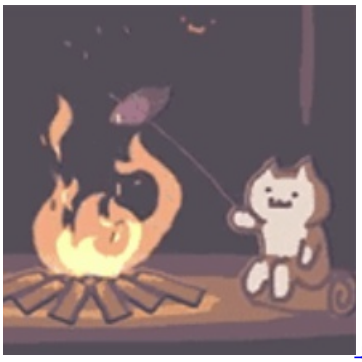
合天网安 在线实验 CTF竞赛 writeup(第一周 | 神奇的磁带、第二周 | 就差一把钥匙、CTF-WEB小技俩、第三周 | 迷了路、第四周 | Check your source code)

原创

shu天 于 2021-12-14 10:00:00 发布 56 收藏 1

分类专栏： ctf 文章标签： ctf web

本文链接：https://blog.csdn.net/weixin_46081055/article/details/121478094



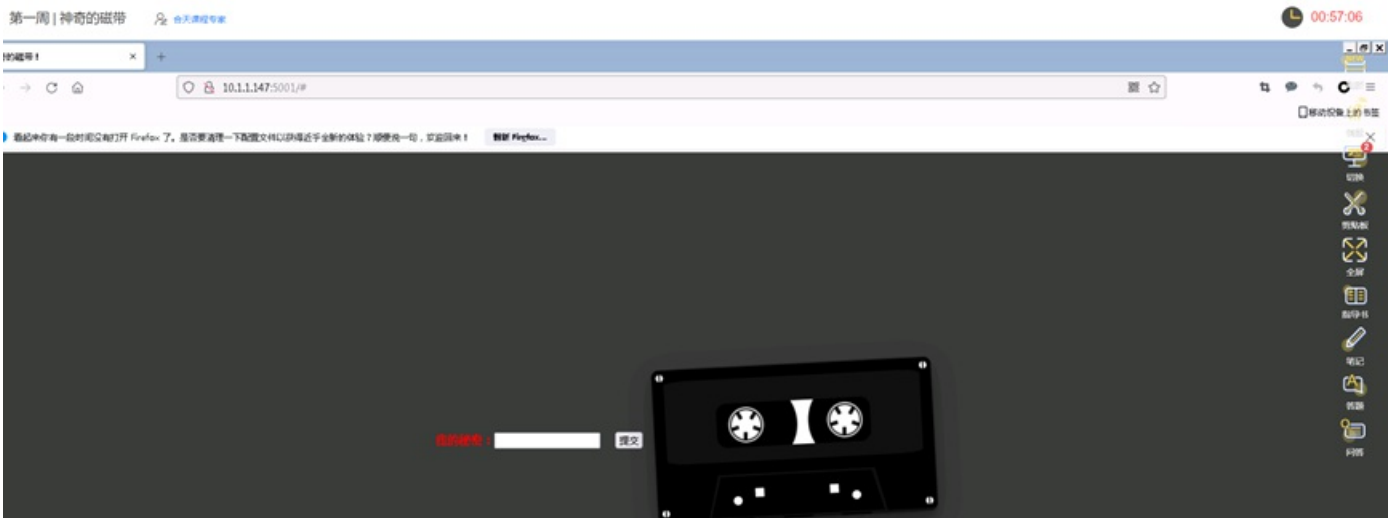
ctf 专栏收录该内容

81 篇文章 4 订阅

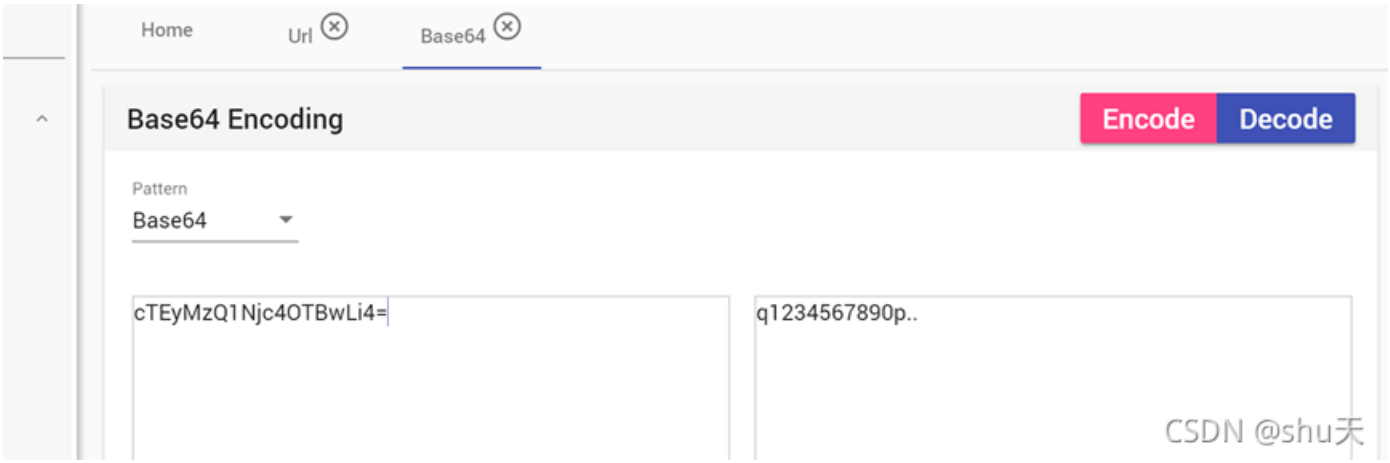
订阅专栏

文章目录

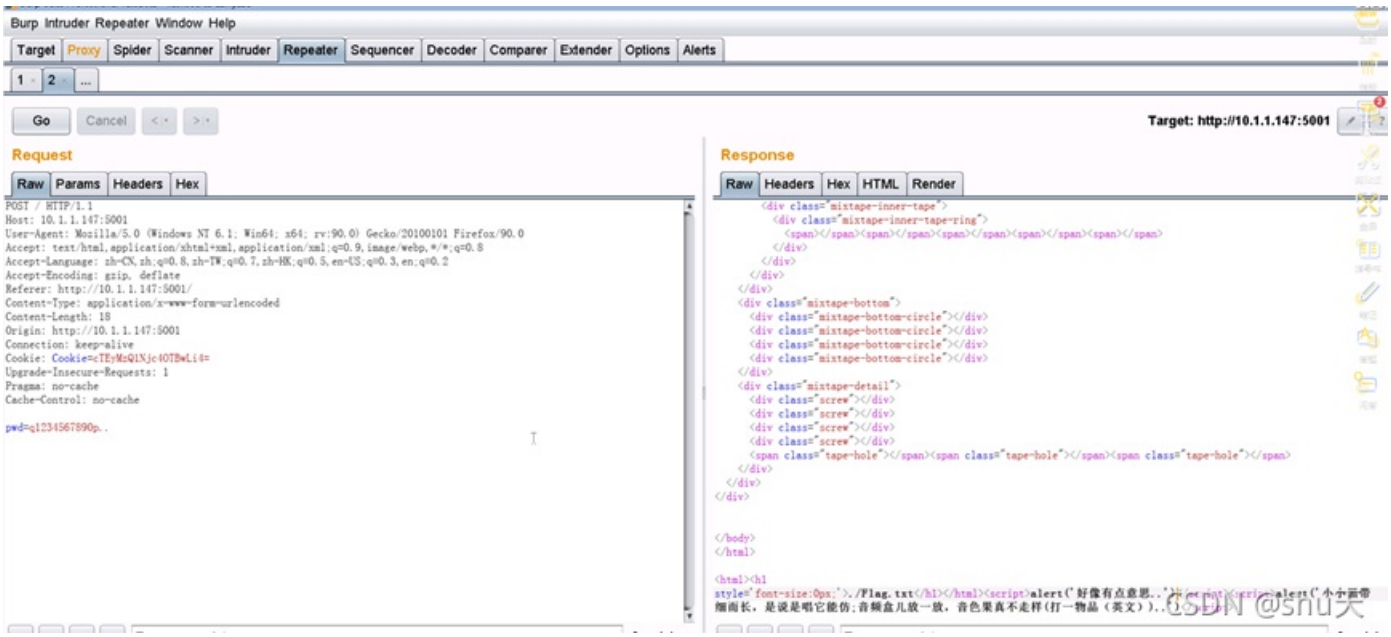
第一周 | 神奇的磁带



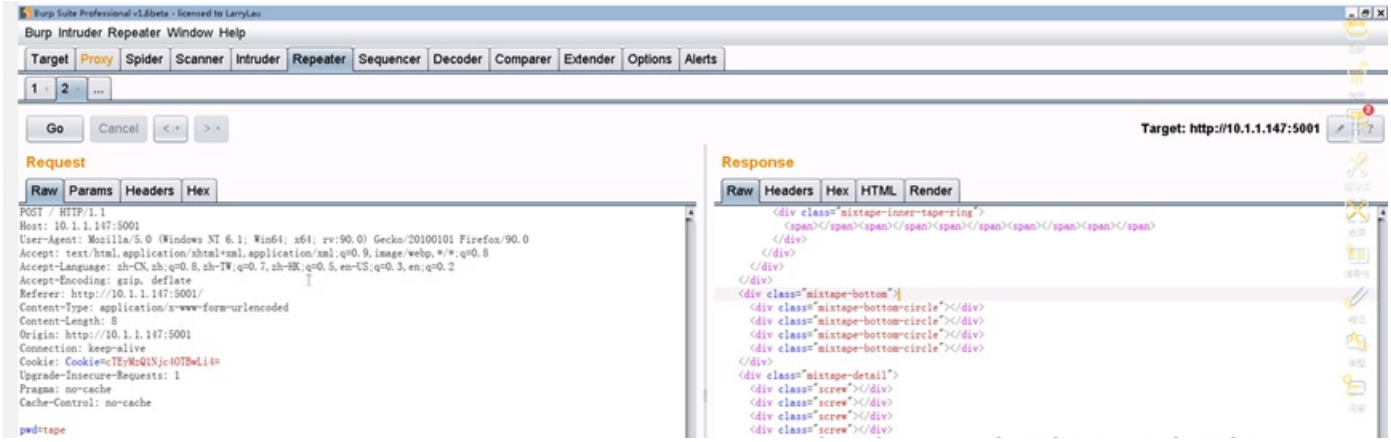
提示在Cookie=cTEyMzQ1Njc4OTBwLi4=



Base64解密后即是密码，登陆得到提示

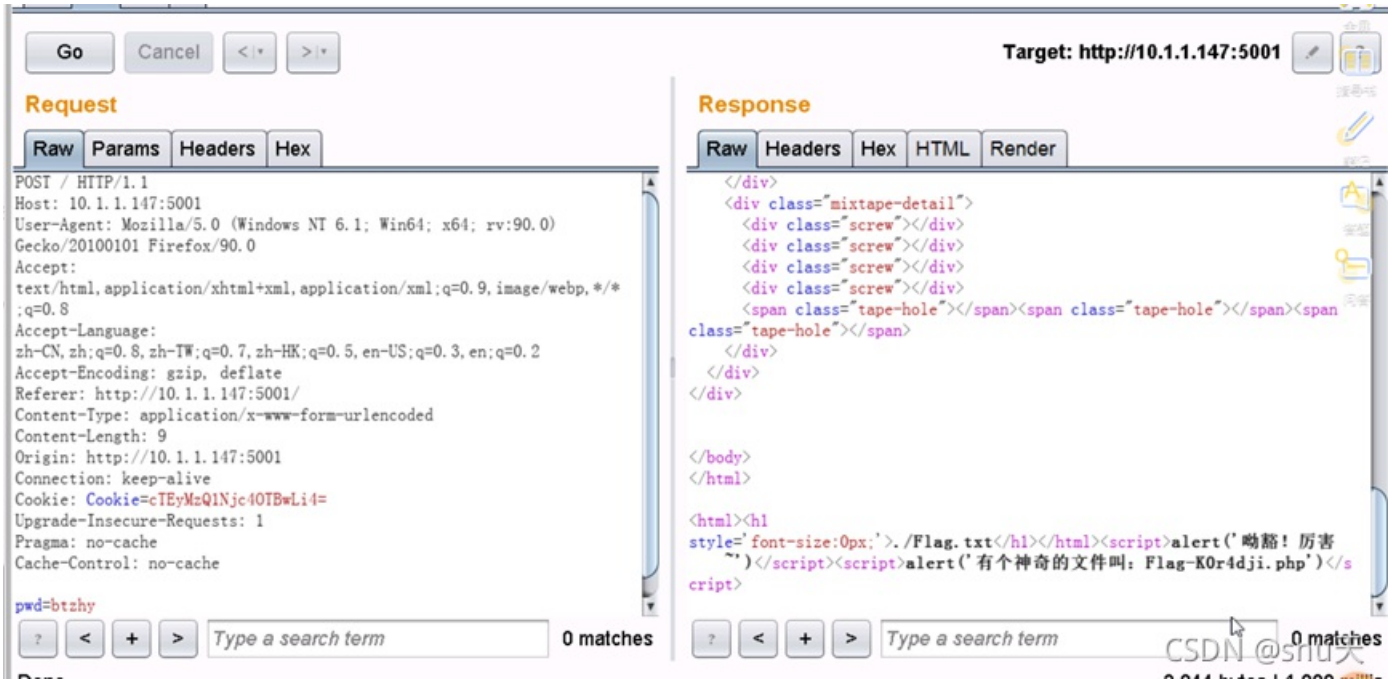


