攻防世界 WEB 新手练习区 writeup 001-006

原创

ChaoYue_miku 于 2021-09-01 23:40:58 发布 102 收藏

分类专栏： # 攻防世界 CTF # Web 文章标签： html BurpSuite

本文链接：https://blog.csdn.net/ChaoYue_miku/article/details/120051290

版权

攻防世界 同时被 3 个专栏收录

6 篇文章 0 订阅

订阅专栏

CTF

127 篇文章 5 订阅

订阅专栏

Web

4 篇文章 0 订阅

订阅专栏

攻防世界 WEB 新手练习区 题目解答

浏览器：Firefox(火狐浏览器)

文章目录

001 view source

难度系数： 1.0
题目来源： Cyberpeace-n3k0
题目描述： X老师让小宁同学查看一个网页的源代码，但小宁同学发现鼠标右键好像不管用了。

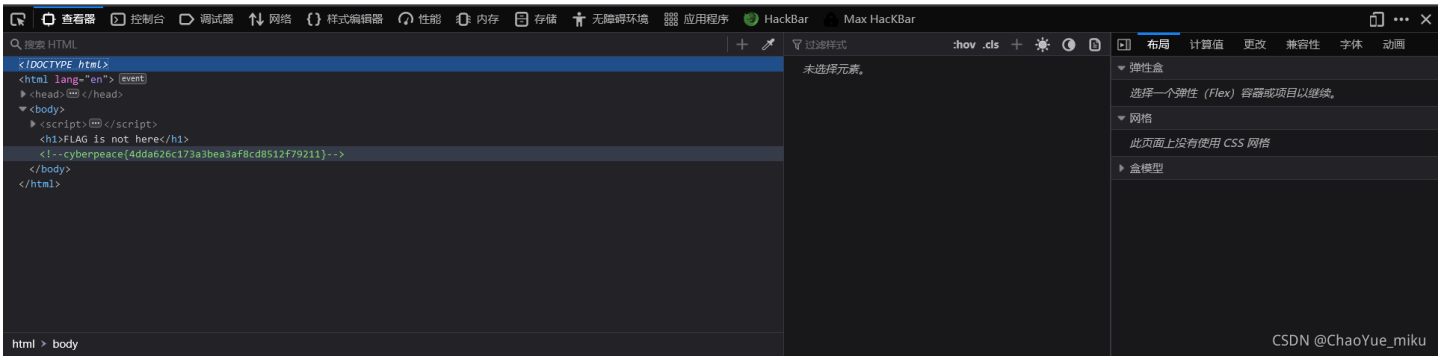
0x01 打开网页

FLAG is not here

网页中显示**FLAG is not here**

0x02 按F12键打开开发者工具

FLAG is not here



或者使用快捷键Ctrl+U打开源代码

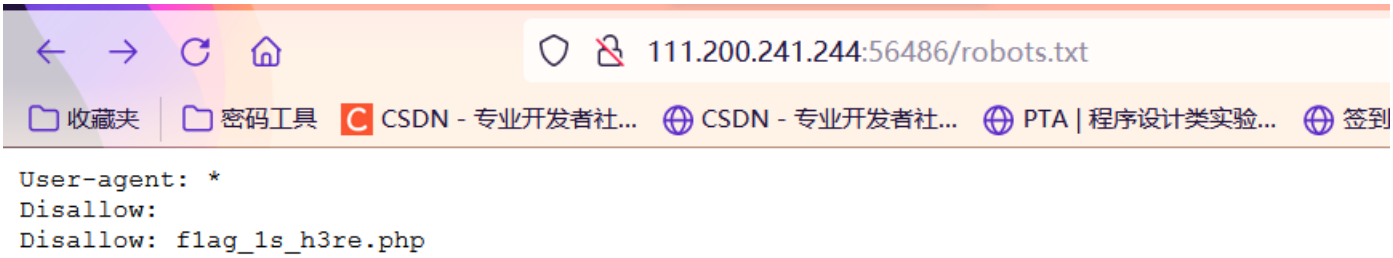
```
1  <!DOCTYPE html>
2  <html lang="en">
3  <head>
4      <meta charset="UTF-8">
5      <title>Where is the FLAG</title>
6  </head>
7  <body>
8  <script>
9  document.oncontextmenu=new Function("return false")
10 document.onselectstart=new Function("return false")
11 </script>
12
13
14 <h1>FLAG is not here</h1>
15
16
17 <!-- cyberpeace{4dda626c173a3bea3af8cd8512f79211} -->
18
19 </body>
20 </html>
```


0x03 得到flag： cyberpeace{4dda626c173a3bea3af8cd8512f79211}

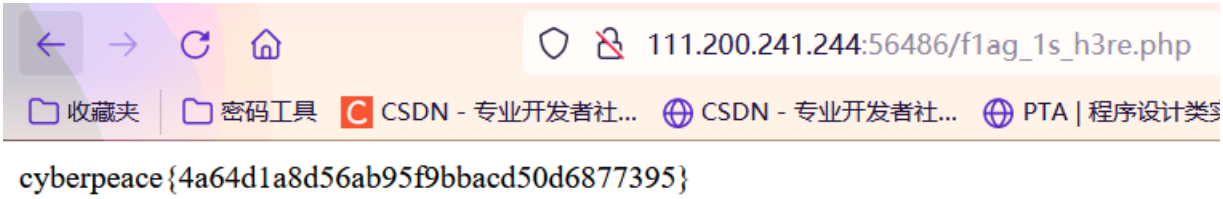
002 robots

难度系数： 1.0
题目来源： Cyberpeace-n3k0
题目描述： X老师上课讲了Robots协议，小宁同学却上课打了瞌睡，赶紧来教教小宁Robots协议是什么吧。

