




# 攻防世界web新手之cookie

原创

彬彬逊  于 2019-04-19 21:56:25 发布  5884  收藏 6

分类专栏: [ctf总结](#) 文章标签: [ctf](#) [攻防世界](#)

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\\_40481505/article/details/89408819](https://blog.csdn.net/qq_40481505/article/details/89408819)

版权



[ctf总结](#) 专栏收录该内容

43 篇文章 1 订阅

订阅专栏

## 攻防世界web新手之cookie

背景知识cookie: [HTTP cookie 详解](#)

打开题目链接, 提示我们查看cookie, cookie是HTTP协议中的一个重要参数, (对HTTP协议不是很熟悉的friends可以看看这个[“HTTP协议其实就是这么简单”](#))

查看cookie的方法有很多, 可以[通过浏览器查看](#), 不过建议直接查看HTTP报头, 以加深对HTTP协议的理解。

此处使用Burpsuit进行抓包，结果如下

The screenshot shows the Burp Suite interface. At the top, there is a table titled "Contents" with the following data:

Host	Method	URL	Params	Sta...	Length	MIM
http://111.198.29.45...	GET	/	<input type="checkbox"/>	200	663	HTM
http://111.198.29.45...	GET	/cookie.php	<input type="checkbox"/>	200	669	HTM

Below the table, there are tabs for "Request" and "Response". Under "Request", there are sub-tabs for "Raw", "Params", "Headers", and "Hex". The "Raw" tab is selected, showing the following HTTP request:

```
GET / HTTP/1.1
Host: 111.198.29.45:30216
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:66.0)
Gecko/20100101 Firefox/66.0
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
Connection: close
Cookie: look-here=cookie.php
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
```

At the bottom of the interface, there is a search bar with the text "Type a search term" and a search button. The search results show "0 matches".

发现cookie值提示访问cookie.php，于是进一步访问111.198.29.45:30216/cookie.php

得到提示查看response

**Contents**

Host	Method	URL	Params	Sta...	Length	MIM
http://111.198.29.45...	GET	/	<input type="checkbox"/>	200	663	HTM
http://111.198.29.45...	GET	/cookie.php	<input type="checkbox"/>	200	669	HTM

Request Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Fri, 19 Apr 2019 13:13:30 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
flag: xctf( [REDACTED] )
Vary: Accept-Encoding
Content-Length: 411
Connection: close
Content-Type: text/html
```

[https://blog.csdn.net/qq\\_40481508](https://blog.csdn.net/qq_40481508)

得到flag

[附Burpsuit安装教程burpsuite1.7 安装及简单介绍](#)



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)