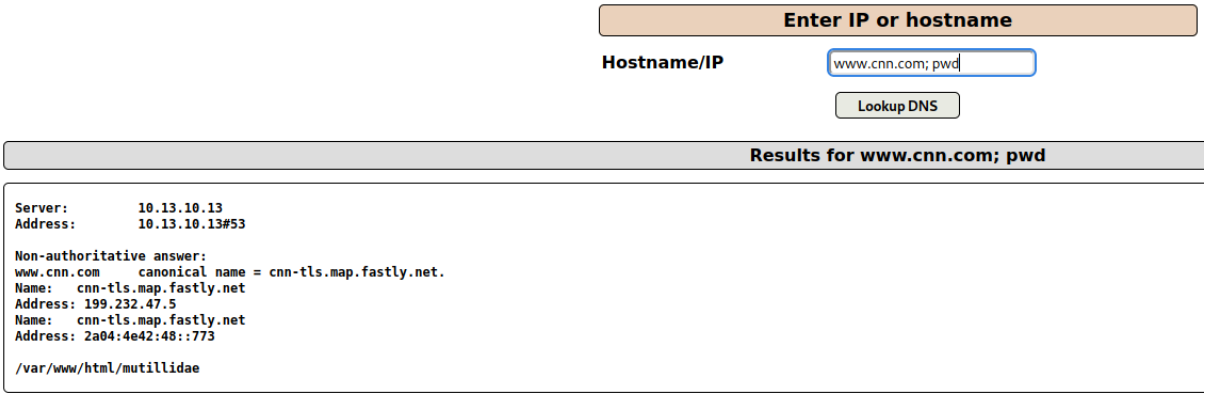
2. Tes DNS *Lookup*.



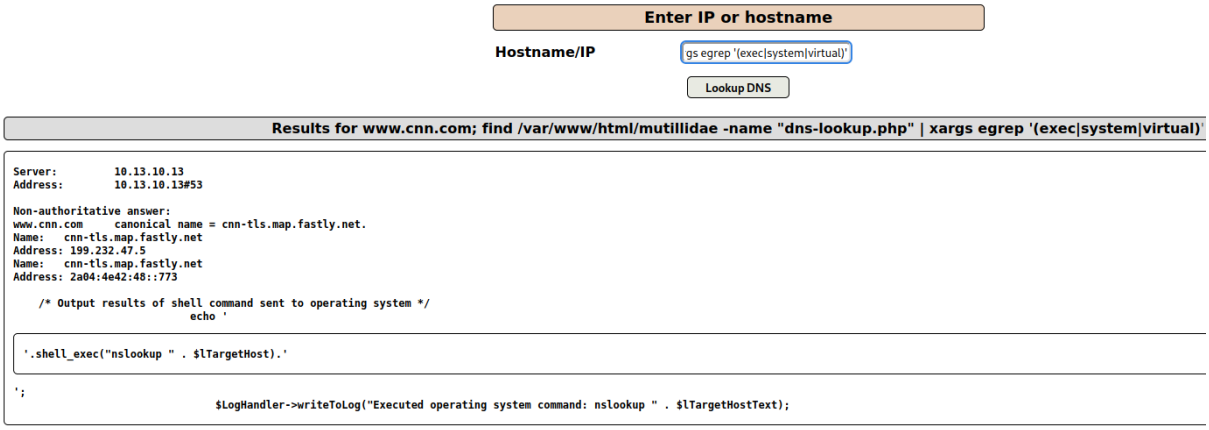
3. Uji kerentanan pencarian DNS.