回去输入Tape，得到第二个提示

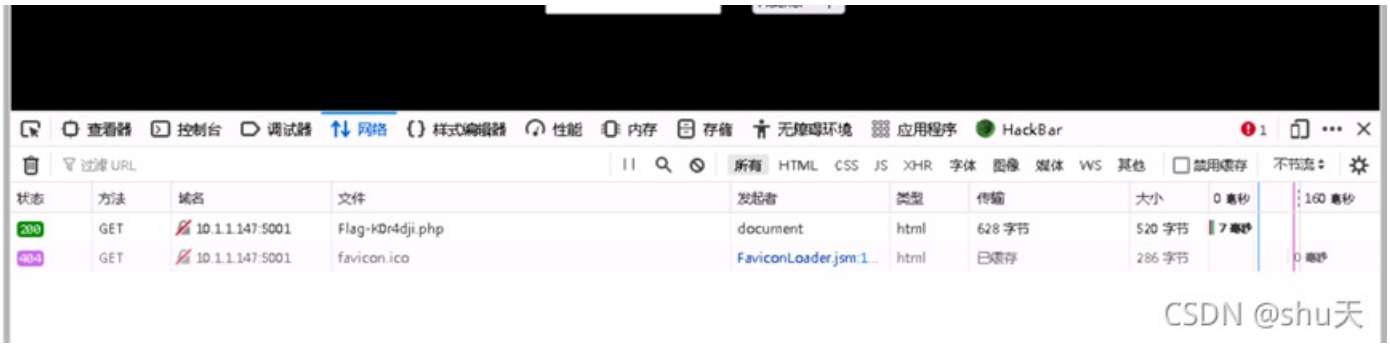


访问http://10.1.1.147:5001/Flag-Win.txt

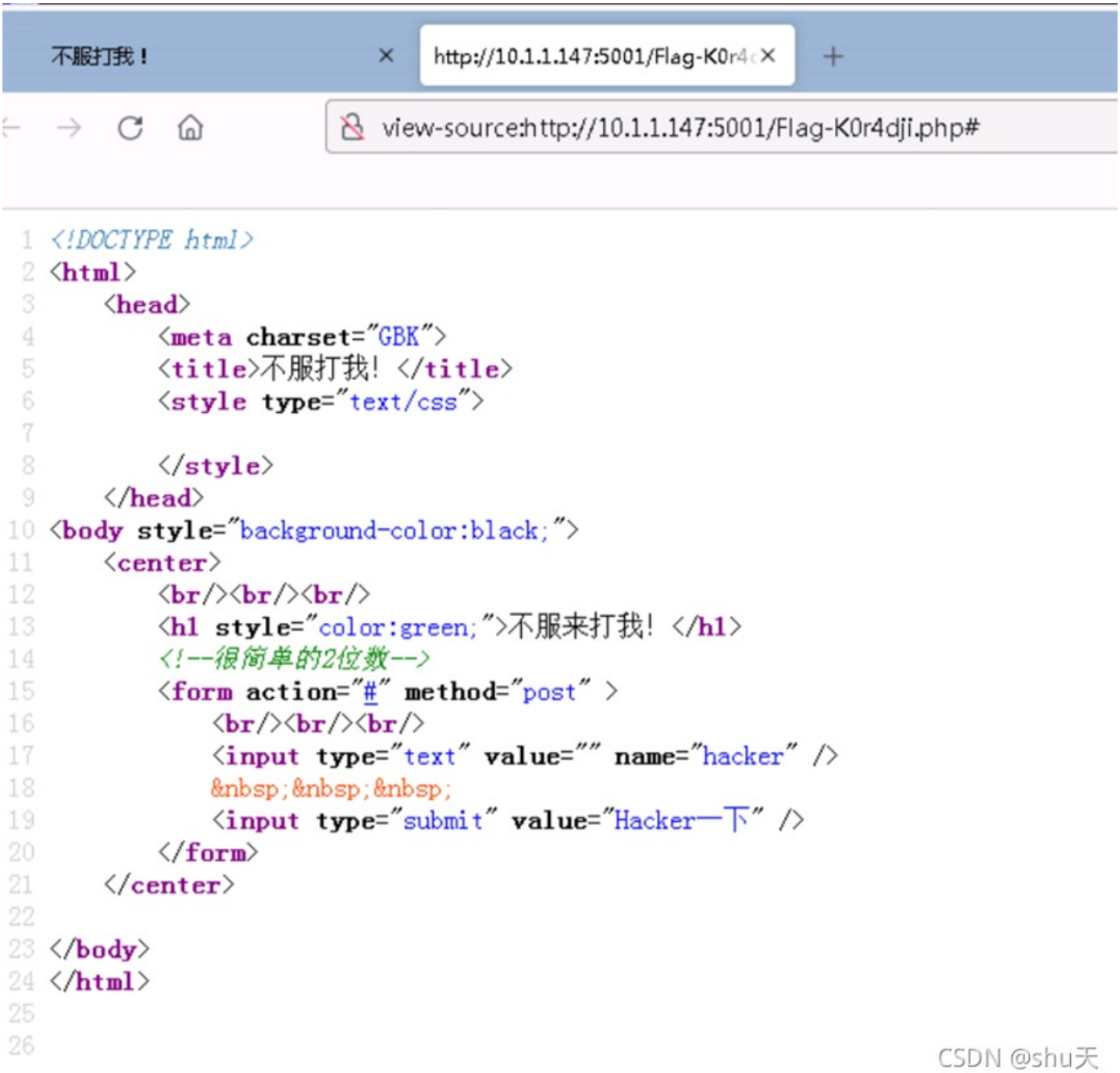
天王盖地虎-宝塔镇河妖-btzhy，重新提交，得到新的提示：



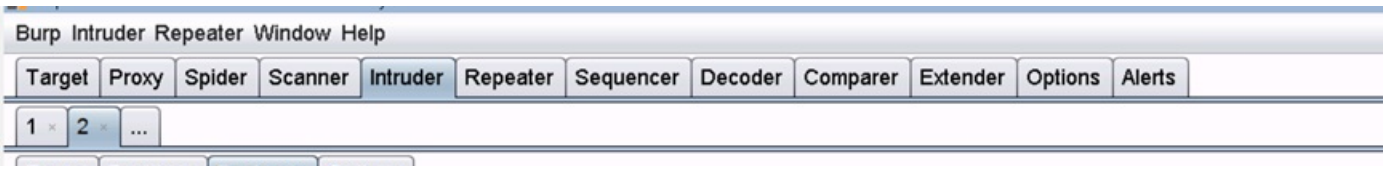
访问Flag-K0r4dji.php

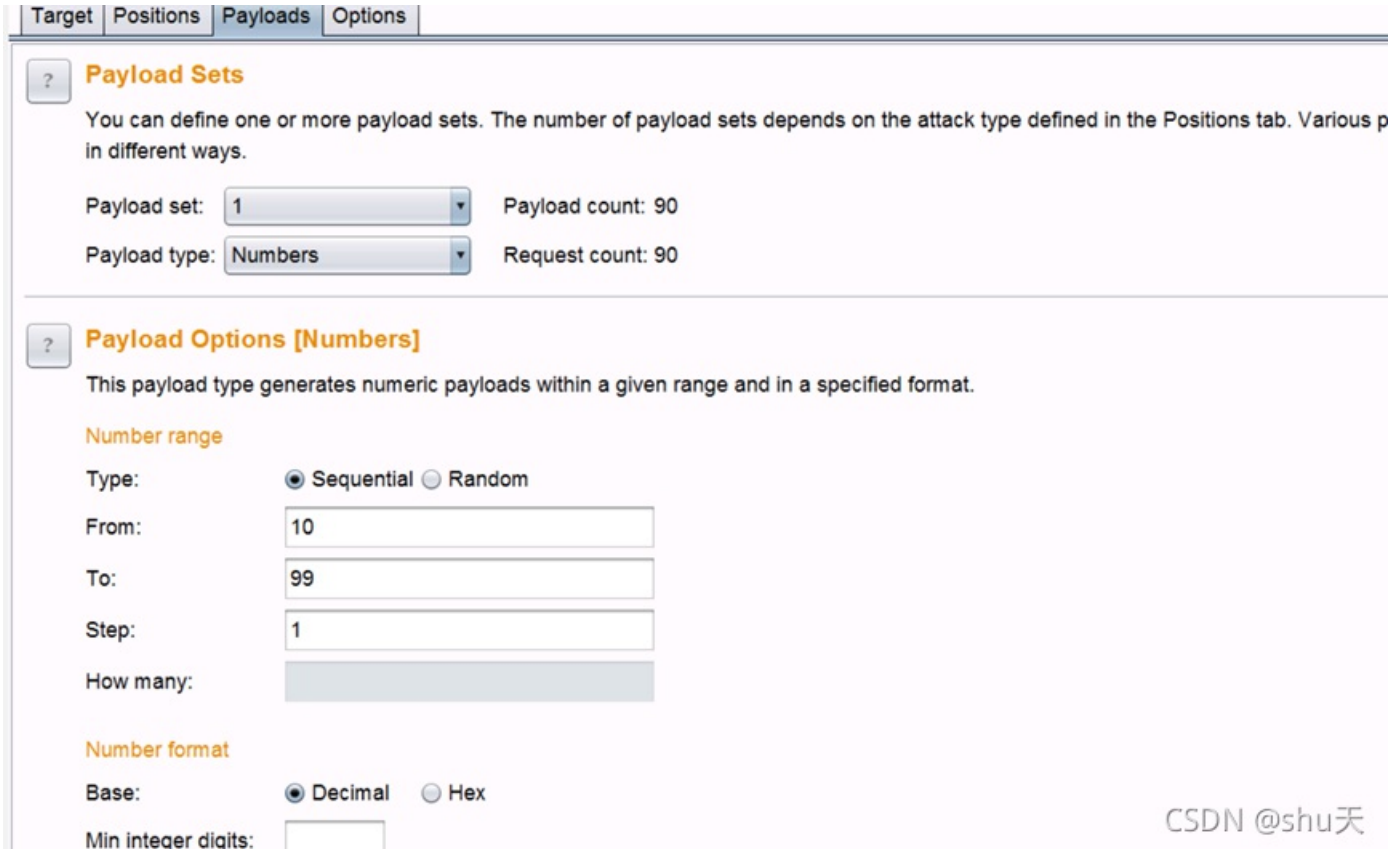


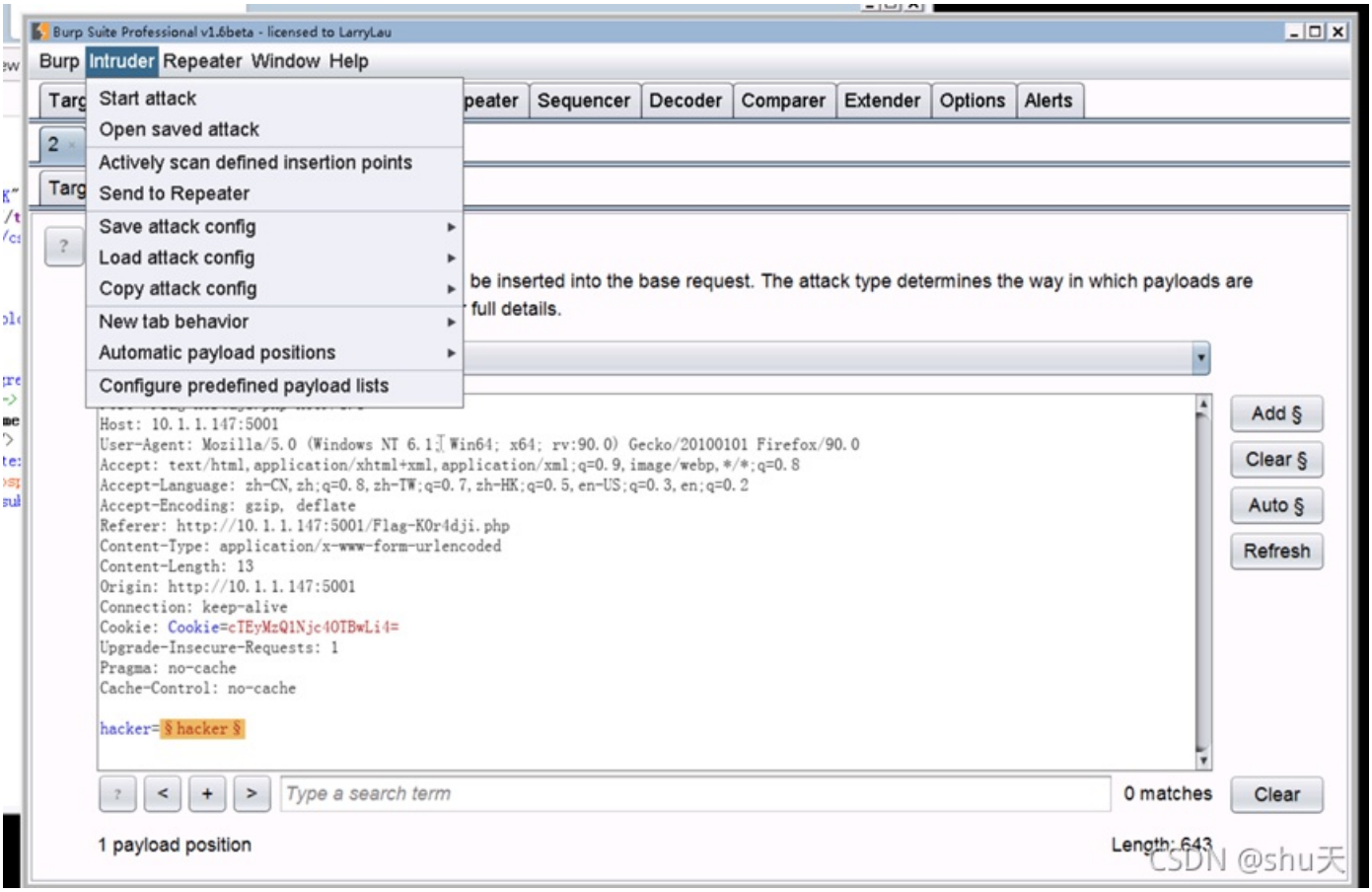
