hackerone CTF练习

m0_55910567　于 2021-11-26 18:11:28 发布　136　收藏

分类专栏：笔记

　笔记 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

第一章

从零开始的小白打算找点题目练练手…

第一章是最简单的trivial模式，只有一个flag

Welcome to level 0. Enjoy your stay.

点进去什么都没有…

遇事不决f12

Elements	Console	Sources	Network	Performance	Memory	Application	Security	Lighthouse

```
<!DOCTYPE html>
<html>
▼<head>
    <style>
            body {
                background-image: url("background.png");
            }
        </style>
    </head>
···▼<body> == $0
    <p>Welcome to level 0.  Enjoy your stay.</p>
```

```
        </body>
    </html>
```

啊也没有…

上网查阅了一下别人的CTF练习记录，偶然看到有人用抓包找到CTF，我也测试一下，打开burp，配置好代理，抓

# ^	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
1	http://35.227.24.107	GET	/257dd4a2a7/			200	361	HTML					35.227.24.107
2	http://35.227.24.107	GET	/257dd4a2a7/background.png			200	242	text	png				35.227.24.107
3	http://35.227.24.107	GET	/257dd4a2a7/			200	361	HTML					35.227.24.107
4	http://35.227.24.107	GET	/257dd4a2a7/background.png			200	242	text	png				35.227.24.107

Request

Pretty Raw Hex

```
1  GET /257dd4a2a7/background.png HTTP/1.1
2  Host: 35.227.24.107
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
   Gecko) Chrome/87.0.4280.141 Safari/537.36
4  Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8
5  Referer: http://35.227.24.107/257dd4a2a7/
6  Accept-Encoding: gzip, deflate
7  Accept-Language: en-US,en;q=0.9
8  Connection: close
9
10
```

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 200 OK
2  Server: nginx/1.14.0 (Ubuntu)
3  Date: Fri, 26 Nov 2021 06:29:30 GMT
4  Content-Type: text/html; charset=utf-8
5  Connection: close
6  Content-Length: 76
7
8  ^FLAG^e                                          bcc604180a19?40c9$FLAG$
```

抓到了…