4. Pengujian Pengintaian/*Reconnaissance.*

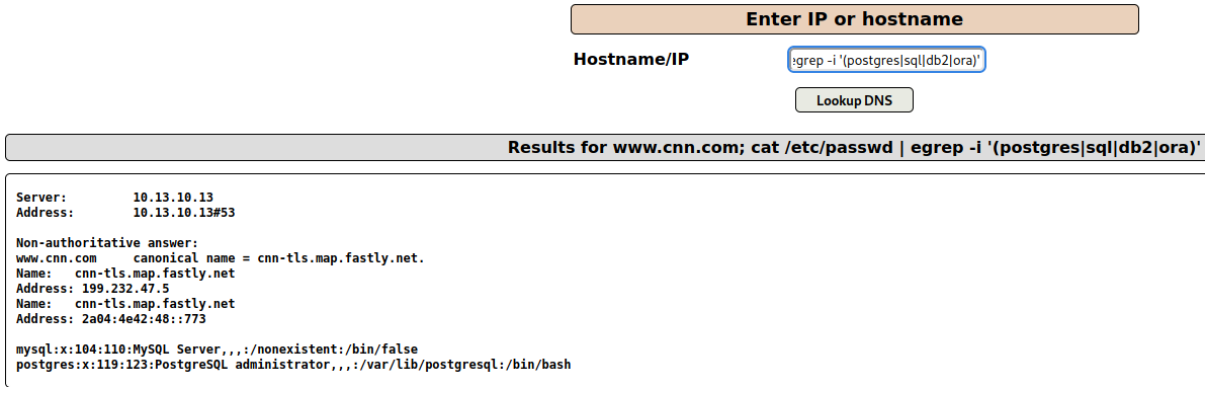


5. Analisis Forensik aplikasi dns-lookup.php.

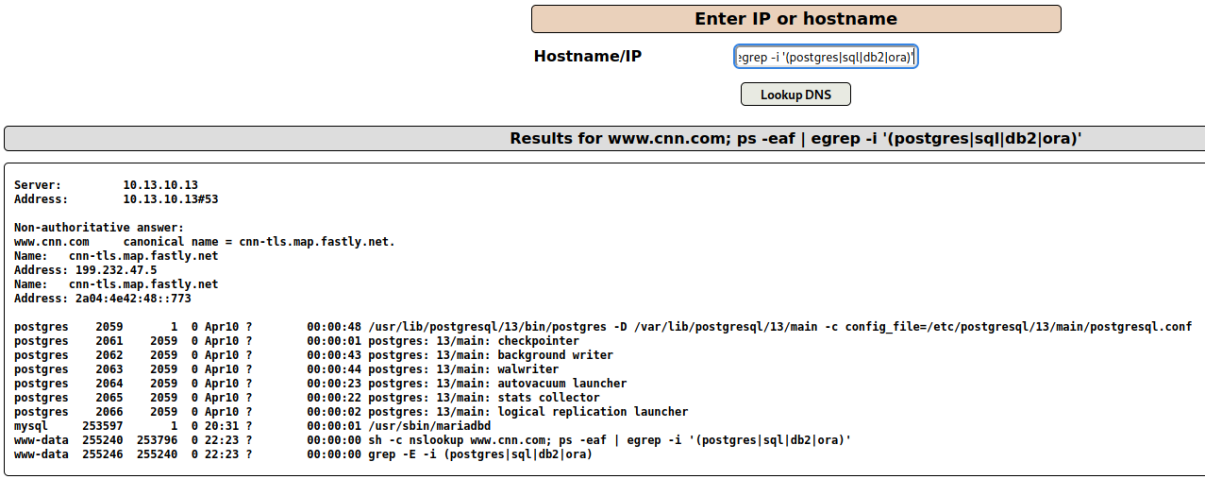


E. *Database Reconnaissance*

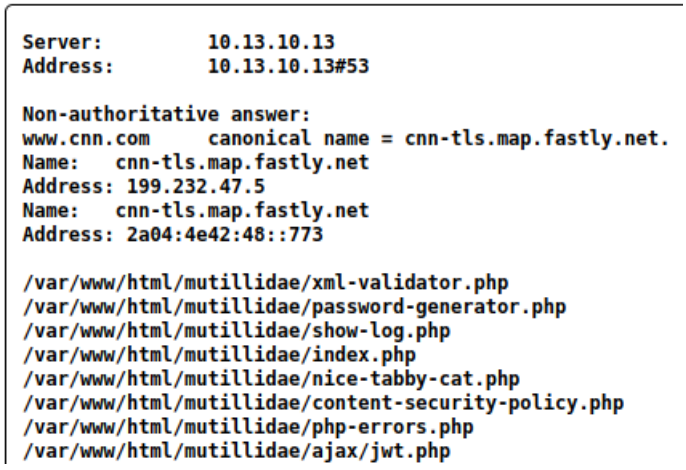
1. Temukan *Database* menggunakan *file* /etc/passwd.