0x01 打开网页，根据题目提示，查看robots.txt文件



0x02 继续打开f1ag_1s_h3re.php文件



0x03 得到flag： cyberpeace{4a64d1a8d56ab95f9bbacd50d6877395}

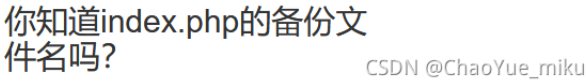
003 backup

难度系数： 1.0

题目来源： Cyberpeace-n3k0

题目描述： X老师忘记删除备份文件，他派小宁同学去把备份文件找出来,一起来帮小宁同学吧！

0x01 打开网页



网页中显示：你知道index.php的备份文件名吗？

通常备份文件的后缀名为.bak

所以index.php的备份文件名为index.php.bak

0x02 打开index.php.bak文件

```
<html>
<head>
    <meta charset="UTF-8">
    <title>备份文件</title>
    <link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" />
    <style>
        body{
            margin-left:auto;
            margin-right:auto;
            margin-TOP:200PX;
            width:20em;
        }
    </style>
</head>
<body>
<h3>你知道index.php的备份文件名吗？</h3>
<?php
$flag="Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}"
?>
</body>
</html>
```

0x03 得到flag： cyberpeace{855A1C4B3401294CB6604CCC98BDE334}

004 cookie

难度系数：1.0

题目来源： Cyberpeace-n3k0

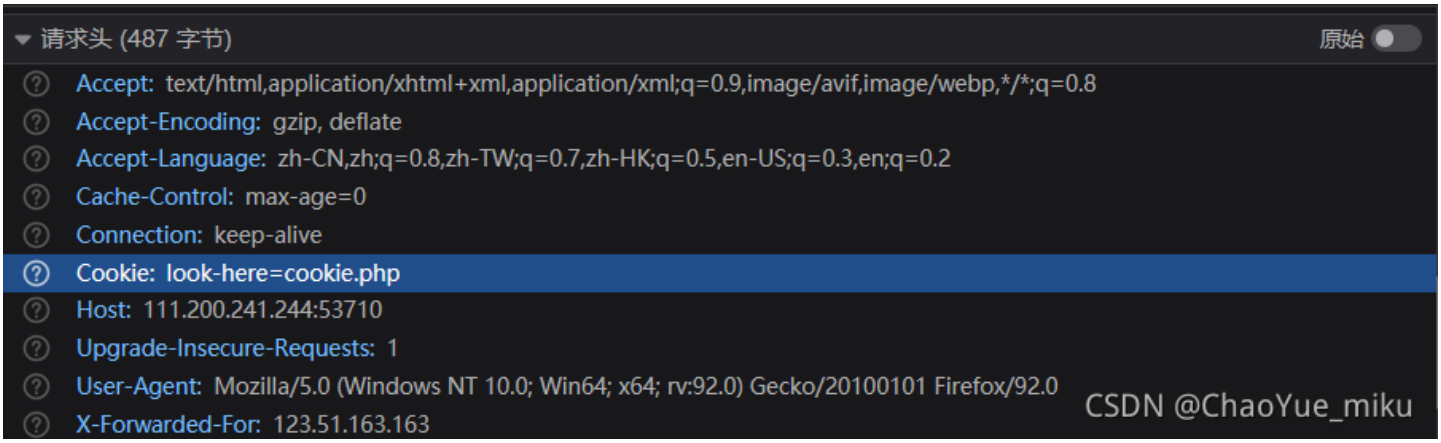
题目描述： X老师告诉小宁他在cookie里放了些东西，小宁疑惑地想：‘这是夹心饼干的意思吗？’

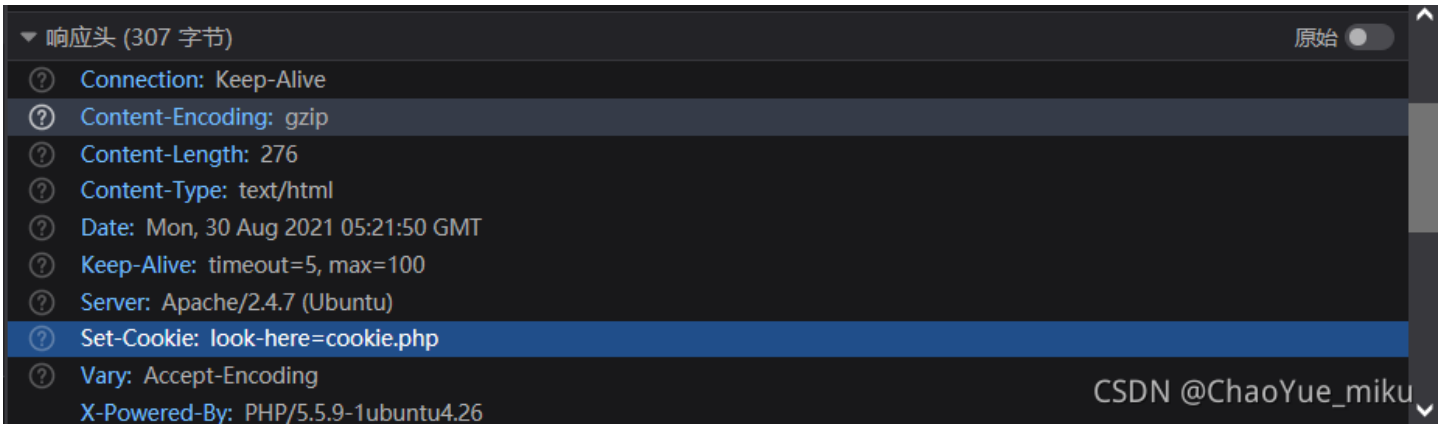
0x01 打开网页

你知道什么是cookie吗?

