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

- Dapat memahami pengujian *data exposed*.
- Dapat memahami pengujian *basic command execution testing*.
- Dapat memahami pengujian *database reconnaissance*.

II. Latar Belakang

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 & Bahan

- *Software Remote Dekstop Connection*
- OS VM 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

┌──(kali㉿kali)-[~]
└─$ sudo mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
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 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
```

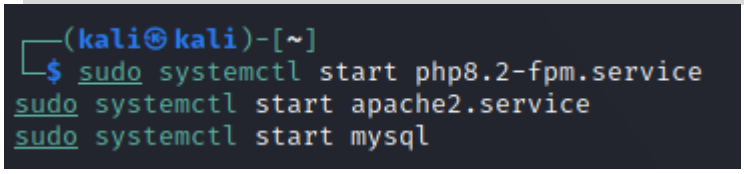
B. INSTALL OWASP Mutillidae II

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

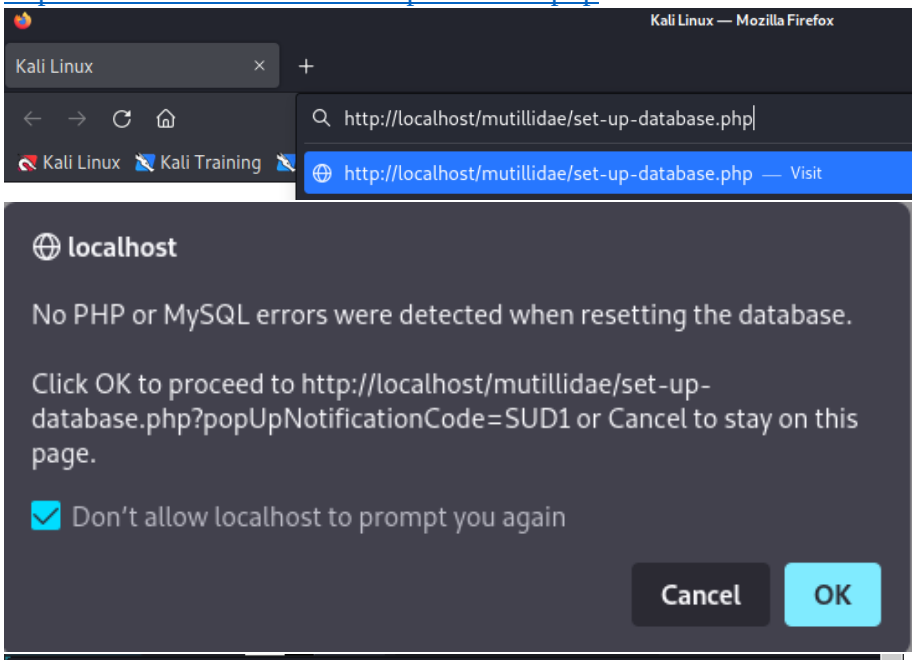
```
MariaDB [(none)]> CREATE DATABASE mutillidae;
ERROR 1007 (HY000): Can't create database 'mutillidae'; database exists
MariaDB [(none)]>
```

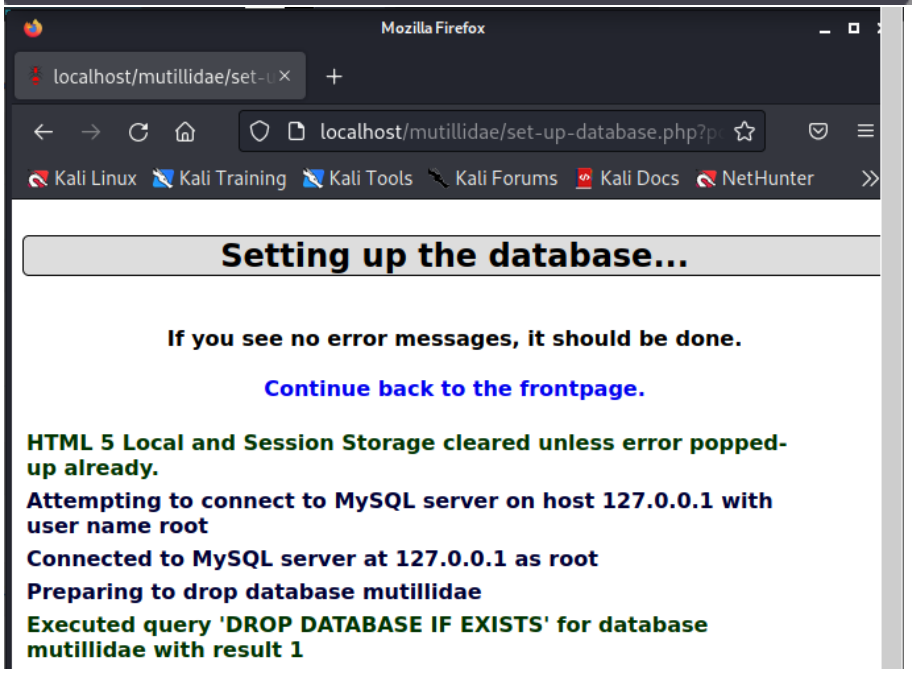
2. Karena database mutillidae telah tersedia, maka jalankan perintah berikut

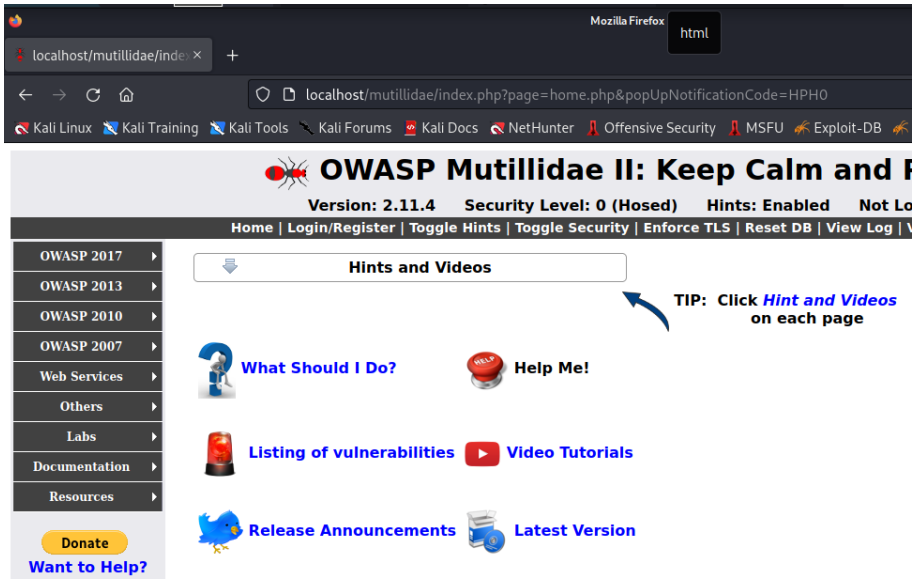
```
sudo systemctl start php8.2-fpm.service
sudo systemctl start apache2.service
sudo systemctl start mysql
```



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

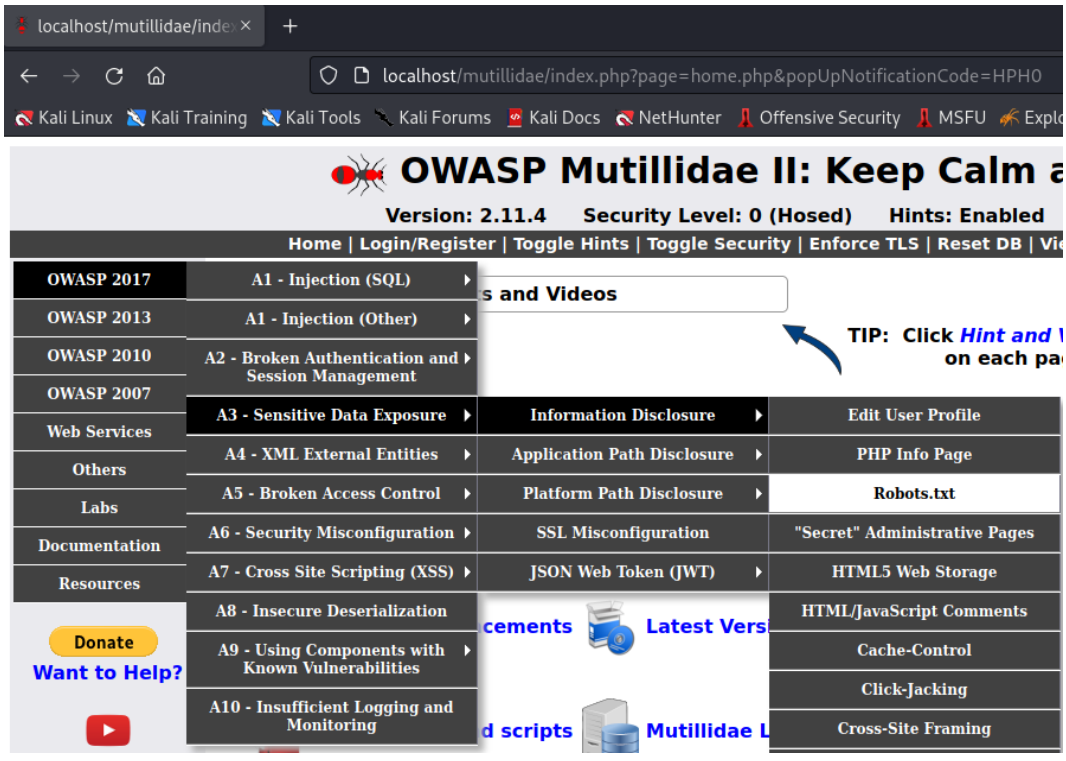




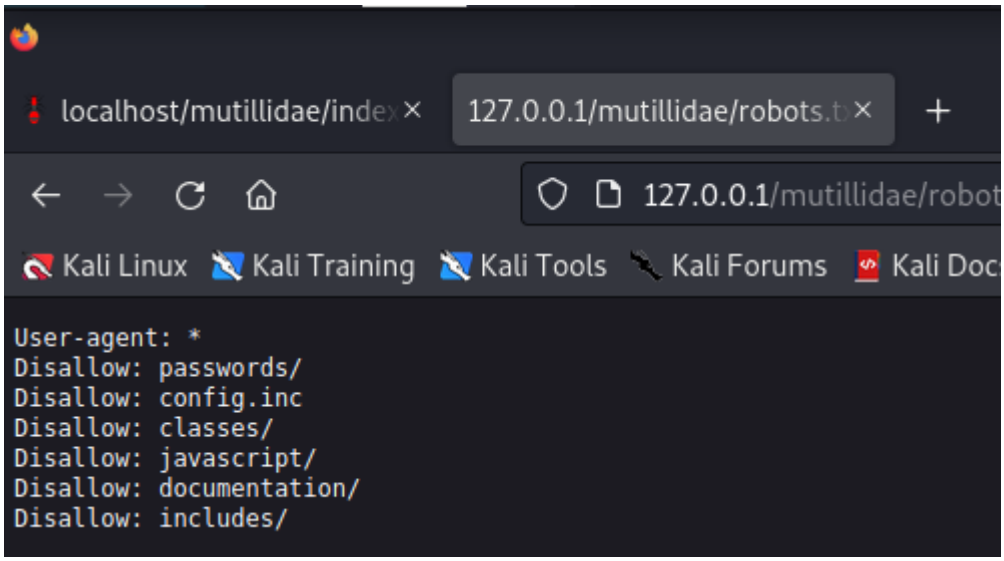


C. PRAKTIK DATA EXPOSED DENGAN ROBOT FILE

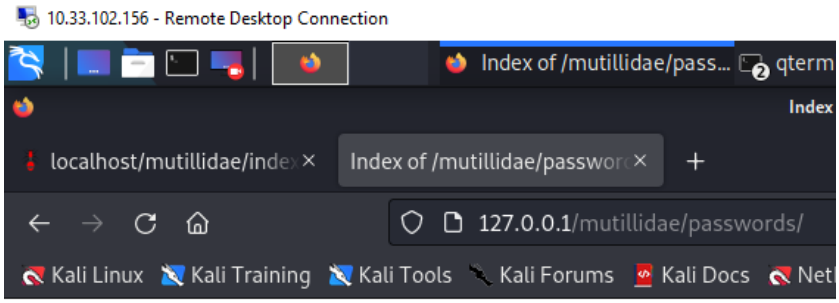
1. Buka jendela mutillidae
2. Pilih menu OWASP 2017 > *sensitive data exposure* > *Information Disclosure* > Robots.txt



