

安全-你必须让他停下 (BugkuCTF)

原创

小狐狸FM  于 2021-07-07 17:54:29 发布  53  收藏 1

分类专栏: [安全 # CTF夺旗](#) 文章标签: [web ctf 安全](#)

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/smallfox233/article/details/118517274>

版权



[安全](#) 同时被 2 个专栏收录

91 篇文章 9 订阅

订阅专栏



[CTF夺旗](#)

38 篇文章 0 订阅

订阅专栏

文章目录

- [一、题目](#)
- [二、WriteUp](#)

一、题目

I want to play Dummy game with others;But I can't stop!
Stop at panda ! u will get flag

CTF

@

Harry

<https://blog.csdn.net/smallfox233>

二、WriteUp

目标机器每隔一段时间就会发送不同的信息过来，需要使用 **burpsuite** 抓包
获取到请求报文后，将报文转到 **Repeater** 模块中

The screenshot shows the Burp Suite Repeater window. The title bar reads "Burp Intruder Repeater Window Help". The menu bar includes "Target", "Proxy", "Spider", "Scanner", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Extender", "Project options", "User options", and "A". The "Intercept" tab is active, showing "HTTP history", "WebSockets history", and "Options". Below the tabs, there is a "Request to http://114.67.246.176:15835" section with buttons for "Forward", "Drop", "Intercept is on", and "Action". The "Raw" tab is selected, displaying the following request details:

```
GET / HTTP/1.1
Host: 114.67.246.176:15835
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

A context menu is open over the request, listing various actions. The "Send to Repeater" option is highlighted, with the keyboard shortcut "Ctrl+R" displayed next to it. Other options include "Send to Spider", "Do an active scan", "Send to Intruder (Ctrl+I)", "Send to Sequencer", "Send to Comparer", "Send to Decoder", "Request in browser", "Engagement tools [Pro version only]", "Change request method", "Change body encoding", "Copy URL", "Copy as curl command", "Copy to file", and "Paste from file".

<https://blog.csdn.net/smallfox233>

- 在 **Repeater** 模块中，点击 **Go** 就能发送报文给目标服务器
如果 **Go** 按钮变暗，可以点击一下取消按钮 **Cancel**，再点 **Go**
- 因为服务器返回的页面是不固定的，所以需要多次发送
右侧的 **Response** 就是返回页面的 **html** 信息

Go Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project opti

10 x 11 x ...

Go Cancel < >

Request

Raw Headers Hex

```
GET / HTTP/1.1
Host: 114.67.246.176:15835
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

Raw

<https://blog.csdn.net/smallfox233>

操作多次后，可以获取到其中的一个返回页面含有 **flag**

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Tue, 06 Jul 2021 03:37:53 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.6
Vary: Accept-Encoding
Content-Length: 638
Connection: close
Content-Type: text/html
```

```
<html>
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta name="description" content="">
<meta name="author" content="">
<title>Dummy game</title>
</head>

<script language="JavaScript">
function myrefresh(){
window.location.reload();
}
setTimeout('myrefresh()',500);
</script>
<body>
<center><strong>I want to play Dummy game with others;But I can't stop!</strong></center>
<center>Stop at panda ! u will get flag</center>
<center><div></div></center><br><a
style="display:none">flag{0274f1dd21a1aa1fc9306c823d58c5e6}</a></body>
</html>
```

<https://blog.csdn.net/smallfox233>



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)