# Practice5

**1094841** 李昱佑

## Stored XSS

先在/var/www/html 新增一個目錄 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。


在目錄中新增一個 cookie.txt，用來記錄被害者的 cookies。

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
```

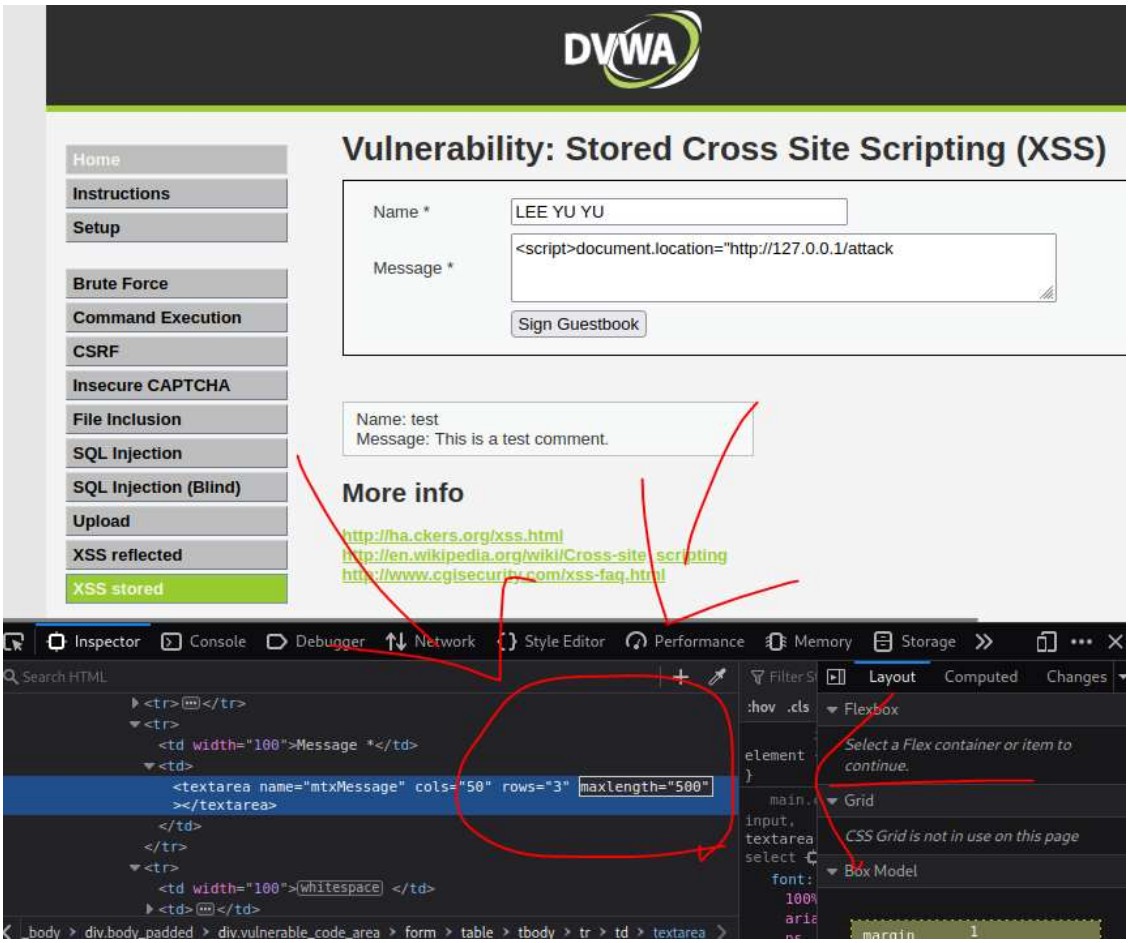
開啟 apache 網頁伺服器，使攻擊者可藉由此網站蒐集被害者的 cookies

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

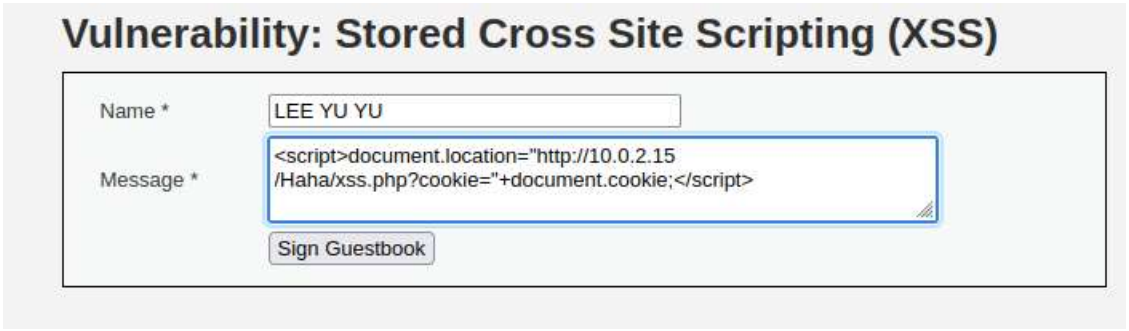
查看伺服器的 IP