3. Akses Robots.txt melalui browser



4. Buka folder *password*

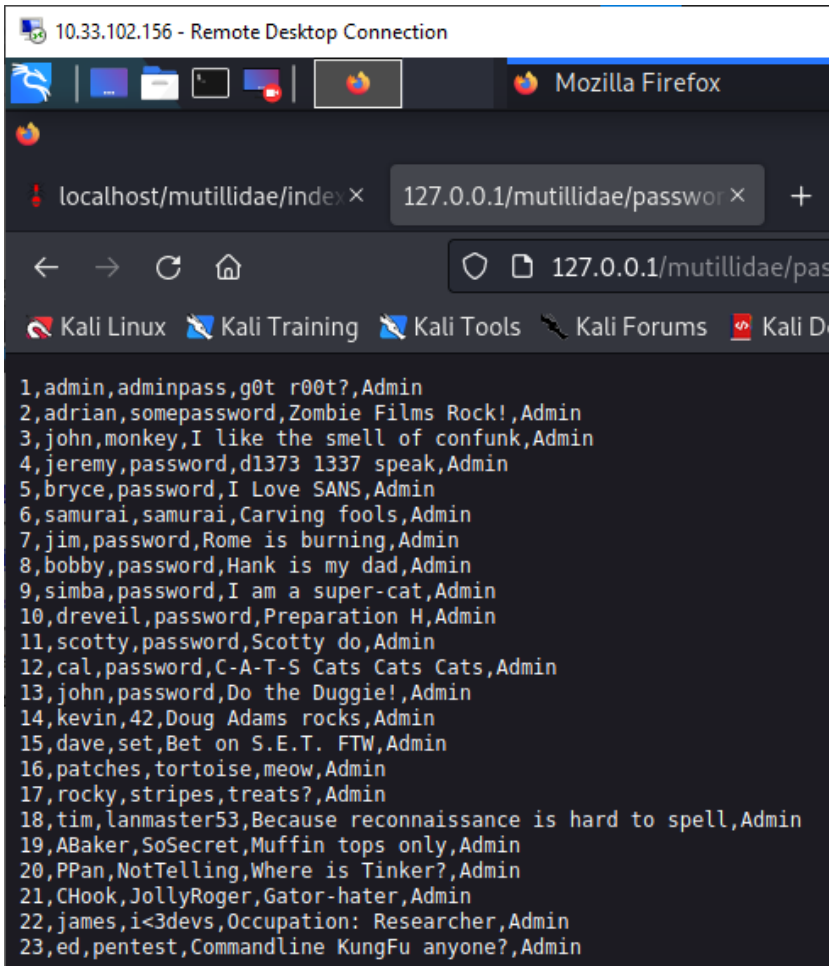


Index of /mutillidae/passwords

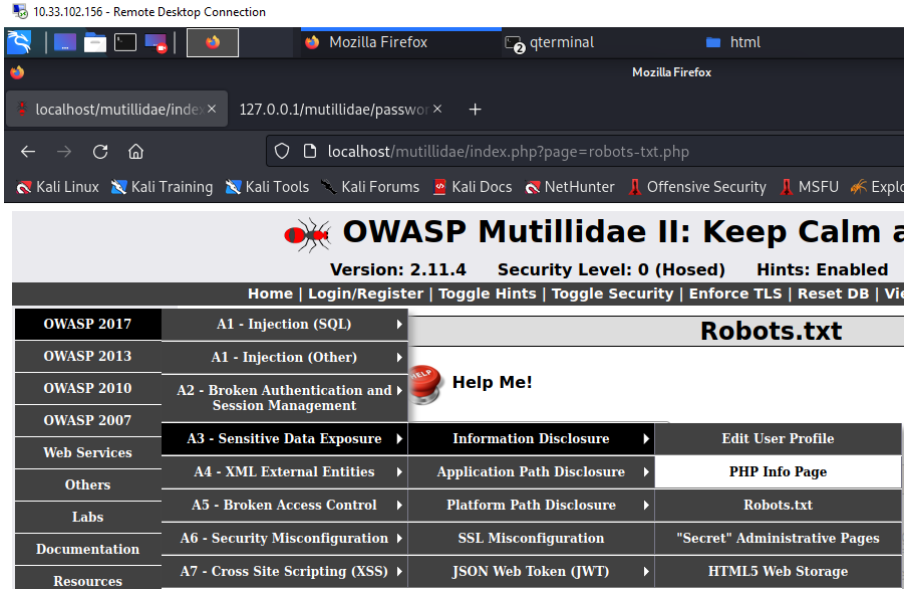
Name	Last modified	Size	Description
Parent Directory		-	
accounts.txt	2023-05-08 20:40	929	

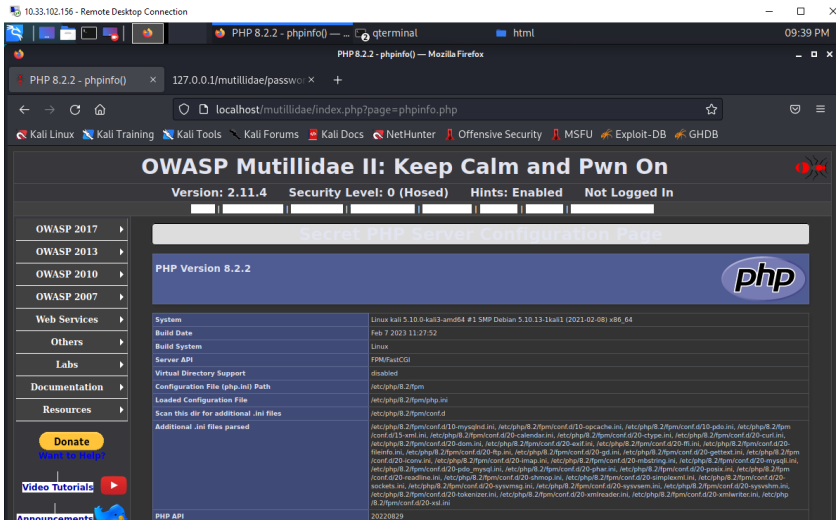
Apache/2.4.46 (Debian) Server at 127.0.0.1 Port 80

5. Buka file accounts.txt



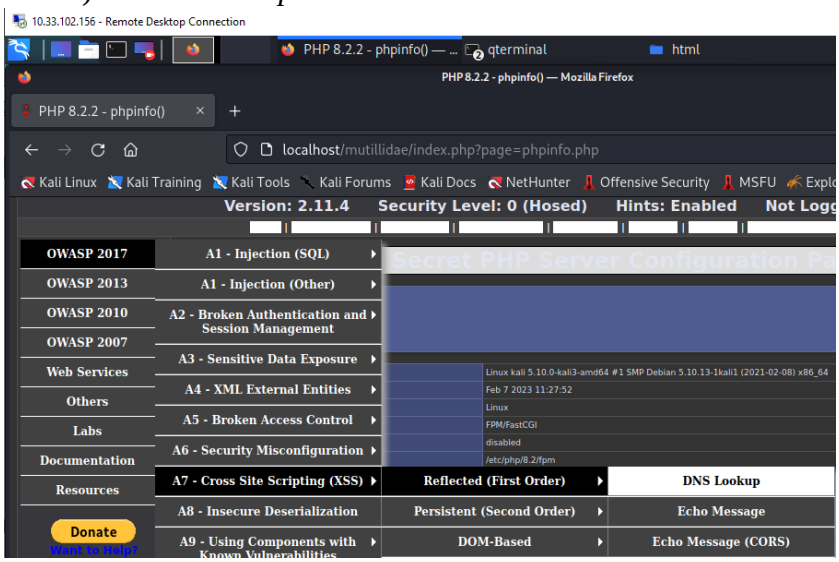
6. Untuk mengecek data sensitive terekspose buka owsp 2017 > *Sensitive Data Exposure* > *Information Disclosure* > php info page



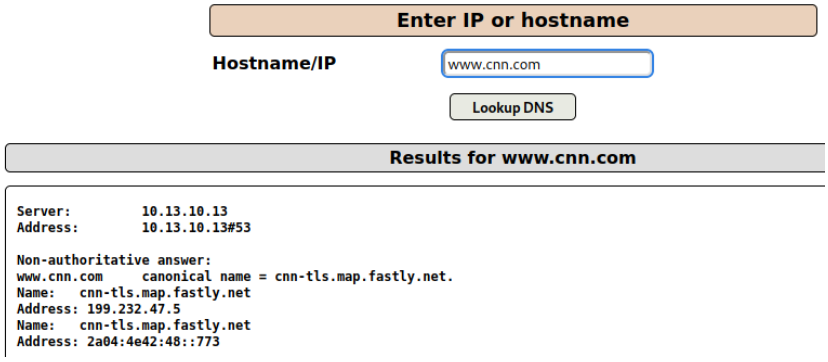


D. Bassic Command Executing Testing

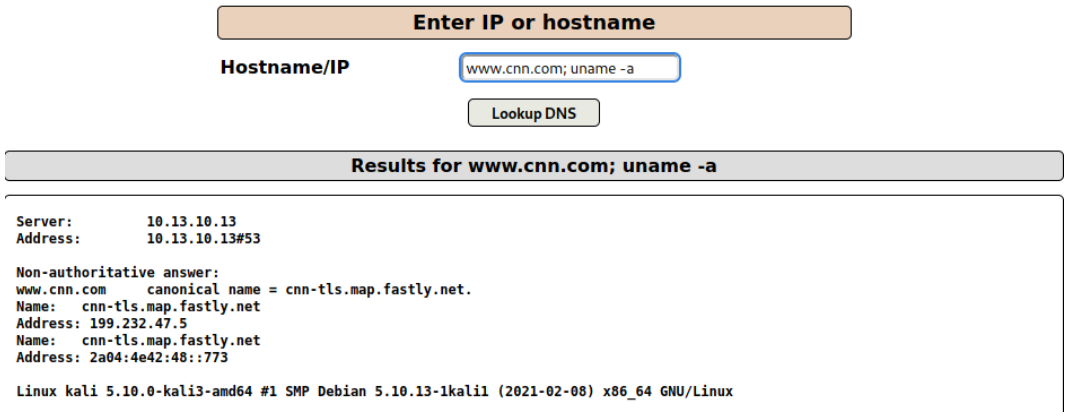