网页中显示：你知道什么是cookie吗？

0x02 按F12进入开发者工具，在“网络”中查看



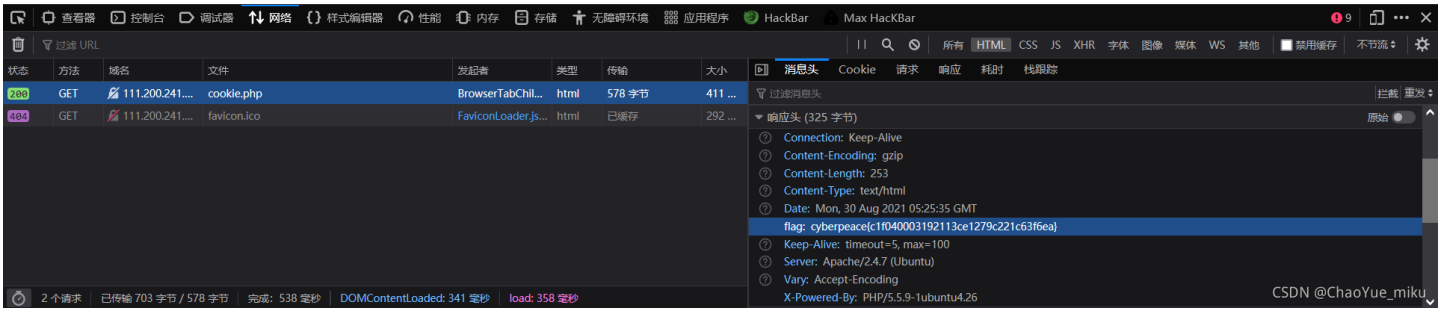


请求头和响应头均有cookie

0x03 打开http://111.200.241.244:53710/cookie.php

网页中显示：See the http response

直接查看响应头，发现flag



0x04 得到flag： cyberpeace{c1f040003192113ce1279c221c63f6ea}

005 disabled_button

难度系数： 1.0
题目来源： Cyberpeace-n3k0
题目描述： X老师今天上课讲了前端知识，然后给了大家一个不能按的按钮，小宁惊奇地发现这个按钮按不下去，到底怎么才能按下去呢？

0x01 打开网页

页面中显示：一个不能按的按钮
下方是一个Button按钮，内容为flag，显示为灰色且不能按下。

在HTML中，button标签可被设置为disabled属性，此时按钮无法被按下
例如：`<button type="button" disabled="disabled">flag</button>`

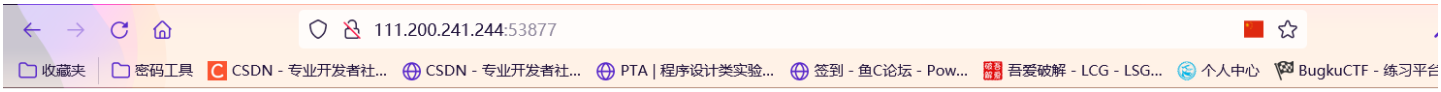
结合题目**disabled_button**，可能是页面的button标签中设置了**disabled**属性

0x02 按F12进入开发者工具，修改页面源代码

```
<html> event
 <script id="allow-copy_script">...</script>
 <head>...</head>
 <body>
   <h3>一个不能按的按钮</h3>
  <form action="" method="post">
    <input class="btn btn-default" disabled="" style="height:50px;width:200px;" type="submit" value="flag" name="auth">
   </form>
  </body>
</html>
```