```
┌──(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 noprefixr
oute eth0
       valid_lft 833sec preferred_lft 833sec
    inet6 fe80::caf4:8ae5:f0b6:fa2d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

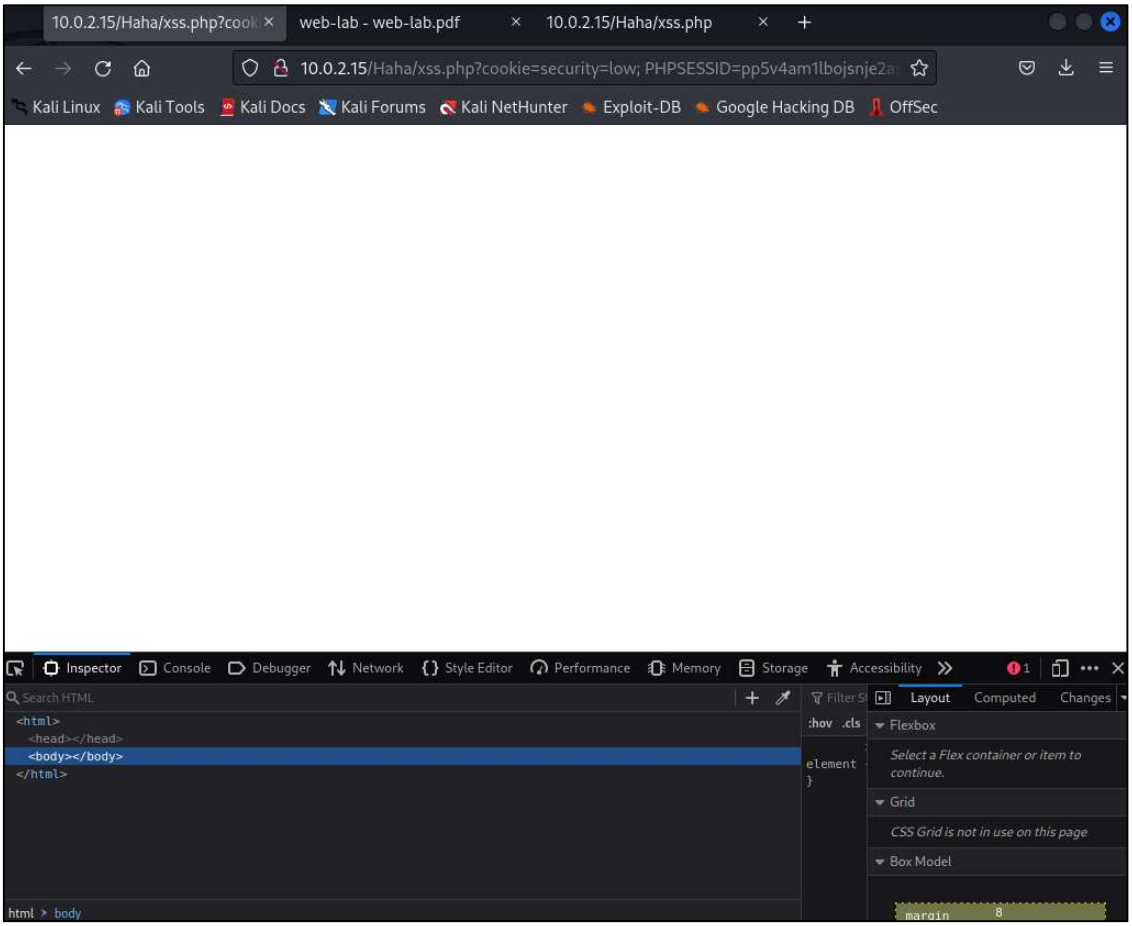
攻擊者來到有漏洞的網站，並修改前端 html 對於輸入的長度限制




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)