1. Akses OWASP Top 10 > A7 - *Cross Site Scripting* (XSS) > *Reflected* (*First Order*) > DNS *Lookup*



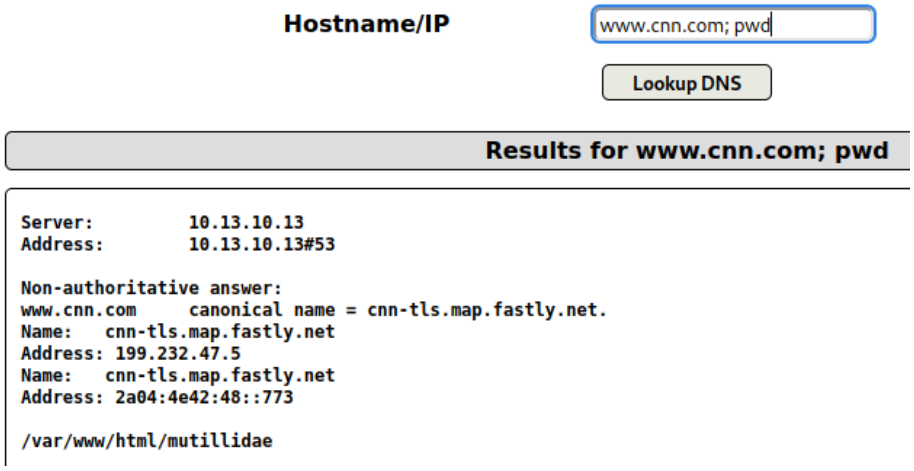
2. Tes DNS Lookup



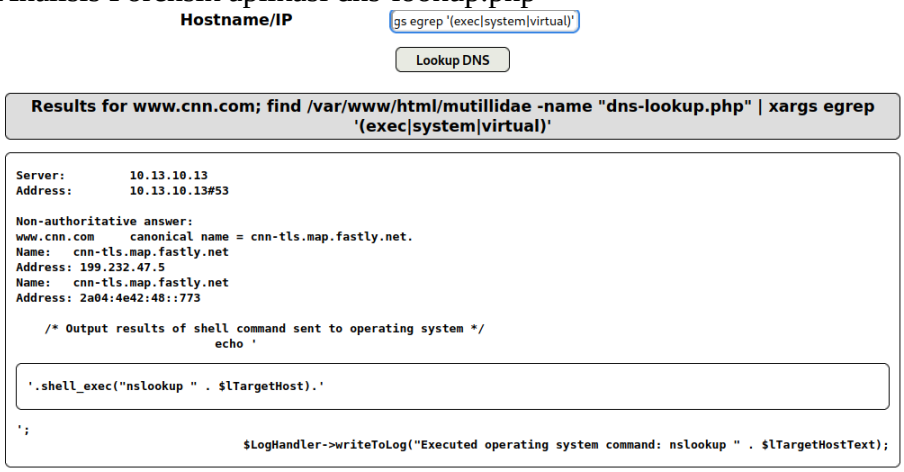
3. Uji kerentanan pencarian DNS



4. Pengujian Pengintaian/Reconnaissance

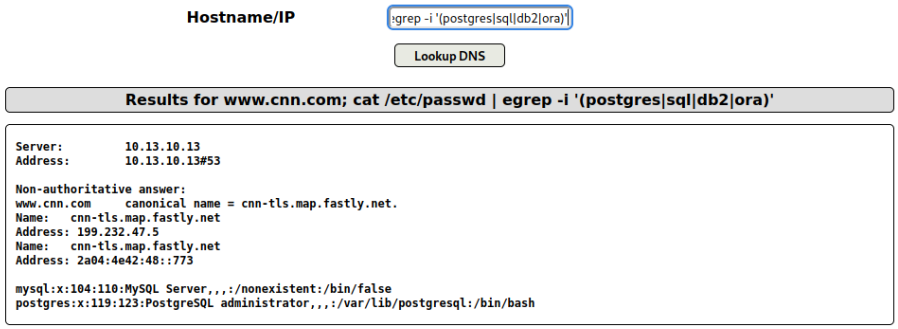


5. Analisis Forensik aplikasi dns-lookup.php

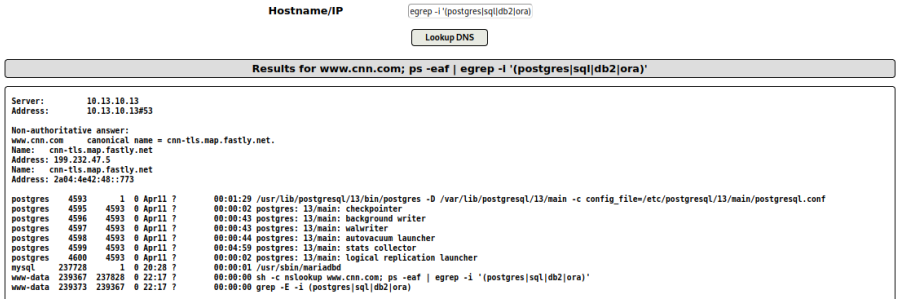


E. Database Reconnaissance

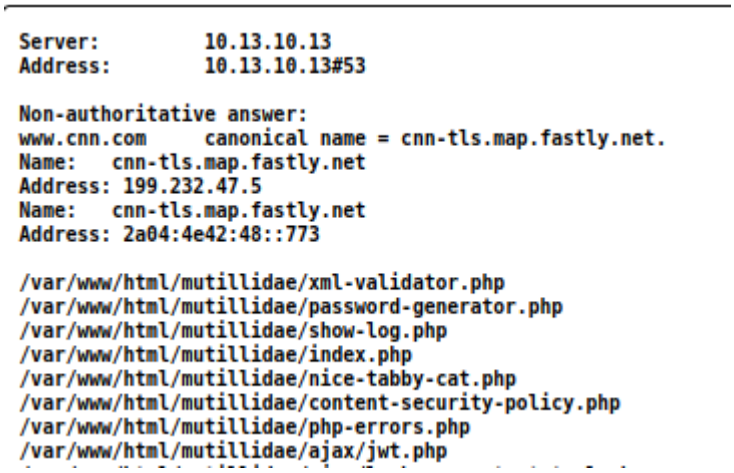
1. Temukan Database menggunakan file /etc/passwd

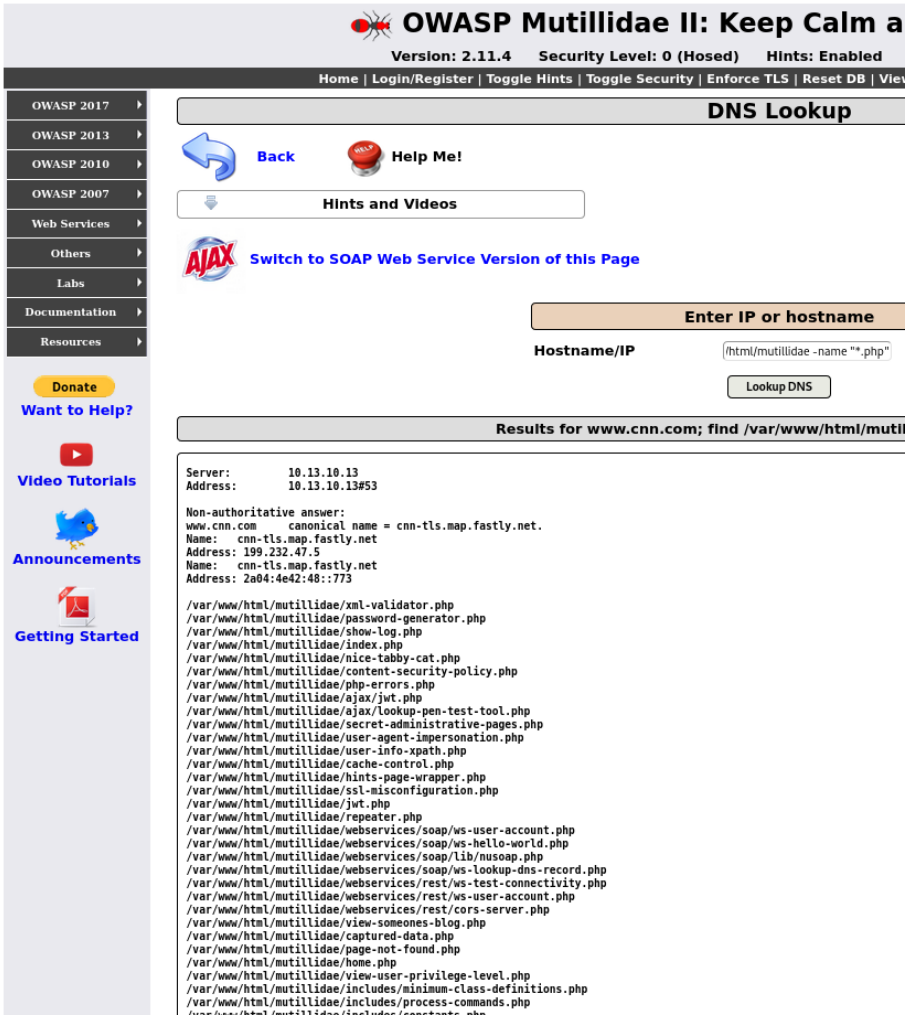


2. Temukan Machine Database menggunakan perintah “ps”

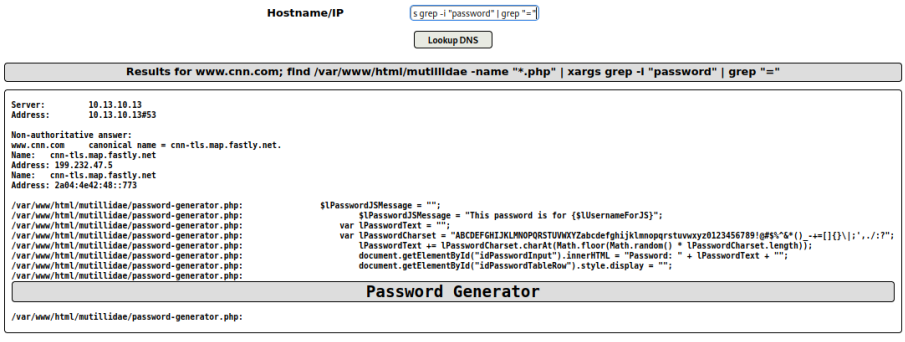


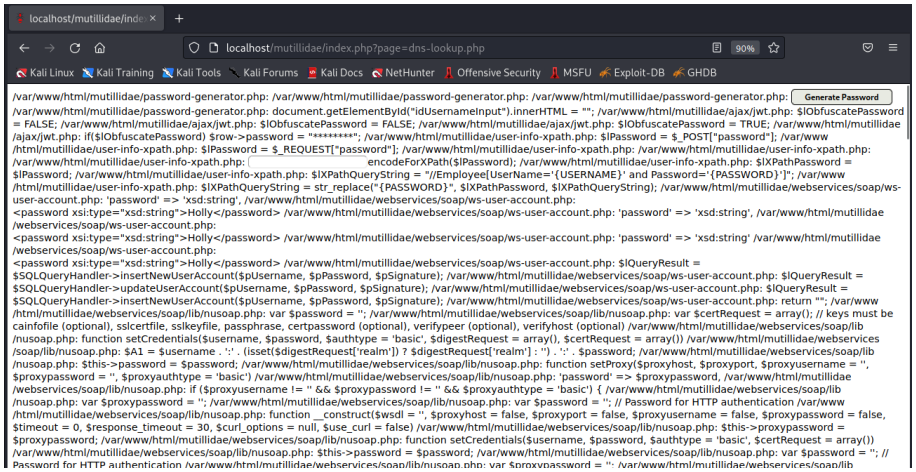
3. Melihat Daftar semua Script Php