源码中有提示

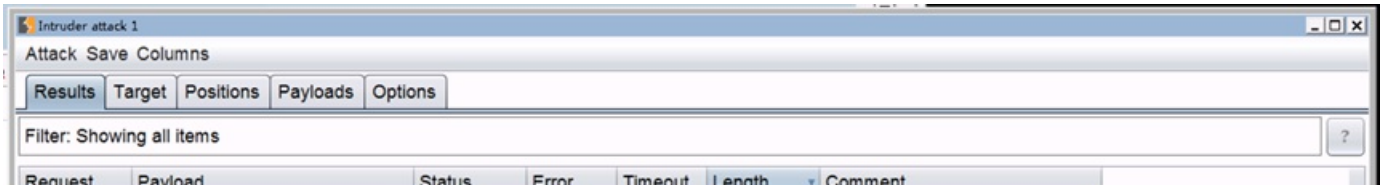


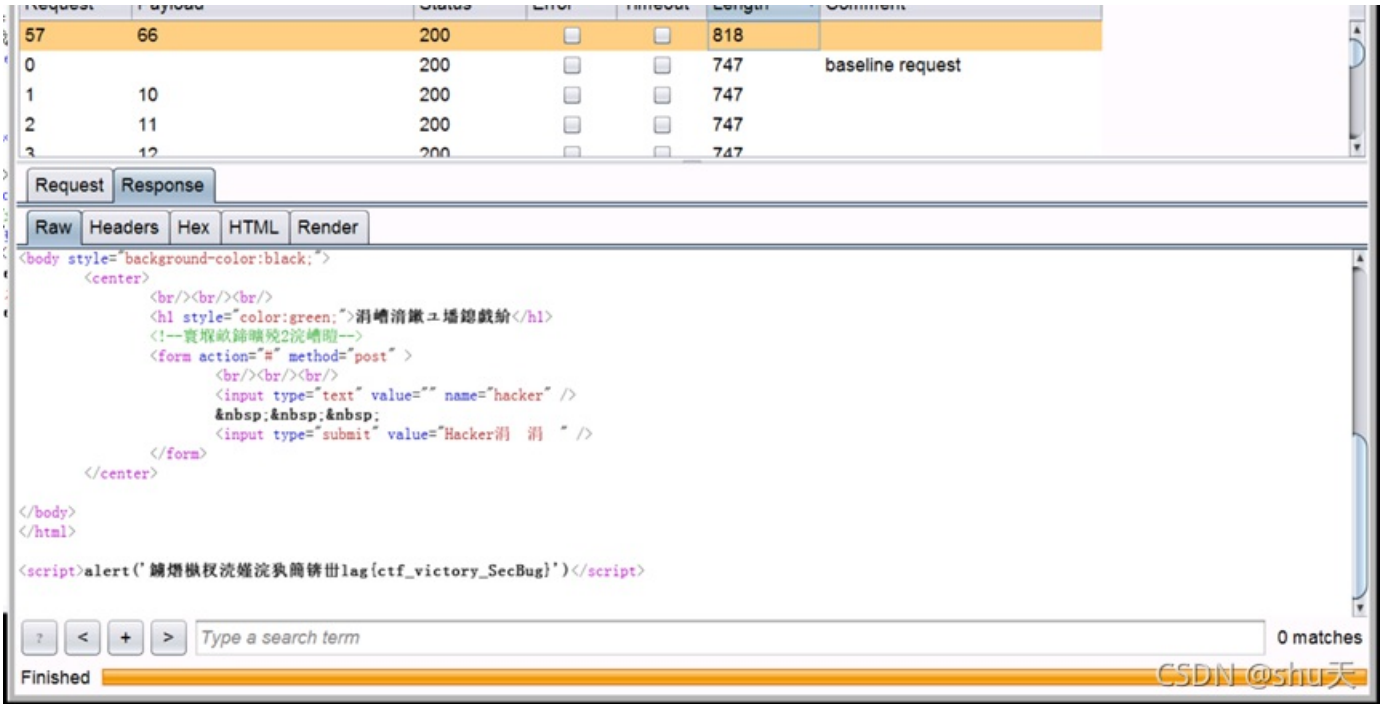
burpsuit两位数爆破



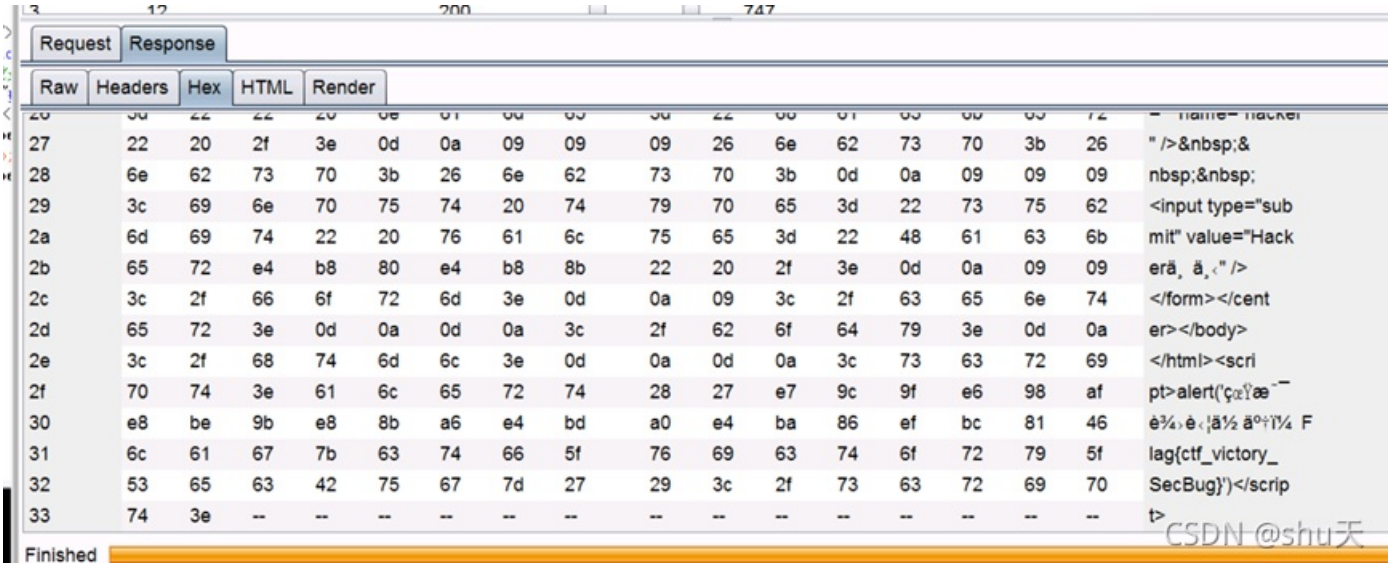

Target
Positions
Payloads
Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various p
in different ways.
Payload set: 1
Payload count: 90
Payload type: Numbers
Request count: 90
Payload Options [Numbers]
This payload type generates numeric payloads within a given range and in a specified format.
Number range
Type: Sequential Random
From: 10
To: 99
Step: 1
How many:
Number format
Base: Decimal Hex
Min integer digits:
CSDN @shu天

