359度防护网站

发表于 2021-03-05 分类于 Challenge， 2020， SWPU CTF 2020， Web
Challenge | 2020 | SWPU CTF 2020 | Web | 359度防护网站

点击此处获得更好的阅读体验

WriteUp来源

官方WP

题目考点

- *SQL注入*

解题思路

常规解

网站目录下有常见遗留文件`robots.txt`与`index.php.bak`

bak文件中是base64 解开后得到`important_index_its_so_long_right.php?id=1`页面

3.在上面得到的页面中直接进行联合注入得到所有数据库名，表，字段及内容

```
1 http://182.150.46.187:8802/important_index_its_so_long_right.php?id=1' and 1=2 union select 1,2,3,group_concat(SCHEMA_NAME) from information_schema.SCHEMATA-- -
```

分别查询LTLT库和h1nt库得到LTLT库中的login表，里面有`pwd,usn`，usn 是`admin123`,pwd是md5,在somd5查询得到`w1lm@123`

```
1 http://182.150.46.187:8802/important_index_its_so_long_right.php?id=1' and 1=2 union select 1,2,3,group_concat(pwd) from login-- -
```

h1nt库中是help表，里面有hint，内容是一个页面名，访问后提示先登录，但是并没有给登录地址，所用会话也不是与 administrator.html 相同，所以这条路先暂停

```
1 http://182.150.46.187:8802/important_index_its_so_long_right.php?id=1' and 1=2 union select 1,2,3,group_concat(hint) from h1nt.help --
```

利用得到的 usn和pwd登录进入robots.txt中的`administrator.html`

进去后是一个后台，翻看页面后发现无明显可利用点，查看源码发现憨憨开发注释掉的部分

访问`writeuser_00001_log.log`后得到一页的base64，丢burp解码，找到可疑页面`up_lo_ad_ad_min.php`

访问发现要登录，但是只有一条信息需要验证，F12发现有输入长度限制为5，猜测是前面log页面中的`user:00001`

登录成功后发现是一个文件上传点,很多师傅在这里上传了很久都没成功，其实在现在的开发中，只要合理运用白名单，基本就能防死文件上传，这里文件上传的后端验证就是白名单，只能上传`jpg,png,gif`，所以理论上无法传马

先上传一个正常图片，得到如下信息

之前在h1nt库中拿到的`last_index_come_on_swpu_ctf.php?id=4`页面现在发现可以进去了，这个页面的登录验证就是用的密码是00001的那个页面，进去后发现可以直接sql注入

getshell的常规方法中，利用sql语句的`into outfile`并不算罕见，只是由于很多情况下`secure_file_priv`并未设置，导致无法进行这类文件读写，但是这在渗透中仍然不应该是被忘记的一种方法，没有尝试就不能凭经验否定这种方法。我们尝试写入一句话，但是考虑到目录可能没有可写权限，我们需要找到一个确定有可写权限的文件夹，很容易联想到上传页面暴漏的文件夹就有可写权限，于是构造语句写入一句话

利用木马文件进行命令执行`system('cat /flag');`即可获得flag

非预期

出题时本意是在前台页面用WAF防死SQL注入，但是由于WAF版本未及时更新，有少数师傅用load_file将文件暴力读取了,类似这种

- ***本文作者：** CTFHub*
- ***本文链接：** https://writeup.ctfhub.com/Challenge/2020/SWPU-CTF-2020/Web/a8JazxMqf3EwaNFZLjGHNk.html*

 # Challenge # 2020 # Web # SWPU CTF 2020
Super Brain
RealEzRE