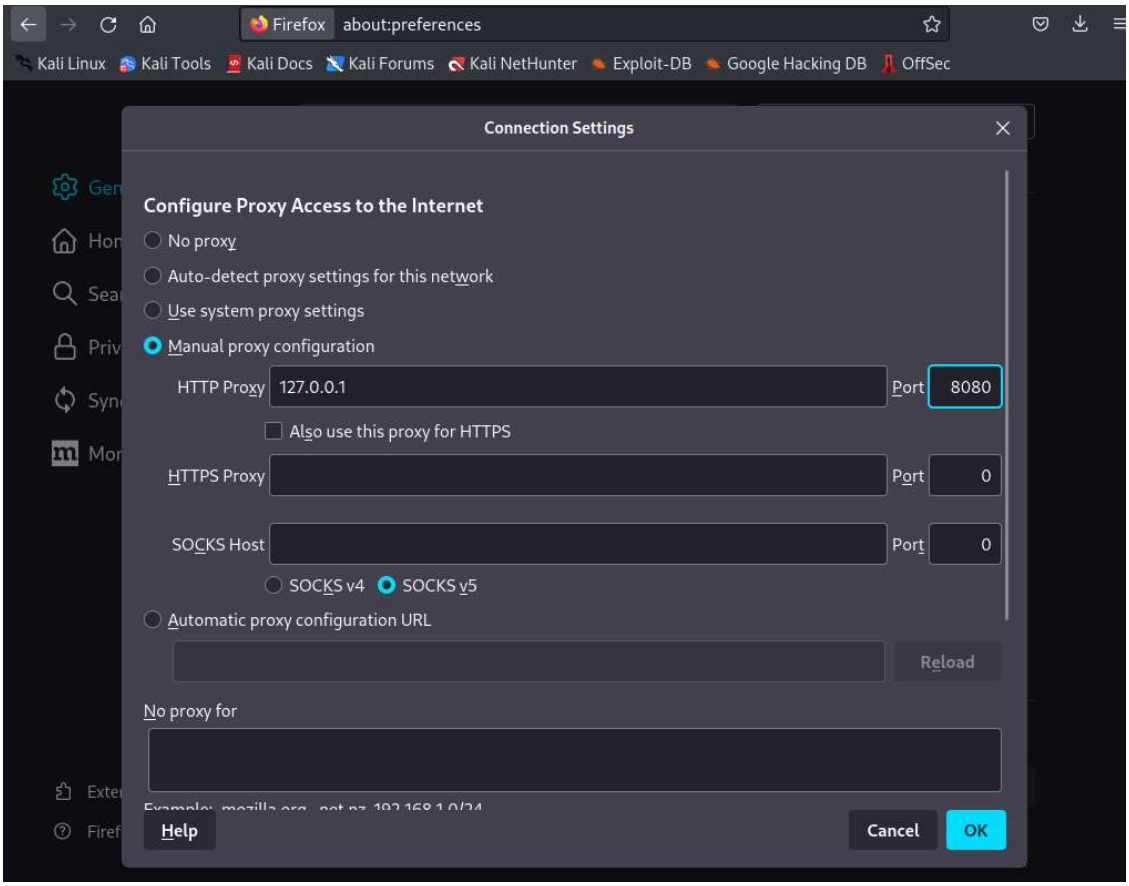
被害者會被導向到攻擊者的網站



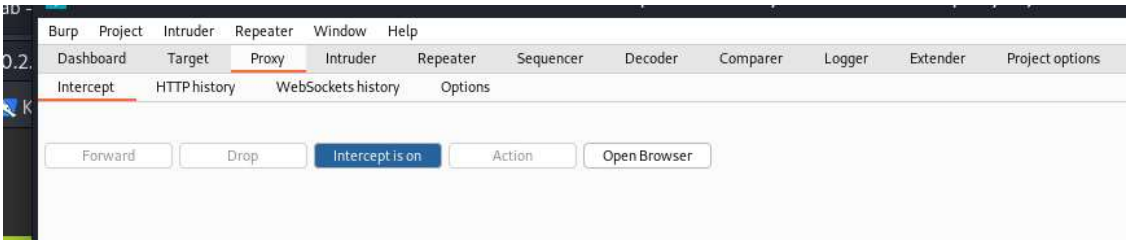

同時，被害者的 cookie 會被寫入攻擊者伺服器中的 cookie.txt