2. Temukan Mesin *Database* menggunakan perintah “ps”.



3. Melihat Daftar semua *Script* Php.



Enter IP or hostname

Hostname/IP /html/mutillidae -name "*.php"

Lookup DNS

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/jwt.php
/var/www/html/mutillidae/repeater.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
```

4. Cari php untuk kata sandi *string*.

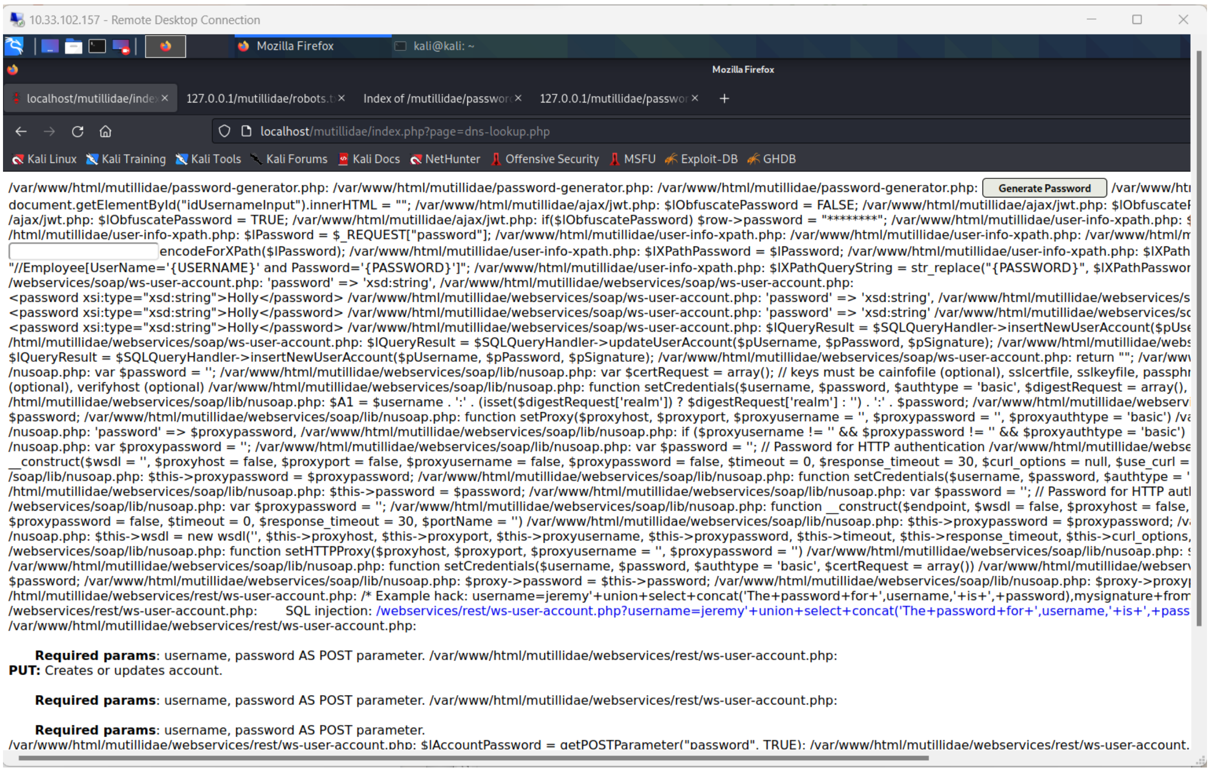
Enter IP or hostname

Hostname/IP s grep -i "password" | grep "="

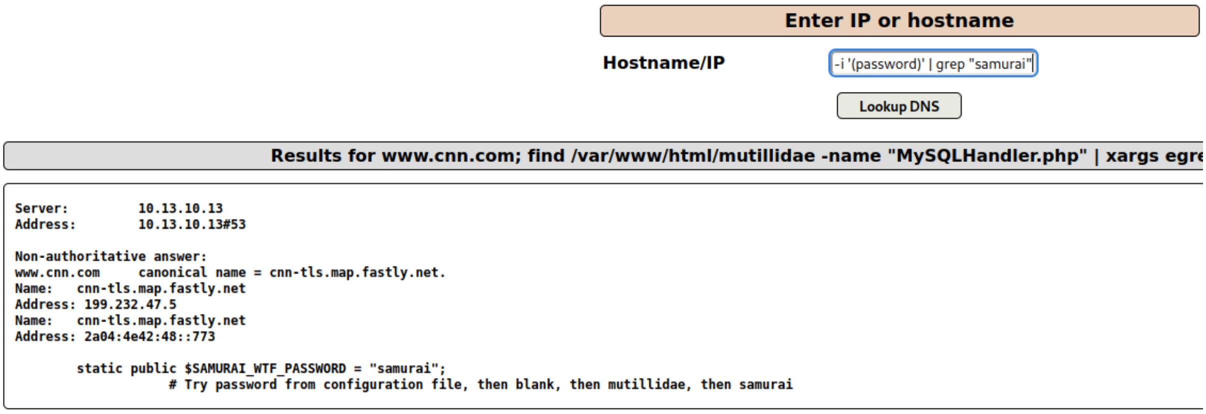
Lookup DNS

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

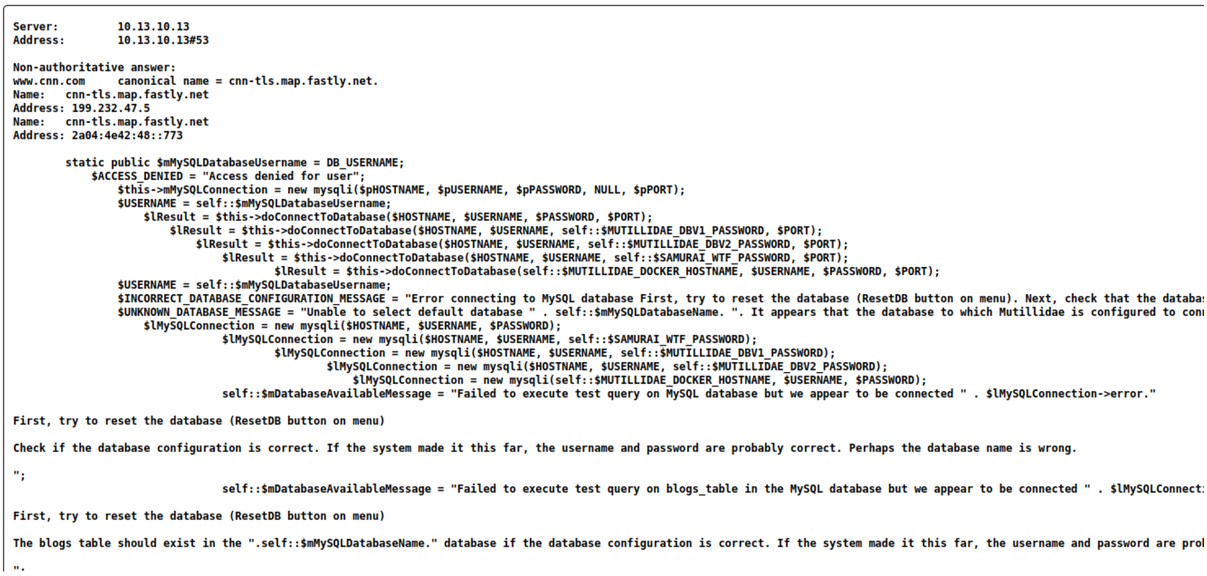
```
Server:         10.13.10.13
Address:        10.13.10.13#53