CSDN @ChaoYue_miku

删除disabled属性后flag按钮就可以按下



一个不能按的按钮

flag

cyberpeace{1137d28f4f0cc032202bcdb6e3c185b8}

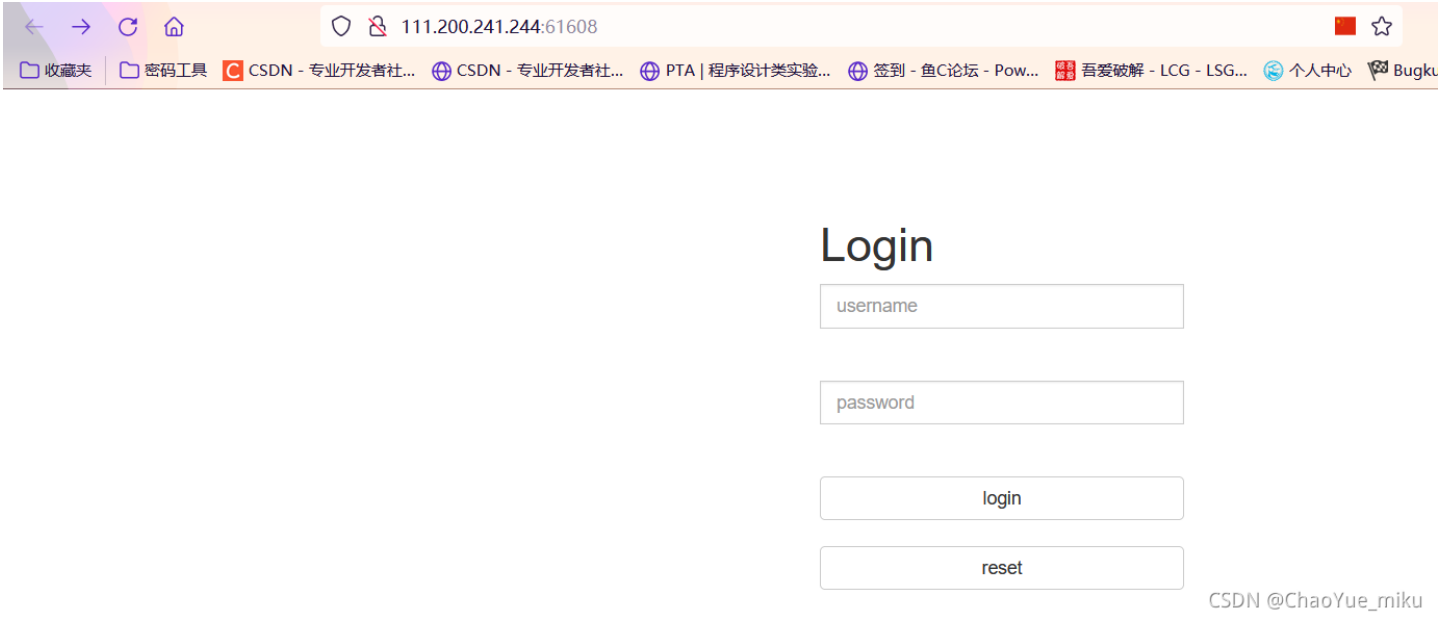
CSDN @ChaoYue_miku

0x03 得到flag： cyberpeace{1137d28f4f0cc032202bcdb6e3c185b8}

006 weak_auth

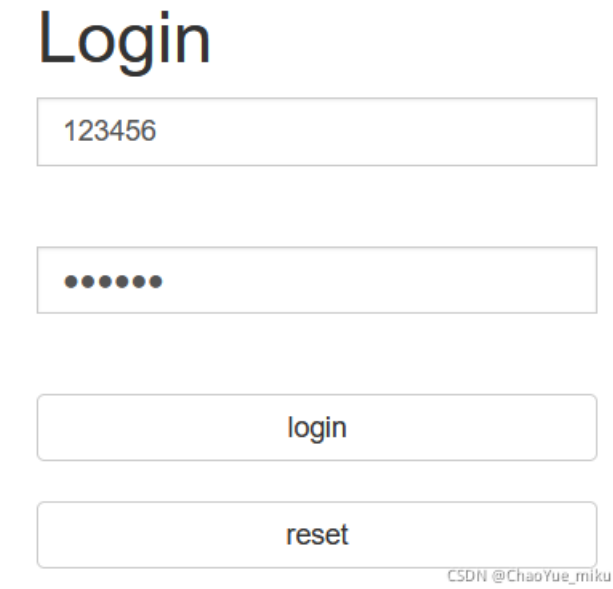
难度系数： 1.0
题目来源： Cyberpeace-n3k0
题目描述： 小宁写了一个登陆验证页面，随手就设了一个密码。

