bugku web 头等舱 writeup

原创

T0mrvvi1b3t 于 2020-12-04 17:08:51 发布 60 收藏

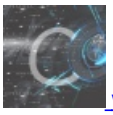
分类专栏： bugku web

本文链接：https://blog.csdn.net/weixin_50597969/article/details/110661662

bugku 同时被 2 个专栏收录

9 篇文章 0 订阅

订阅专栏



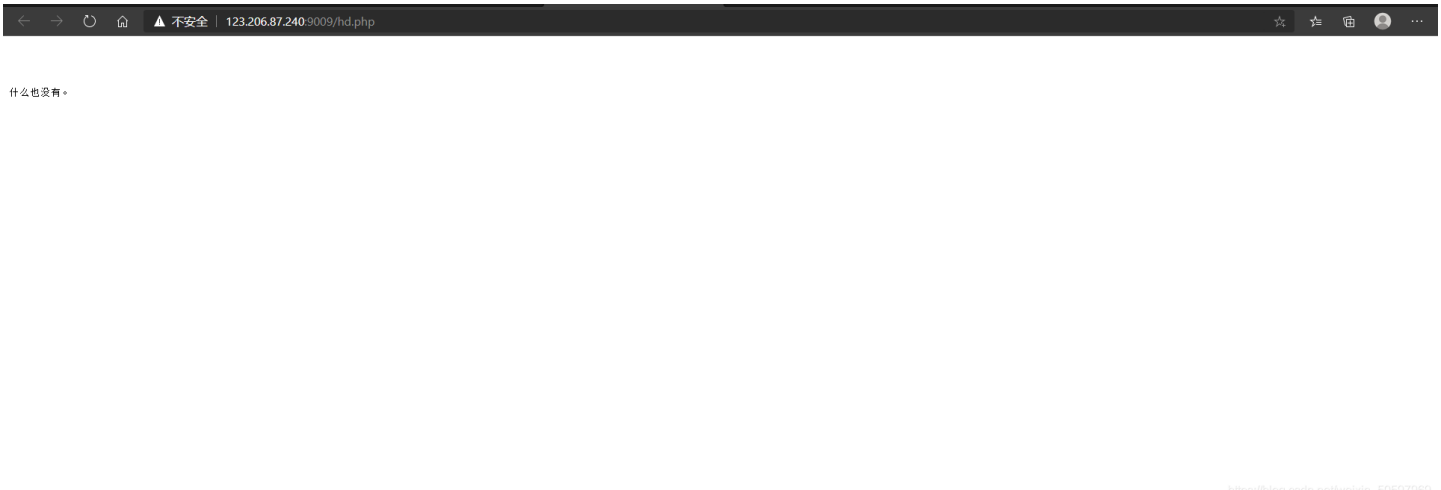
web

19 篇文章 0 订阅

订阅专栏