# Burp Suite

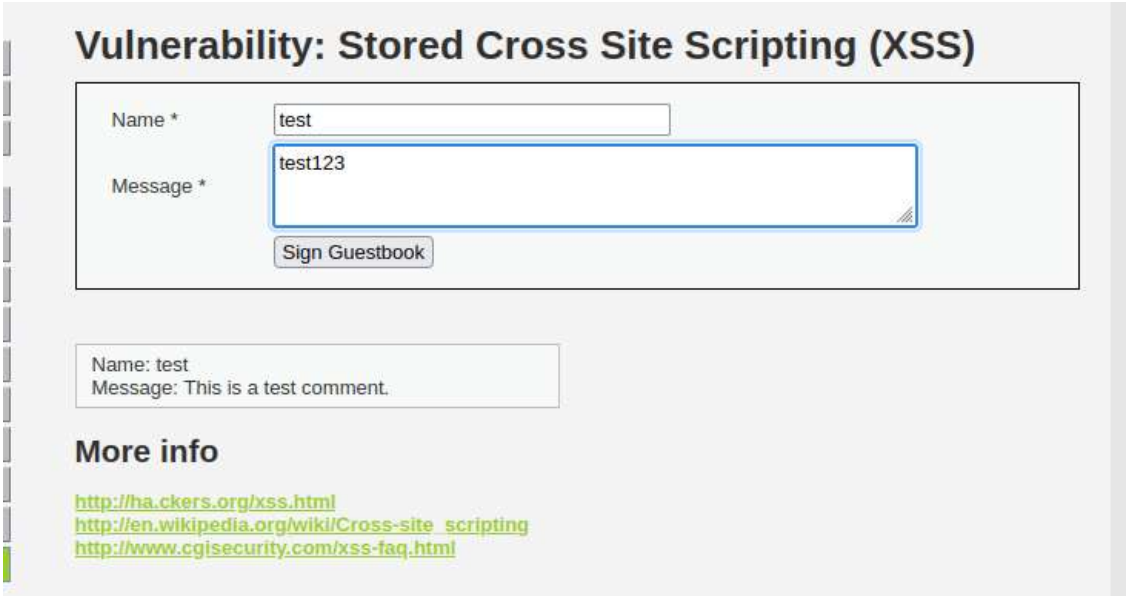
先設定 local proxy




將攔截開啟

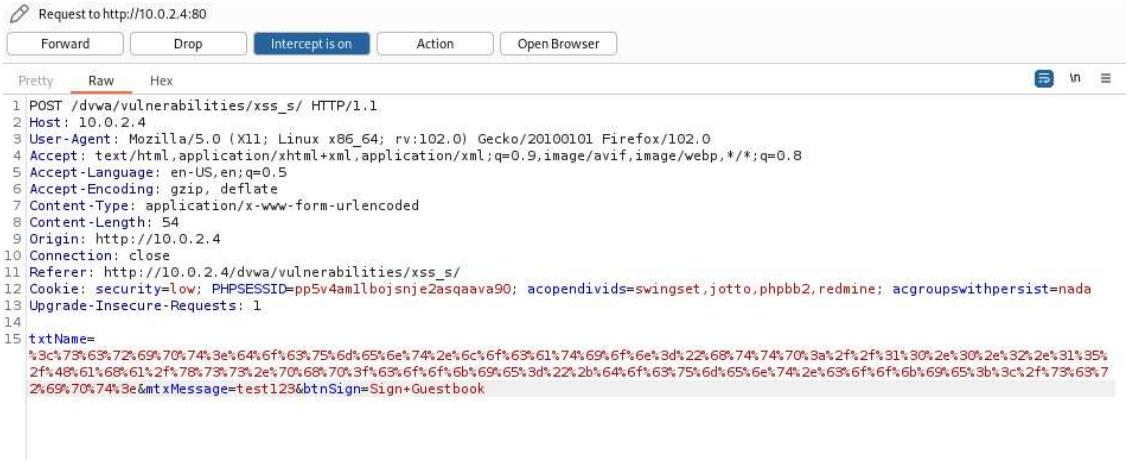


隨意輸入並 submit

