

攻防世界-web-cookie writeup

原创

码啊码 已于 2022-02-09 10:53:27 修改 15 收藏

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

于 2022-02-08 16:51:14 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/m0_48108919/article/details/122826783

版权



[CTF 专栏收录该内容](#)

29 篇文章 0 订阅

订阅专栏

题目描述: X老师告诉小宁他在cookie里放了东西, 小宁疑惑地想: ‘这是夹心饼干的意思吗?’

访问网站

你知道什么是cookie吗?

F12打开控制台

输入document.cookie获取当前网站的cookie, 提示存在cookie.php文件

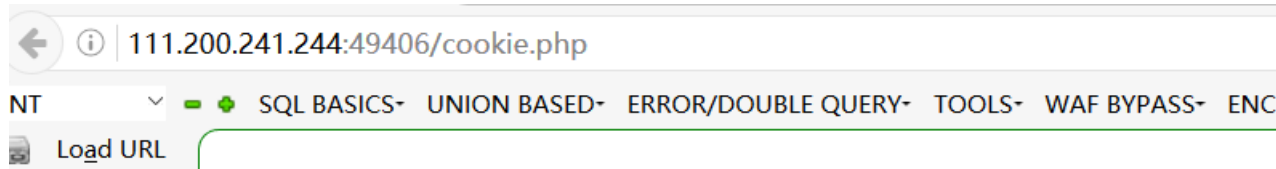
访问/cookie.php,提示查看response



See the http response

CSDN @码啊码

查看请求头得到flag



Split URL
Execute

Post data Referrer 0xHEX %URL BASE64

控制台 HTML CSS 脚本 DOM 网络 Cookies

清除 保持 全部 HTML CSS JavaScript XHR 图片 插件 媒体 字体

URL	状态	域
GET cookie.php	200 OK	111.200.241.244:49406

头信息 响应 HTML 缓存

响应头信息 原始头信息

Connection Keep-Alive
Content-Encoding gzip
Content-Length 253
Content-Type text/html
Date Tue, 08 Feb 2022 08:47:38 GMT
Keep-Alive timeout=5, max=100
Server Apache/2.4.7 (Ubuntu)
Vary Accept-Encoding
X-Powered-By PHP/5.5.9-1ubuntu4.26
flag cyberpeace{337c91c6dad7b0e423fd99edc59a5bd1}

请求头信息 原始头信息

Accept text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding gzip, deflate
Accept-Language zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Cache-Control max-age=0
Connection keep-alive
DNT 1
Host 111.200.241.244:49406
User-Agent Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/30.0 @码阿码

cyberpeace{337c91c6dad7b0e423fd99edc59a5bd1}