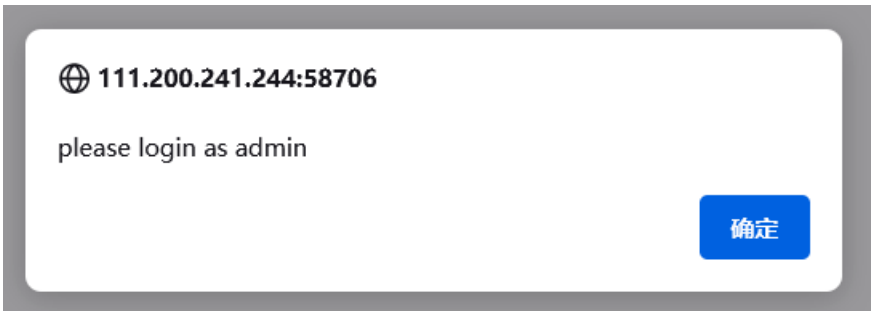
0x01 打开网页，页面中出现一个登录界面



根据题目以及题目描述，估计密码是一个弱口令，可以进行爆破

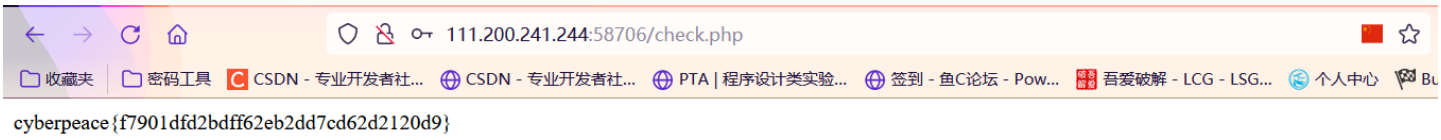
0x02 输入任意用户名和密码，查看回显





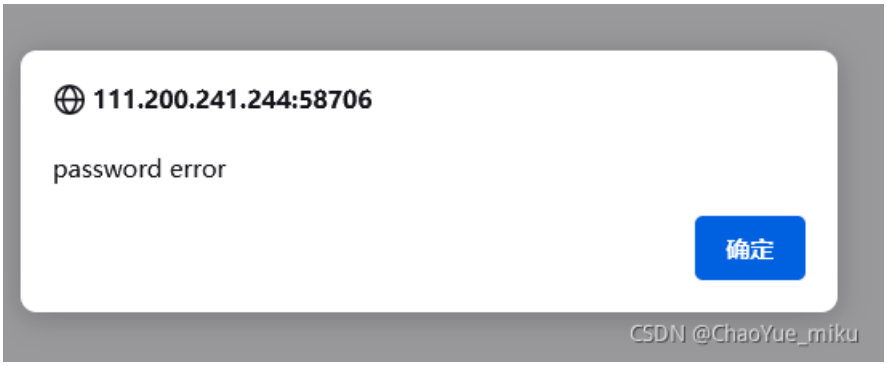
提示我们要用admin账户登录

0x03 用户名输入admin 密码随意输入（这里输入123456）



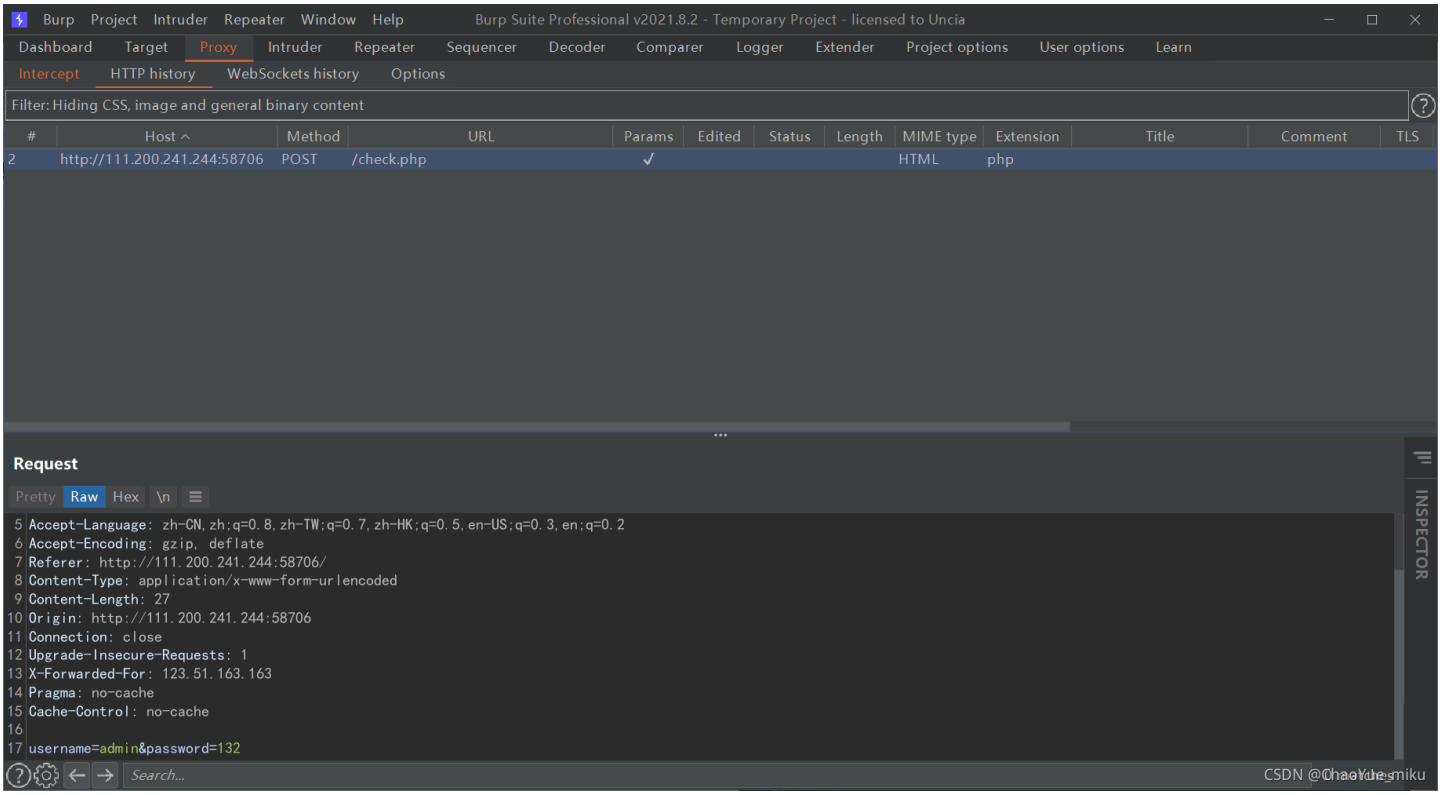
直接登录成功，的确是最为常见的一个弱口令，其实这里也是有些巧合，接下来介绍密码输入错误的情况