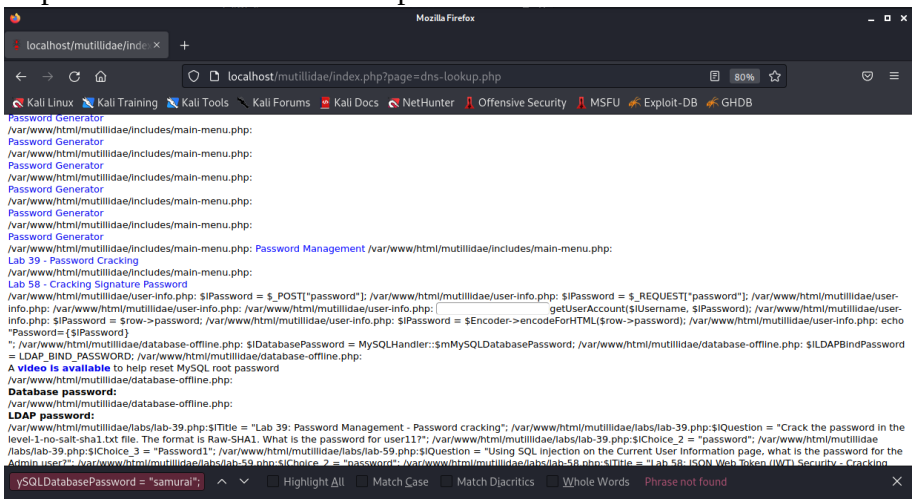


4. Cari php untuk kata sandi string

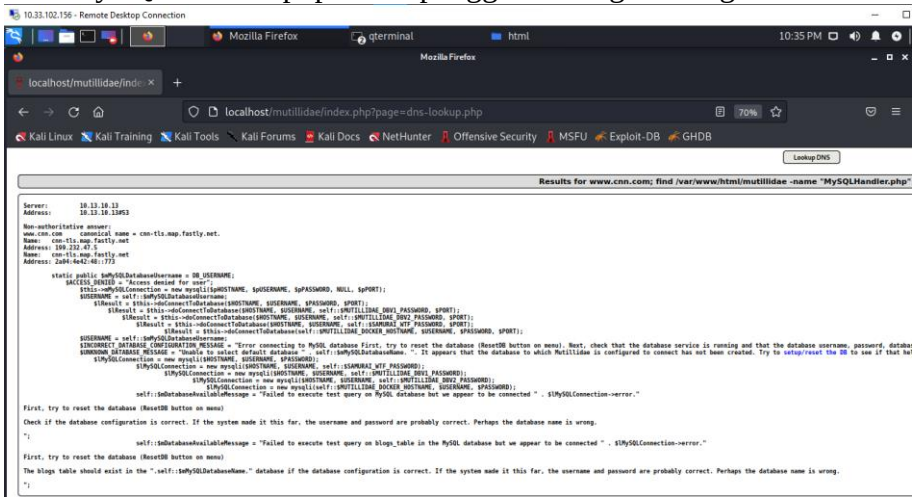




5. Dapatkan kata sandi dari hasil pencarian



6. Cari MySQLHandler.php untuk pengguna string atau login



V. Pembahasan

Pada praktikum ini mahasiswa akan melakukan percobaan *web footprinting*. Sebelum melakukan serangan, perlu dilakukan beberapa persiapan seperti menggunakan MySQL dan menyambungkannya ke *Database Management System*, kemudian membuat *database* baru bernama mutillidae. Selanjutnya pada terminal Kali Linux jalankan beberapa layanan seperti PHP-FPM untuk memproses skrip PHP, Apache untuk melayani permintaan HTTP, dan MySQL untuk manajemen basis data. Lalu lakukan inisialisasi *database* ke situs mutillidae dengan tautan http://localhost/mutillidae/set-up-database.php.

