




Cookie 攻防世界

原创

今天不学习，明天变腊鸡  已于 2022-04-14 17:02:10 修改  2189  收藏

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

于 2022-04-07 11:23:04 首次发布

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_53568983/article/details/124009863

版权



[笔记](#) 同时被 2 个专栏收录

29 篇文章 0 订阅

订阅专栏



[CTF](#)

3 篇文章 0 订阅

订阅专栏

1. 第一步还是看题:



The screenshot shows a CTF challenge interface for a challenge named "cookie". At the top, it has a title "cookie" with a thumbs-up icon and the number "2", and a note "最佳Writeup由神秘人·孔雀翎提供". There are two buttons: "WP" and "建议". Below the title, the "难度系数" (Difficulty Coefficient) is shown as "★ 1.0". The "题目来源" (Source) is "Cyberpeace-n3k0". The "题目描述" (Description) says: "X老师告诉小宁们在cookie里放了东西, 小宁疑惑地想: '这是夹心饼干的意思吗?'". The "题目场景" (Scenario) is "http://111.200.241.244:50280". There is a progress bar and a "删除场景" (Delete Scenario) button. The "倒计时" (Timer) is "03:40:22" with a "延时" (Extend) button. Below the timer, it says "题目附件: 暂无" (No attachments). At the bottom, there is a large green button that says "题目已答对" (Challenge solved) and a blue button that says "分享wp点赞赚金币哦" (Share wp to earn gold coins) with a sub-button "马上去写" (Go write now). The footer of the page says "CSDN @今天不学习, 明天变腊鸡".

由题目信息我们可以知道, 这次题目和Cookie有关

2. 进入题目进行分析:

你知道什么是cookie吗?

CSDN @今天不学习, 明天变腊鸡

题目问我们知道什么是Cookie, Cookie: (比如说你进入一个网站, 输入你的密码和用户名, 客户端就会把你的信息传递给服务器, 传递信息(用户名, 密码)的载体就是Cookie, request就是一串数据, 其中就会包括Cookie等信息, 服务器接收request信息后, 就会给客户端发送response应答(密码正确还是错误))

Request 和 Response 对象起到了服务器与客户机之间的信息传递作用。

Request 对象用于接收客户端浏览器提交的数据，

Response 对象的功能则是将服务器端的数据发送到客户端浏览器。

比如说你进入一个网站，输入你的密码和用户名，客户端就会把你的信息传递给服务器，传递信息（用户名，密码）的载体就是Cookie，response:

（一般有服务器名称）

Connection: Keep-Alive

Content-Encoding: gzip

Content-Length: 253

Content-Type: text/html

Date: Thu, 07 Apr 2022 03:06:36 GMT

flag: cyberpeace{b96c80999a82b4f8eb5b2241cabde6b8}

Keep-Alive: timeout=5, max=99

Server: Apache/2.4.7 (Ubuntu)

Vary: Accept-Encoding

X-Powered-By: PHP/5.5.9-1ubuntu4.26

request:

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/s

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

Cache-Control: max-age=0

Connection: keep-alive

Cookie: look-here=cookie.php

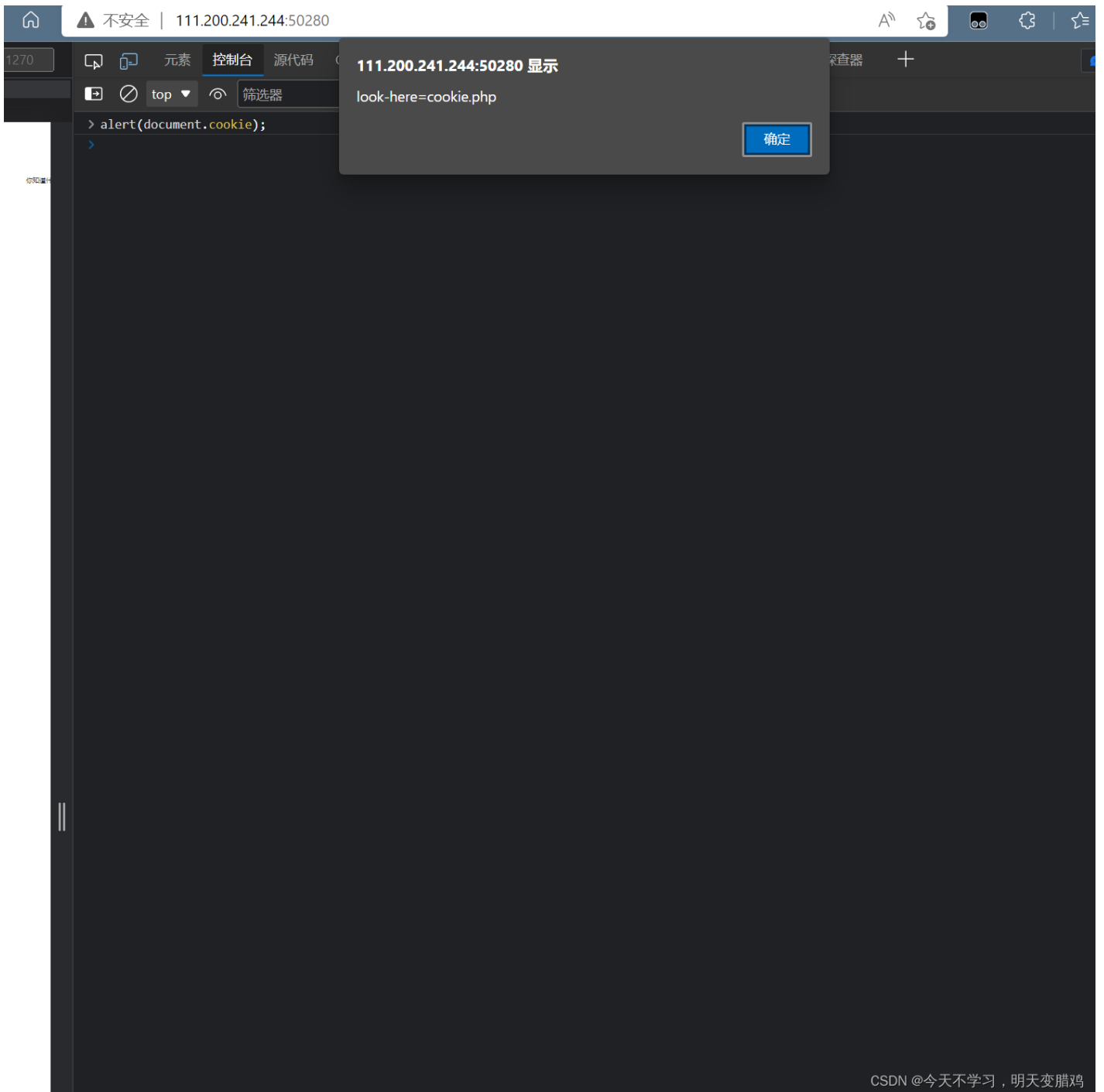
Host: 111.200.241.244:50280

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) C

然后我们查看Cookie:

按f12,再按照如下图所示: (在控制台输入alert(document.cookie))



cookie放在cookie.php文件中：（进入文件：网址加\cookie）

See the http response

题目要我们看http response:

按如下图所示进行操作:

不安全 | 111.200.241.244:50280/cookie.php

网络 × 应用程序 安全性 Lighthouse JavaScript 探查器

名称 × 标头 预览 响应 发起程序 计时 Cookie

- cookie.php
- bootstrap.min.css

常规

请求 URL: http://111.200.241.244:50280/cookie.php
请求方法: GET
状态代码: 200 OK
远程地址: 111.200.241.244:50280
引用站点策略: strict-origin-when-cross-origin

响应头 查看源

Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 253
Content-Type: text/html
Date: Thu, 07 Apr 2022 02:52:27 GMT
flag: cyberpeace{b96c80999a82b4f8eb5b2241cabde6b8}
Keep-Alive: timeout=5, max=100
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
X-Powered-By: PHP/5.5.9-1ubuntu4.26

请求标头 查看源

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cache-Control: max-age=0
Connection: keep-alive
Cookie: look-here=cookie.php
Host: 111.200.241.244:50280
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.60 Mobile Safari/537.36 Edg/100.0.1185.29

CSDN @今天不学习，明天变腊鸡

最后看到flag



[创作打卡挑战赛](#)
[赢取流量/现金/CSDN周边激励大奖](#)