0x04 用户名输入admin 密码随意输入（这里输入123）



提示密码错误，说明用户名输入正确

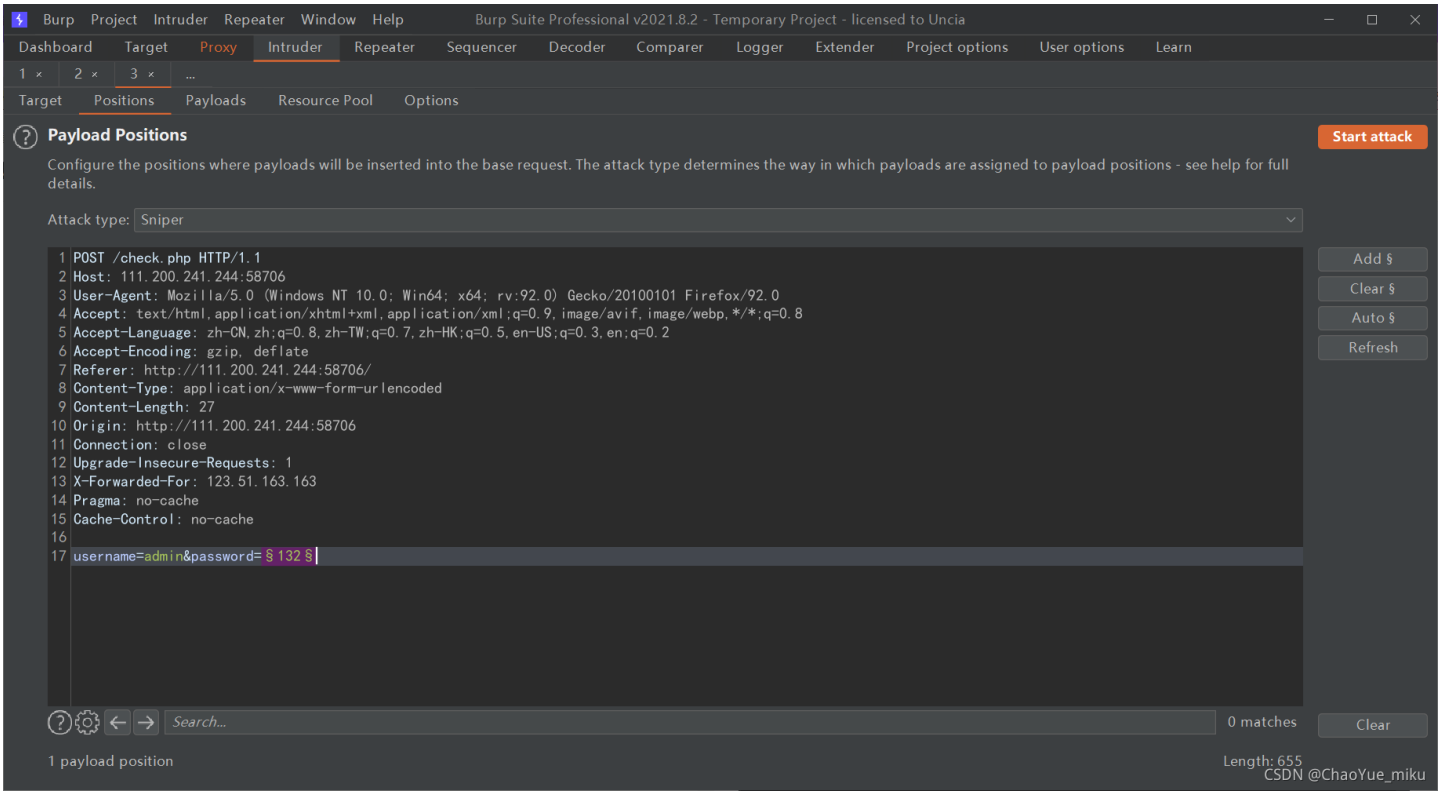
0x05 使用BurpSuite进行抓包，准备爆破

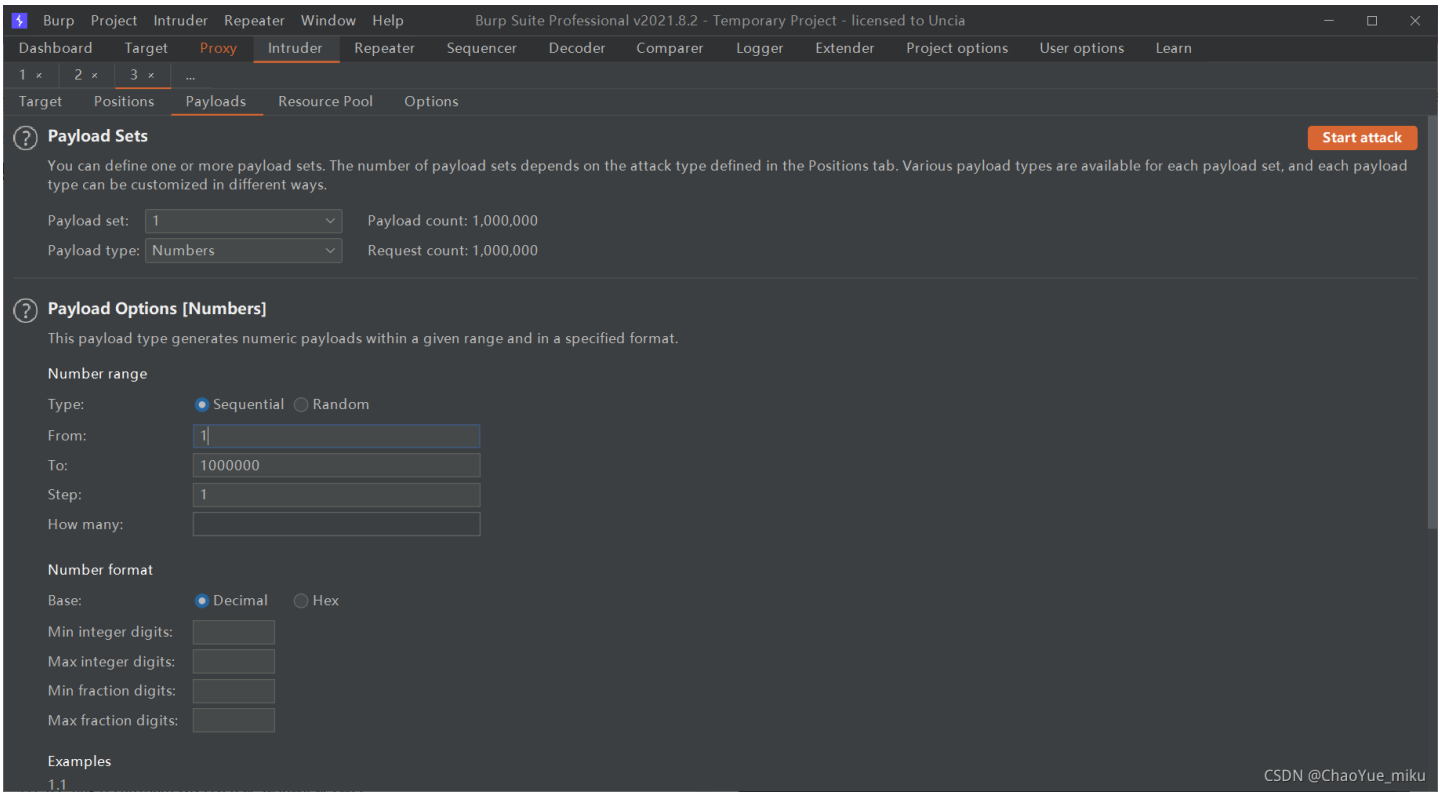


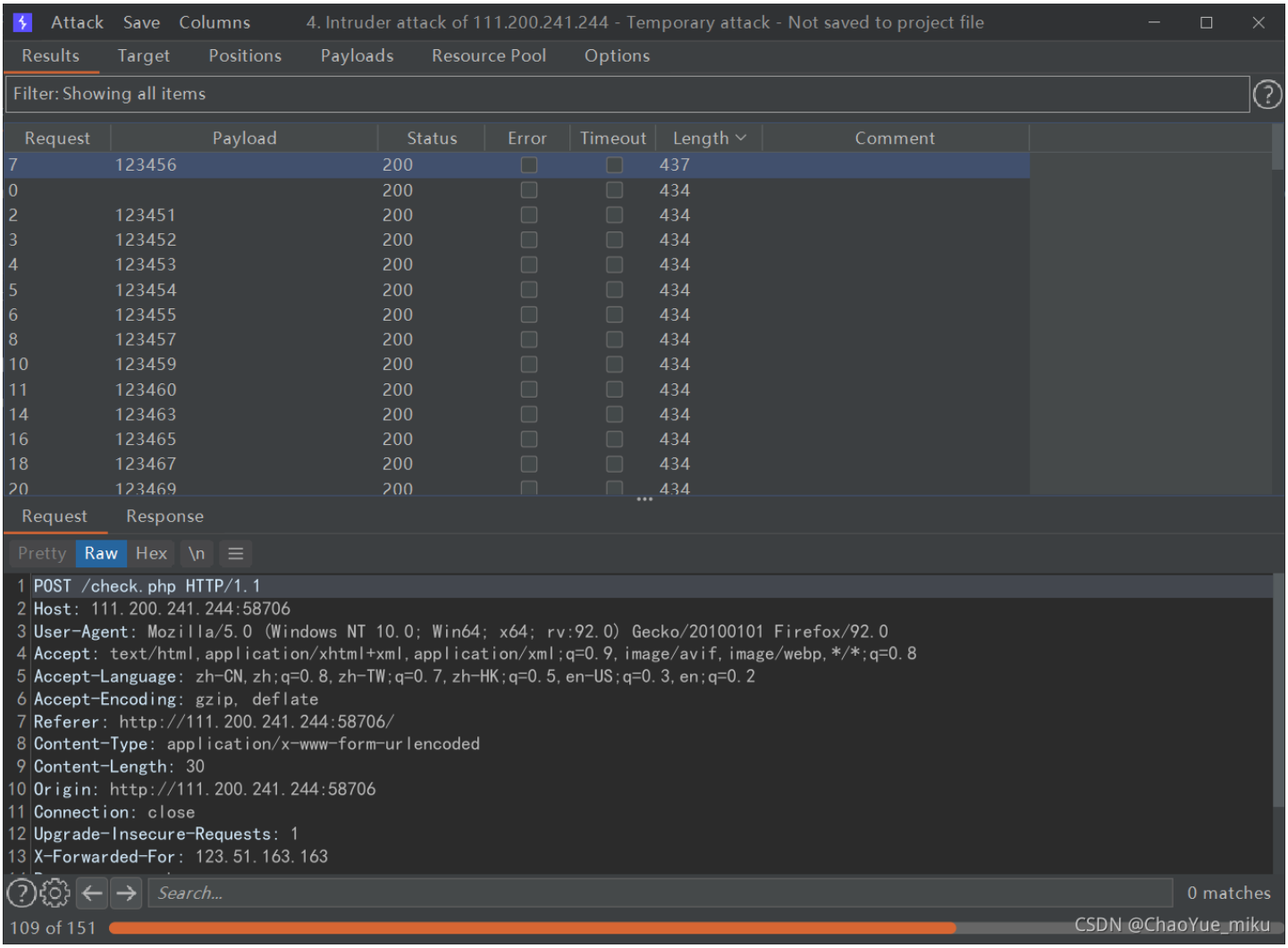
抓包后发送给Intruder模块

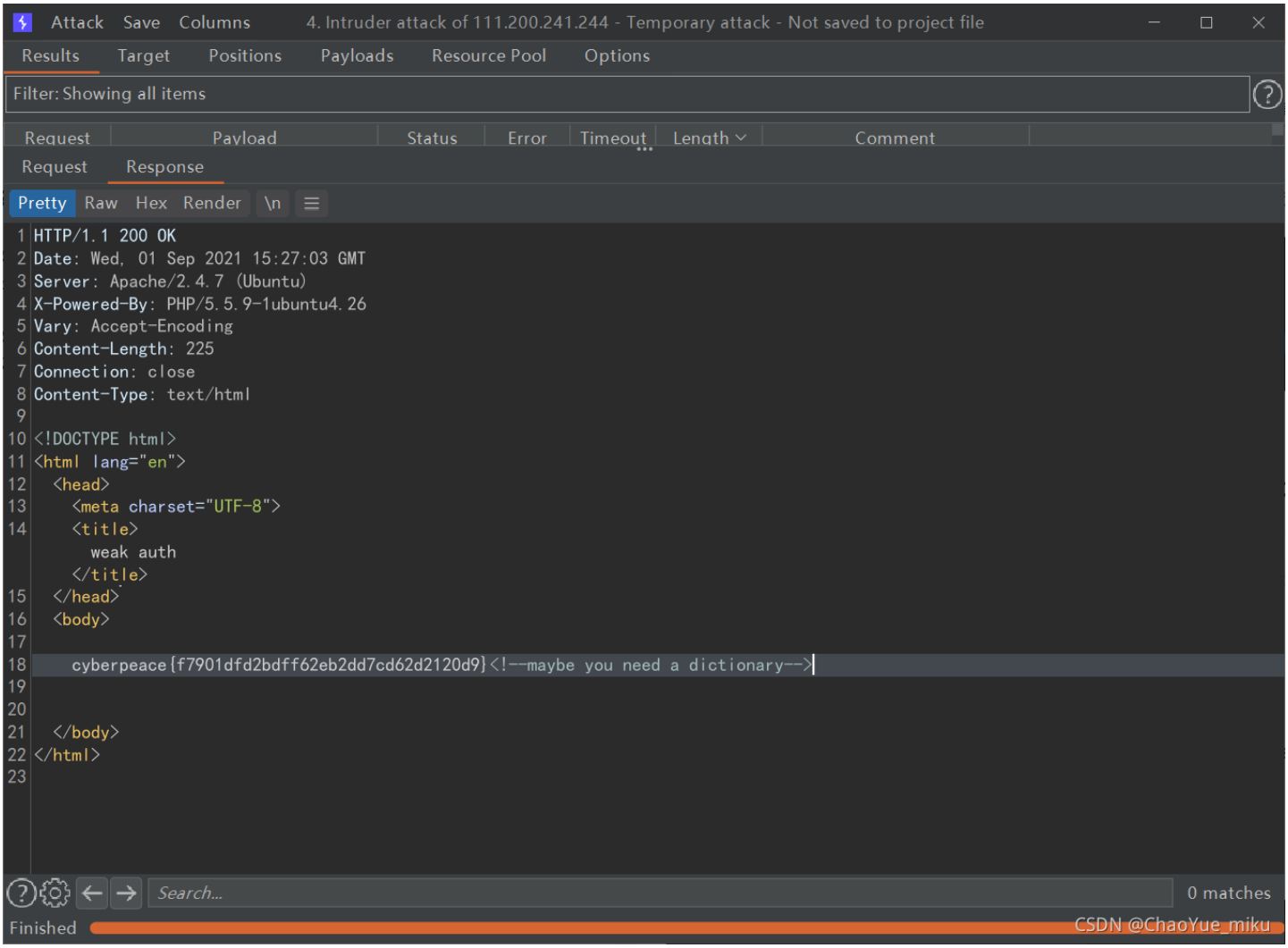
0x06 使用Intruder模块进行爆破

我们可以寻找弱口令字典进行爆破，密码正确时的响应长度与密码错误时不同，以此找出正确的密码


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2021.8.2 - Temporary Project - licensed to Uncia
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × 3 × ...
Target Positions Payloads Resource Pool Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
1 POST /check.php HTTP/1.1
2 Host: 111.200.241.244:58706
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Referer: http://111.200.241.244:58706/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 27
10 Origin: http://111.200.241.244:58706
11 Connection: close
12 Upgrade-Insecure-Requests: 1