Percobaan pertama adalah praktik *Data Exposed* dengan *file* robots.txt. *Data exposed* merupakan kondisi dimana data atau informasi tidak dilindungi dengan baik, sehingga penyerang berkesempatan untuk mengeksploitasi dan mencuri data. Setelah mengakses robots.txt, ditemukan path folder yang di dalamnya memuat informasi mengenai akun dan password pengguna. Hal ini menunjukkan adanya potensi pengungkapan informasi sensitif melalui robots.txt. Saat melakukan percobaan, folder *passwords* berhasil diakses dan isi *file* accounts.txt dapat dilihat dengan mudah tanpa enkripsi apapun. Hal ini menunjukkan adanya praktik *data exposed* yang serius, dimana data sensitif akun dan *password* 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.

Web footprinting kedua yaitu melakukan percobaan *Basic Command Execution Testing*, dimana pengujian ini merupakan 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*.

Percobaan terakhir yaitu *database reconnaissance*. *Database reconnaissance* merupakan proses pengumpulan informasi tentang sistem (dalam hal ini adalah basis data) yang dimiliki oleh suatu organisasi atau entitas secara diam-diam. 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

Pada praktikum kali ini dapat disimpulkan bahwa :

1. Web *footprinting* merupakan tahap awal untuk mengumpulkan informasi tentang target berupa pemantauan dan analisis situs web.
2. Kita dapat menemukan informasi-informasi penting pada suatu situs web yang tidak dilindungi oleh keamanan dari situs tersebut menggunakan pengujian seperti *web exposed* seperti pengujian yang dilakukan pada praktikum ini.

VII. Daftar Pustaka

Iqbal, M. (*unknown*). Praktek Footprinting. Retrieved May 15, 2023, from https://miqbal.staff.telkomuniversity.ac.id/praktek-footprinting/

Surantha, N. (February 09,2018). SENSITIVE DATA EXPOSURE. Retrieved May 15, 2023, from https://mti.binus.ac.id/2018/02/09/sensitive-data-exposure/#:~:text=Sedangkan%20pengertian%20data%20exposure%20adalah,untuk%20mengekploitasi%20dan%20mencuri%20data.

Blumira. (*unknown*). Reconnaissance. Retrieved May 15, 2023, from https://www.blumira.com/glossary/reconnaissance/