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:                $lPasswordJSMessage = "";
/var/www/html/mutillidae/password-generator.php:                        $lPasswordJSMessage = "This password is for {$lUsernameForJS}";
/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 = "";
/var/www/html/mutillidae/password-generator.php:
                                        Password Generator
/var/www/html/mutillidae/password-generator.php:
```



5. Dapatkan kata sandi dari hasil pencarian.



6. Cari MySQLHandler.php untuk pengguna string atau login.



V. Pembahasan

Pada praktikum ini, melakukan percobaan *web footprinting*. Sebelum melakukan serangan, lakukan beberapa persiapan seperti menggunakan MySQL dan menyambungkannya ke DBMS atau *Database Management System* (dalam hal ini menggunakan MariaDB), kemudian membuat *database* mutillidae. Selanjutnya pada terminal Kali mulai beberapa layanan seperti PHP-FPM untuk memproses skrip PHP, Apache untuk melayani permintaan HTTP, dan MySQL untuk manajemen basis data. Layanan-layanan tersebut penting dalam *stack* teknologi *web*. Lalu lakukan inisialisasi terhadap *database.*

Pertama, dilakukan praktik *Data Exposed* dengan *file* robots.txt. *Data exposed* atau pengungkapan data adalah situasi di mana data sensitif atau rahasia dapat diakses oleh pihak yang tidak berwenang atau publik secara tidak sengaja. Setelah mengakses robots.txt, ditemukan referensi terhadap *folder* "passwords" dan *file* "accounts.txt". Hal ini menunjukkan adanya potensi pengungkapan informasi sensitif melalui robots.txt. Saat melakukan percobaan, *folder passwords* berhasil diakses dan *file* accounts.txt dapat dilihat isinya. Hal ini menunjukkan adanya praktik *data exposed* yang serius, di mana data sensitif seperti kata sandi atau informasi akun dapat diakses oleh publik secara tidak sah. Selanjutnya dilakukan pengecekan terkakit sensitivitas *data exposure*, dimana ditemukan *file* yang memuat data sensitif dan dapat diakses tanpa otorisasi yang sesuai. Ini menunjukkan adanya praktik data.

Kedua, melakukan *Basic Command Execution Testing* atau pengujian eksekusi perintah dasar adalah sebuah metode pengujian keamanan yang bertujuan untuk mengidentifikasi celah keamanan yang terkait dengan eksekusi perintah yang tidak aman pada aplikasi *web* atau sistem. Pada praktikum ini, pengujian dilakukan pada menu DNS *Lookup*.

Terakhir, *database reconnaissance* atau pengintai *database* merujuk pada proses pengumpulan informasi tentang sistem basis data yang dimiliki oleh suatu organisasi atau entitas. Aktivitas-aktivitas dalam *database reconnaissance* biasanya meliputi identifikasi jenis dan versi basis data, pemindaian *port* dan layanan, enumerasi pengguna, mencari informasi sensitif, dan analisis eksternal. Pada praktikum ini, *database reconnaissance* dilakukan dengan menemukan *database* menggunakan file /etc/passwd, menemukan mesin *database* menggunakan perintah "ps", melihat daftar semua *script* php, mencari php untuk kata sandi *string*, mendapatkan kata sandi dari hasil pencarian, dan mencari MySQLHandler.php untuk pengguna *string* atau *login*.

VI. Kesimpulan

1. Praktik data *exposed* dapat dinilai serius jika data sensitif seperti kata sandi atau informasi akun dapat diakses oleh publik secara tidak sah.
2. Melalui langkah-langkah *database reconnaissance*, jenis dan versi basis data yang digunakan oleh sistem target dapat diidentifikasi.

VII. Daftar Pustaka

Iqbal, Muhammad. (2022). *Praktek Footprinting*. Diakses pada 12 Mei 2023 dari https://miqbal.staff.telkomuniversity.ac.id/praktek-footprinting/#:~:text=Website%20Footprinting%20%3A%20Teknik%20ini%20mengacu,dan%20rekayasa%20sosial%20lebih%20lanjut.