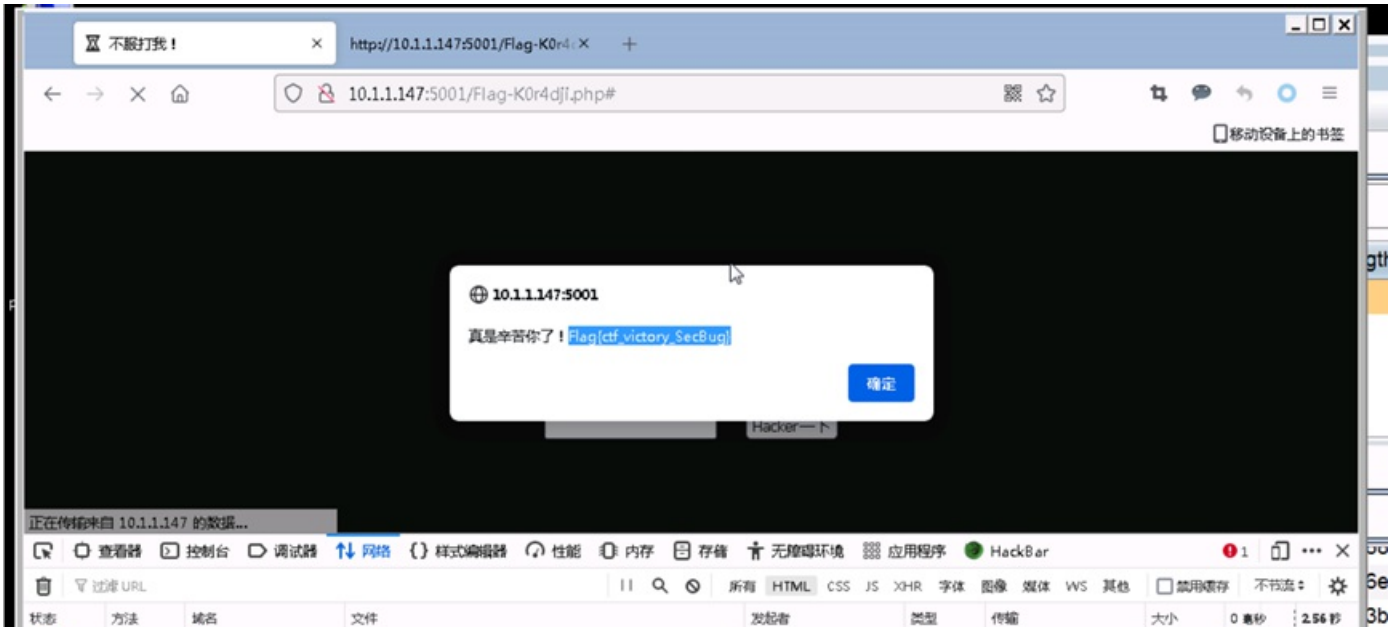

Burp Suite Professional v1.6beta - licensed to LarryLau
Burp Intruder Repeater Window Help
Start attack
Open saved attack
Actively scan defined insertion points
Send to Repeater
Save attack config
Load attack config
Copy attack config
New tab behavior
Automatic payload positions
Configure predefined payload lists
Sequencer Decoder Comparer Extender Options Alerts
be inserted into the base request. The attack type determines the way in which payloads are
full details.
Host: 10.1.1.147:5001
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
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
Referer: http://10.1.1.147:5001/Flag-K0r4dji.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 13
Origin: http://10.1.1.147:5001
Connection: keep-alive
Cookie: Cookie=cTEyMzQ1Njc4OTBwLi4=
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
hacker=§hacker§
Add §
Clear §
Auto §
Refresh
Type a search term
0 matches
Clear
1 payload position
Length: 643
CSDN @shu天


Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment



可以看到密码是66，可能网页编码有点问题



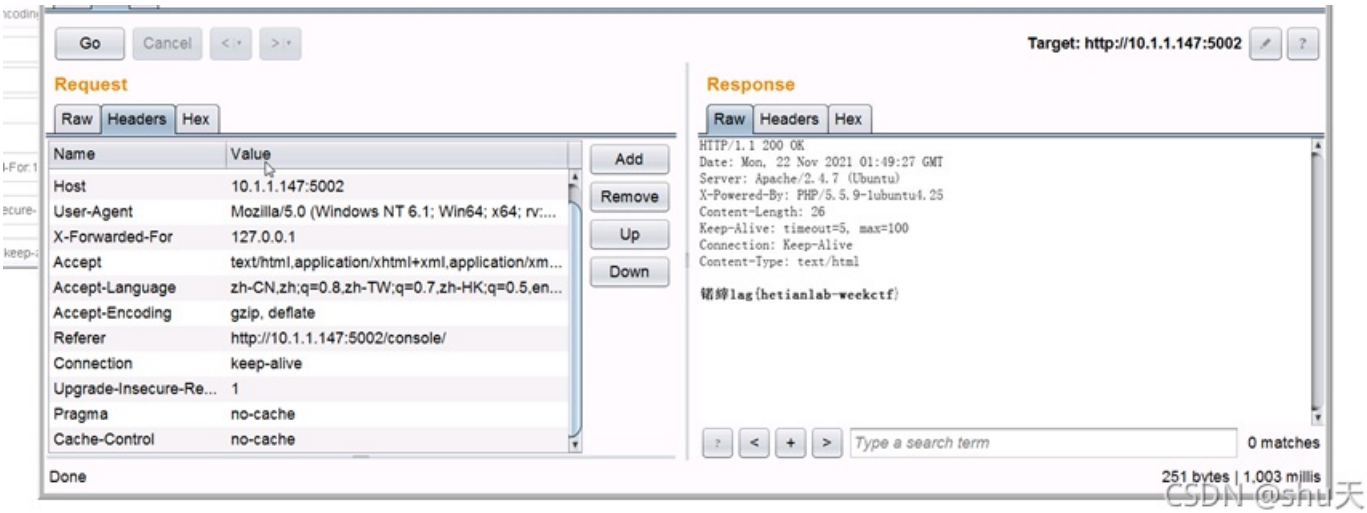


Flag{ctf_victory_SecBug}

第二周 | 就差一把钥匙

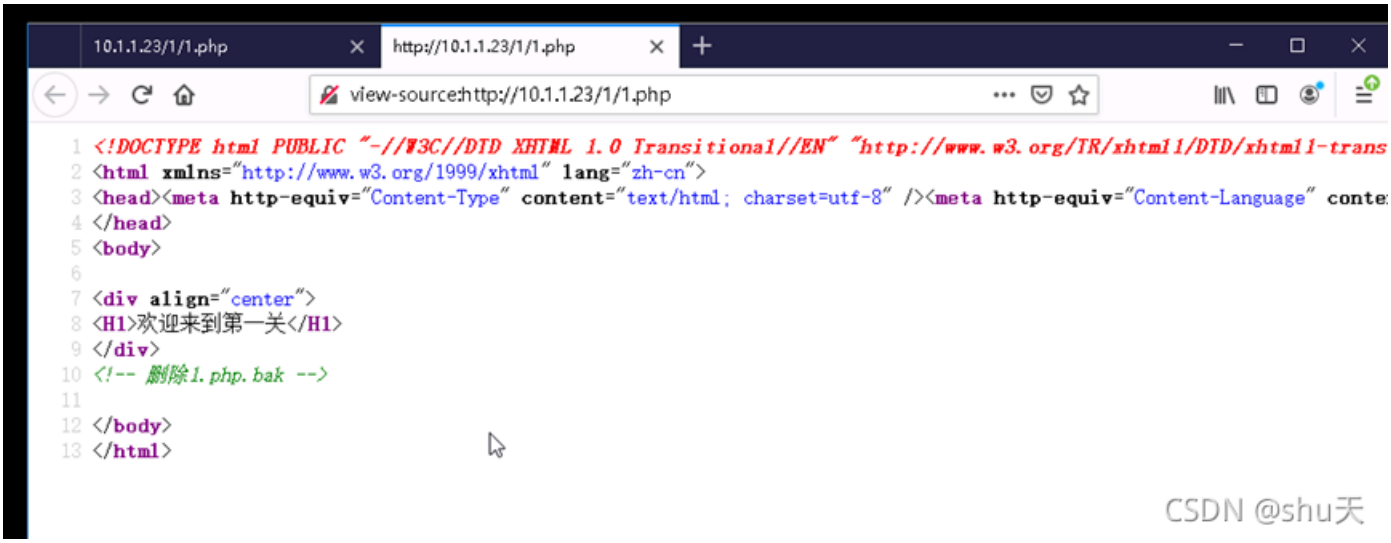
提示查看robots.txt，提示去console

修改header伪造本地地址X-Forwarded-For:127.0.0.1