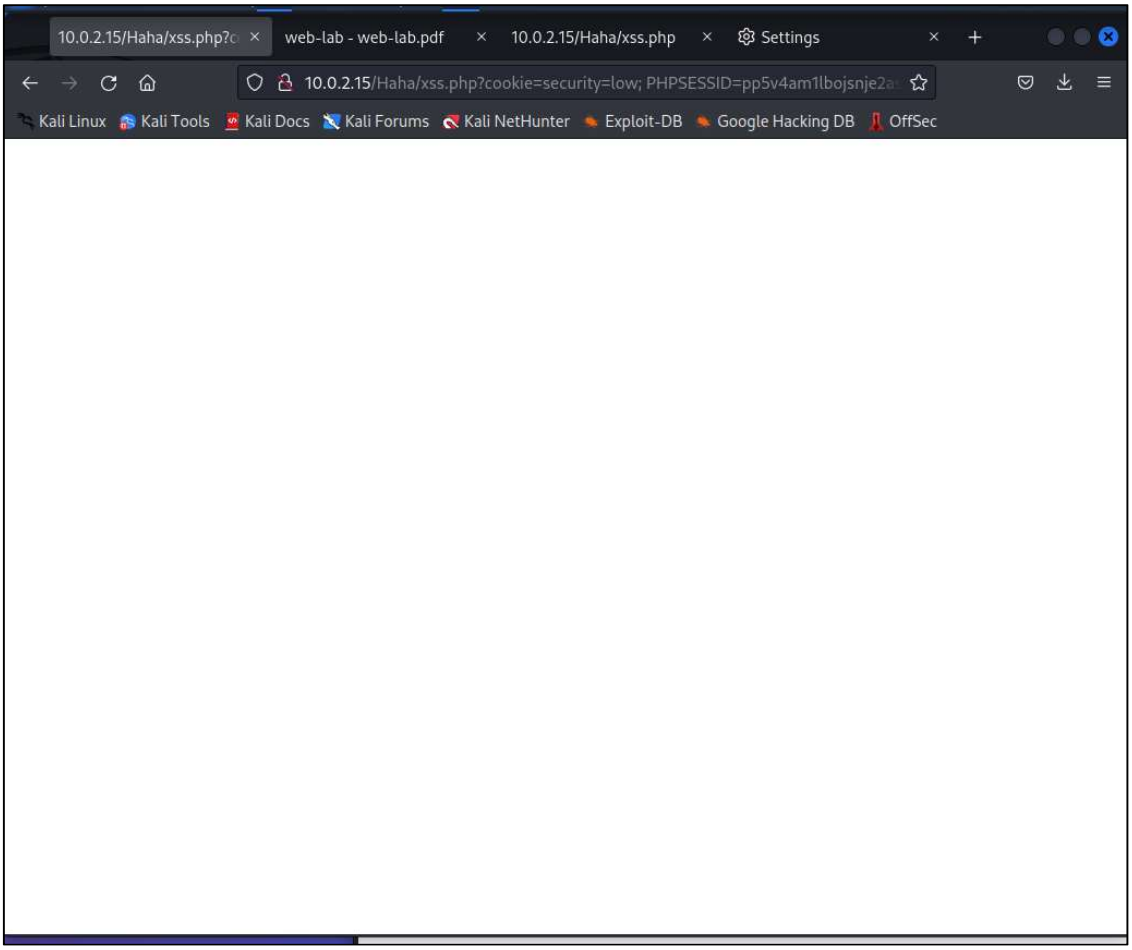



將我們的惡意輸入編碼成 URL


修改我們的封包，將 name 改為我們剛剛編碼的 URL



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