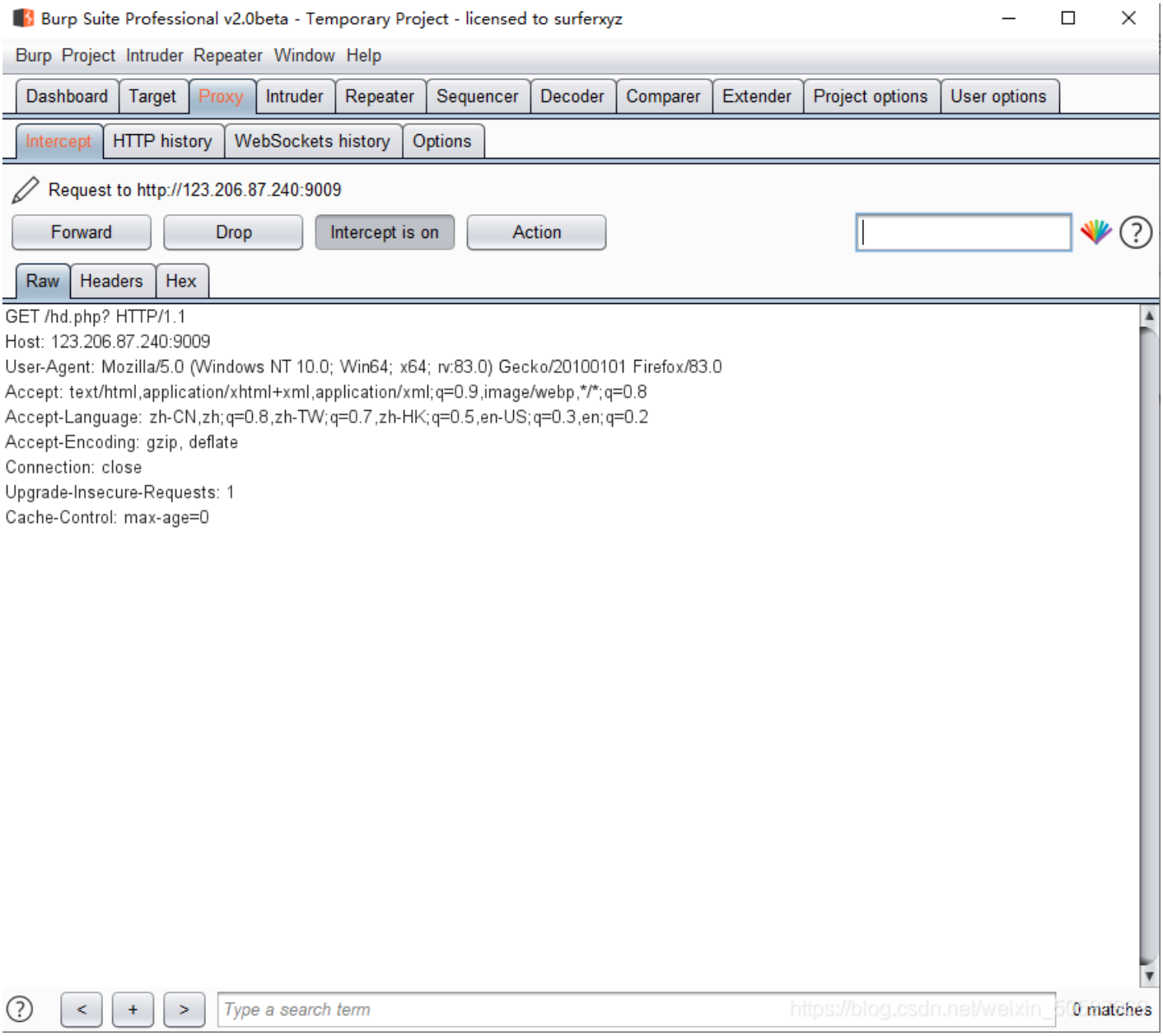
bugku 头等舱

题目信息

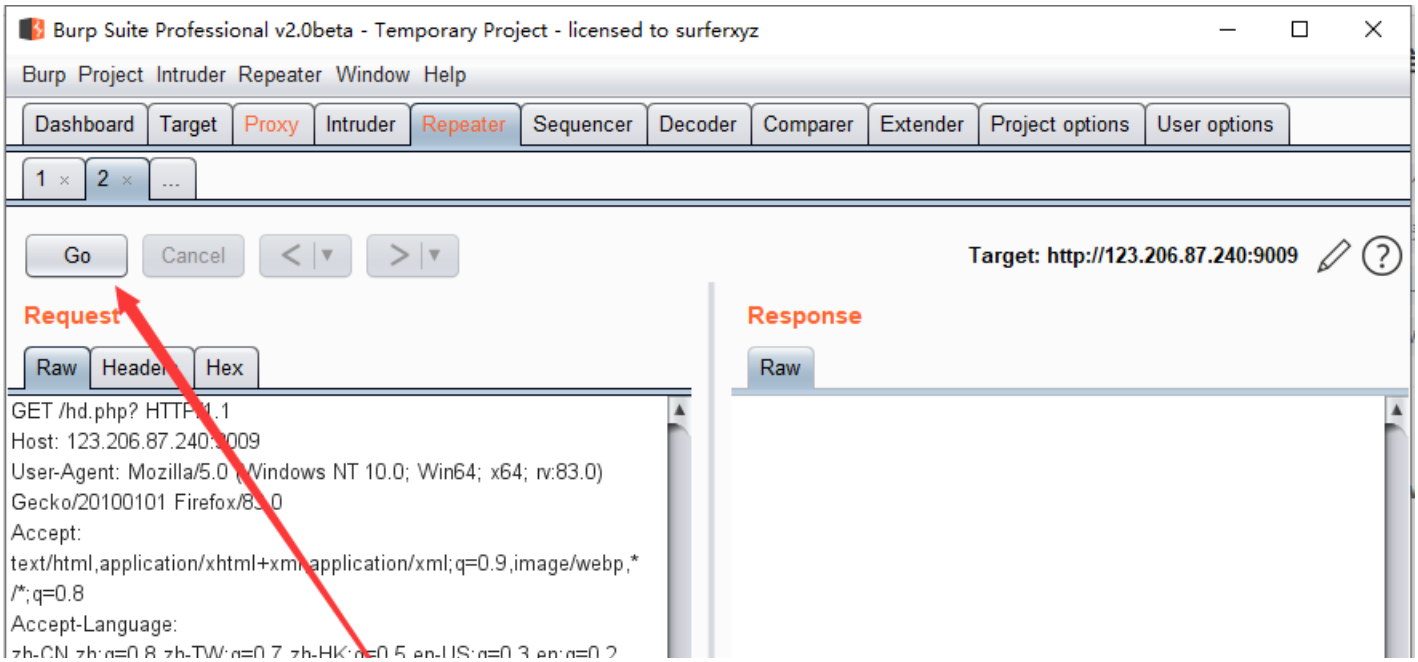


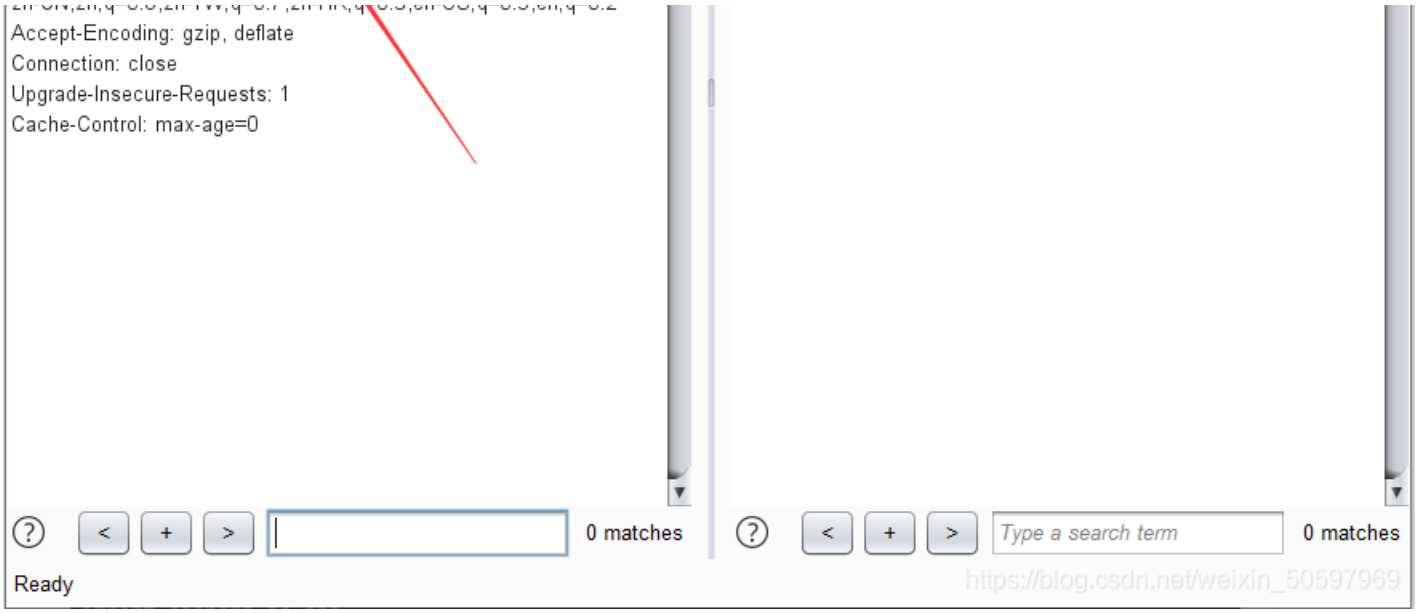
做法：

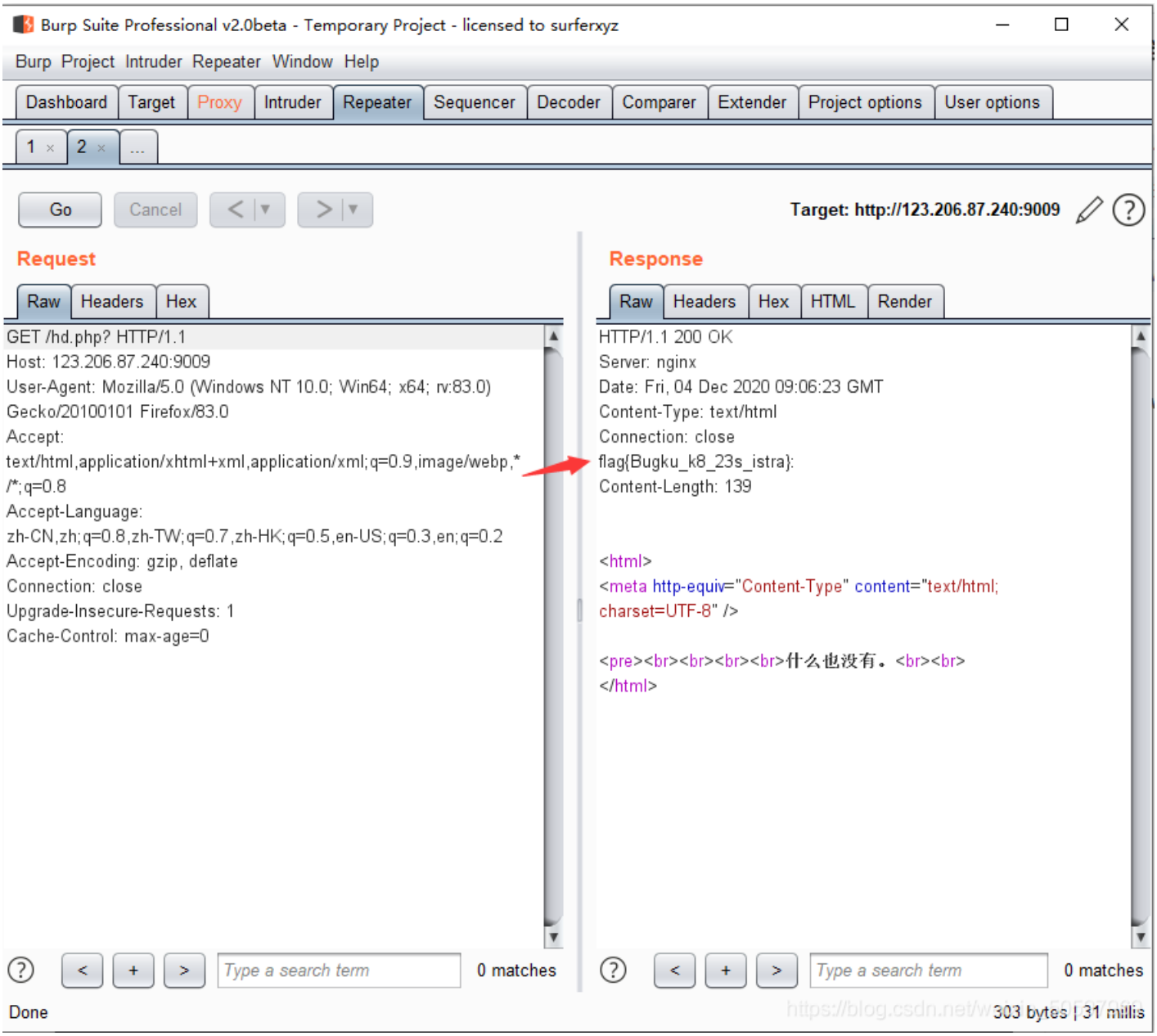
根据题目信息可以得知flag应该和“头”有关
所以考虑用burp suite抓包



ctrl+R 发送到Repeater




Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
0 matches
Type a search term
0 matches
Ready


Burp Suite Professional v2.0beta - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Go
Cancel
Target: http://123.206.87.240:9009
Request
Raw Headers Hex
GET /hd.php? HTTP/1.1
Host: 123.206.87.240:9009
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 04 Dec 2020 09:06:23 GMT
Content-Type: text/html
Connection: close
flag{Bugku_k8_23s_istra}
Content-Length: 139
<html>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<pre>

什么也没有。

</html>
Type a search term
0 matches
Done
303 bytes | 31 millis

这样就发现了flag

FLAG

flag：~~flag{Bugku_k8_23s_istra}~~