13 X-Forwarded-For: 123.51.163.163
14 Pragma: no-cache
15 Cache-Control: no-cache
16
17 username=admin&password=§132§
Add §
Clear §
Auto §
Refresh
Search...
0 matches
Clear
1 payload position
Length: 655
CSDN @ChaoYue_miku


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2021.8.2 - Temporary Project - licensed to Uncia
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × 3 × ...
Target Positions Payloads Resource Pool Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 1,000,000
Payload type: Numbers
Request count: 1,000,000
Payload Options [Numbers]
This payload type generates numeric payloads within a given range and in a specified format.
Number range
Type: Sequential Random
From: 1
To: 1000000
Step: 1
How many:
Number format
Base: Decimal Hex
Min integer digits:
Max integer digits:
Min fraction digits:
Max fraction digits:
Examples
1.1
CSDN @ChaoYue_miku


Attack Save Columns
4. Intruder attack of 111.200.241.244 - Temporary attack - Not saved to project file
Results Target Positions Payloads Resource Pool Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
7 123456 200 437
0 200 434
2 123451 200 434
3 123452 200 434
4 123453 200 434
5 123454 200 434
6 123455 200 434
8 123457 200 434
10 123459 200 434
11 123460 200 434
14 123463 200 434
16 123465 200 434
18 123467 200 434
20 123469 200 434
Request Response
Pretty Raw Hex \n
1 POST /check.php HTTP/1.1
2 Host: 111.200.241.244:58706
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Referer: http://111.200.241.244:58706/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 30
10 Origin: http://111.200.241.244:58706
11 Connection: close
12 Upgrade-Insecure-Requests: 1
13 X-Forwarded-For: 123.51.163.163
Search...
0 matches
109 of 151
CSDN @ChaoYue_miku



0x07 得到flag： **cyberpeace{f7901dfd2bdff62eb2dd7cd62d2120d9}**