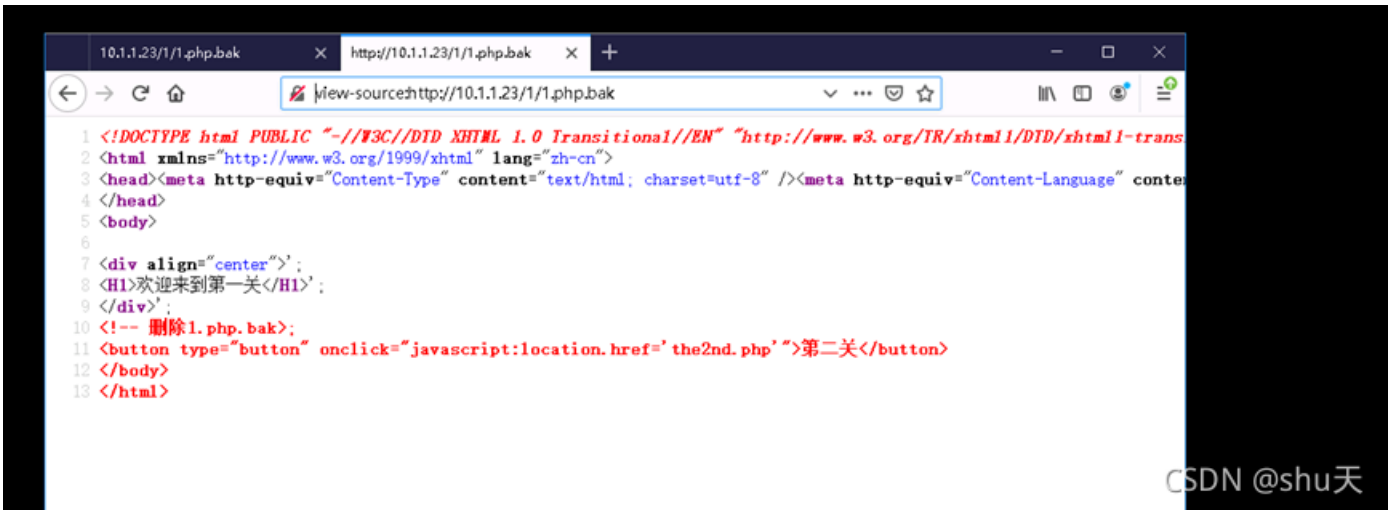


flag{hetianlab-weekctf}

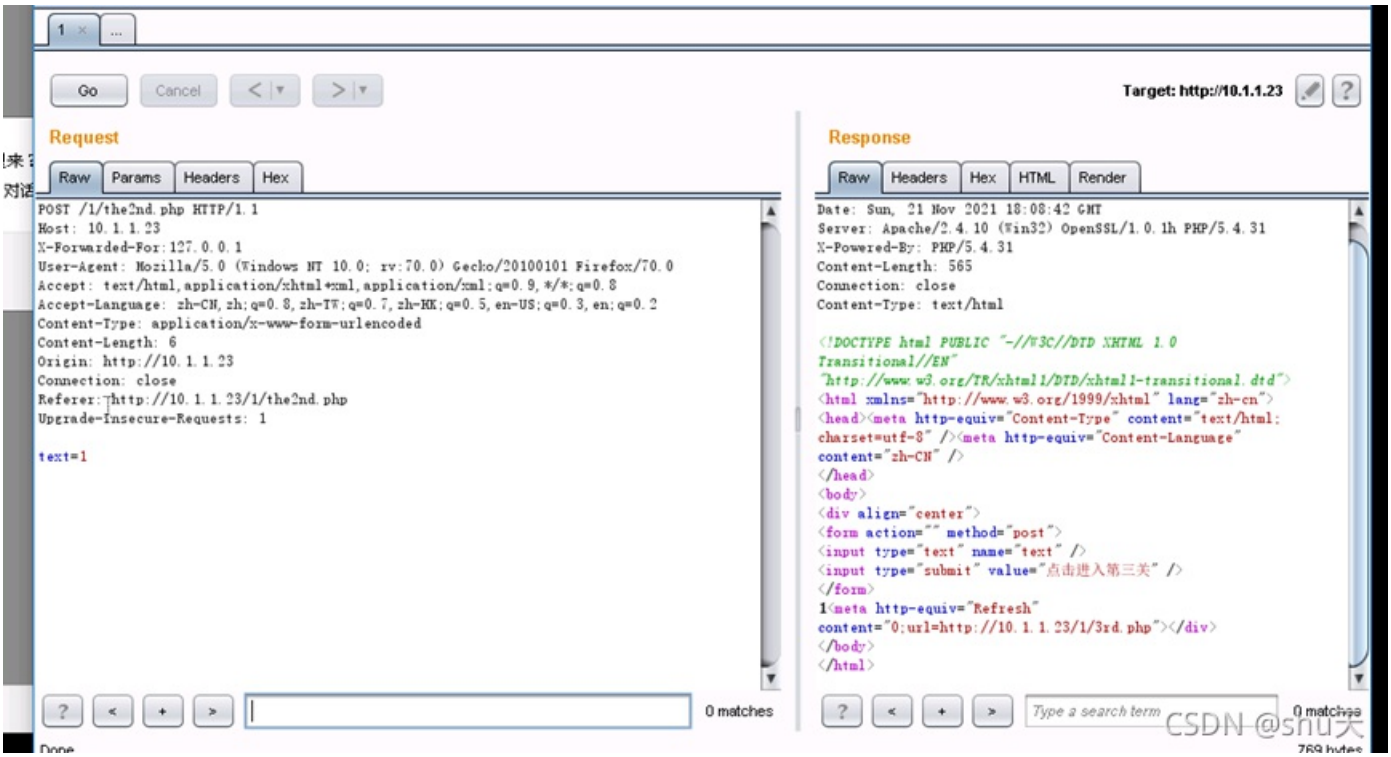
CTF-WEB小技俩



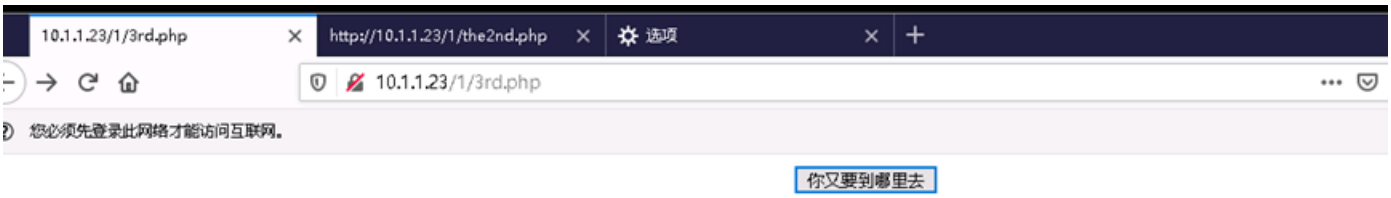
源码提示1.php.bak

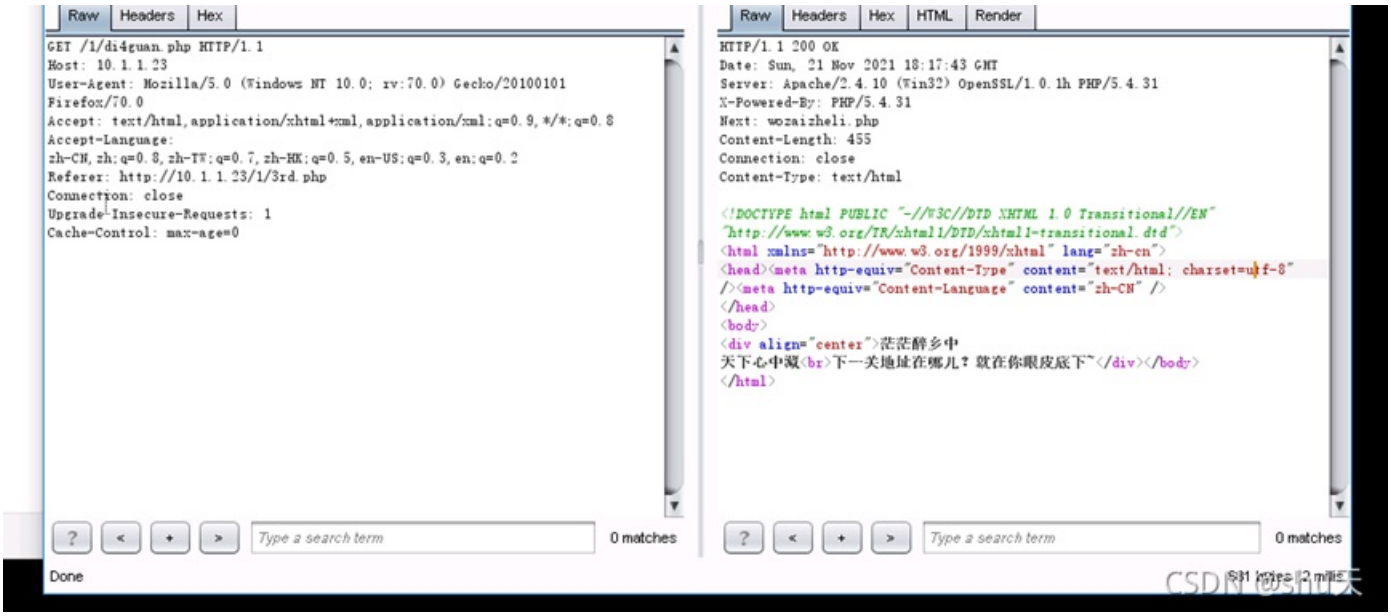


去the2nd.php

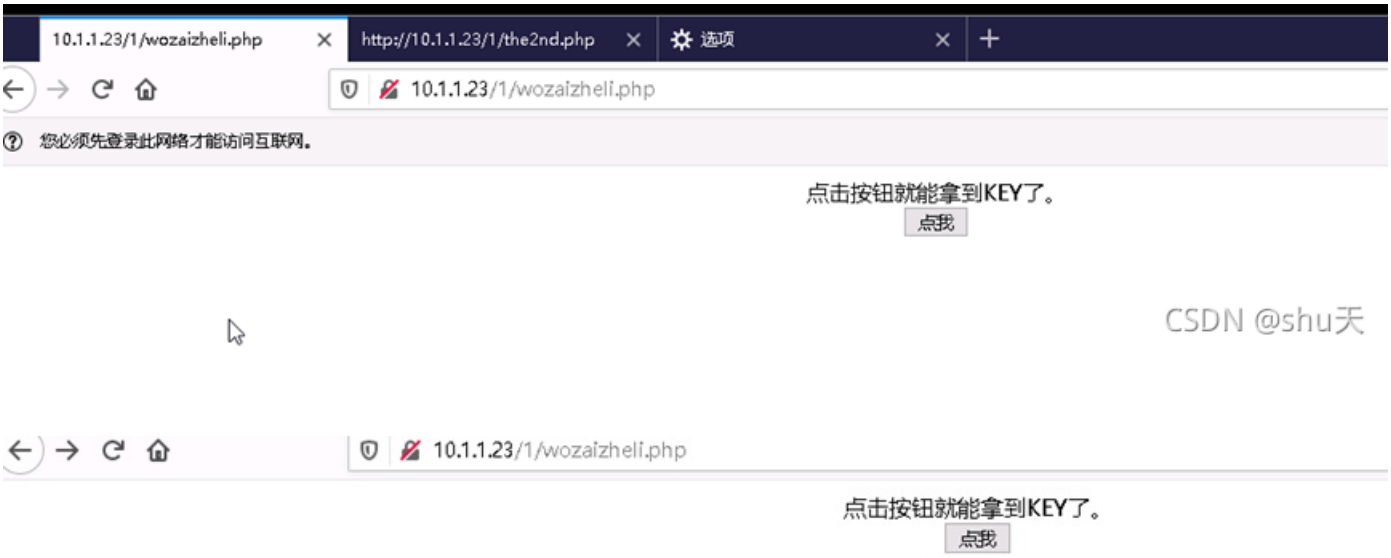


改XFF伪造失败，尝试js跳转





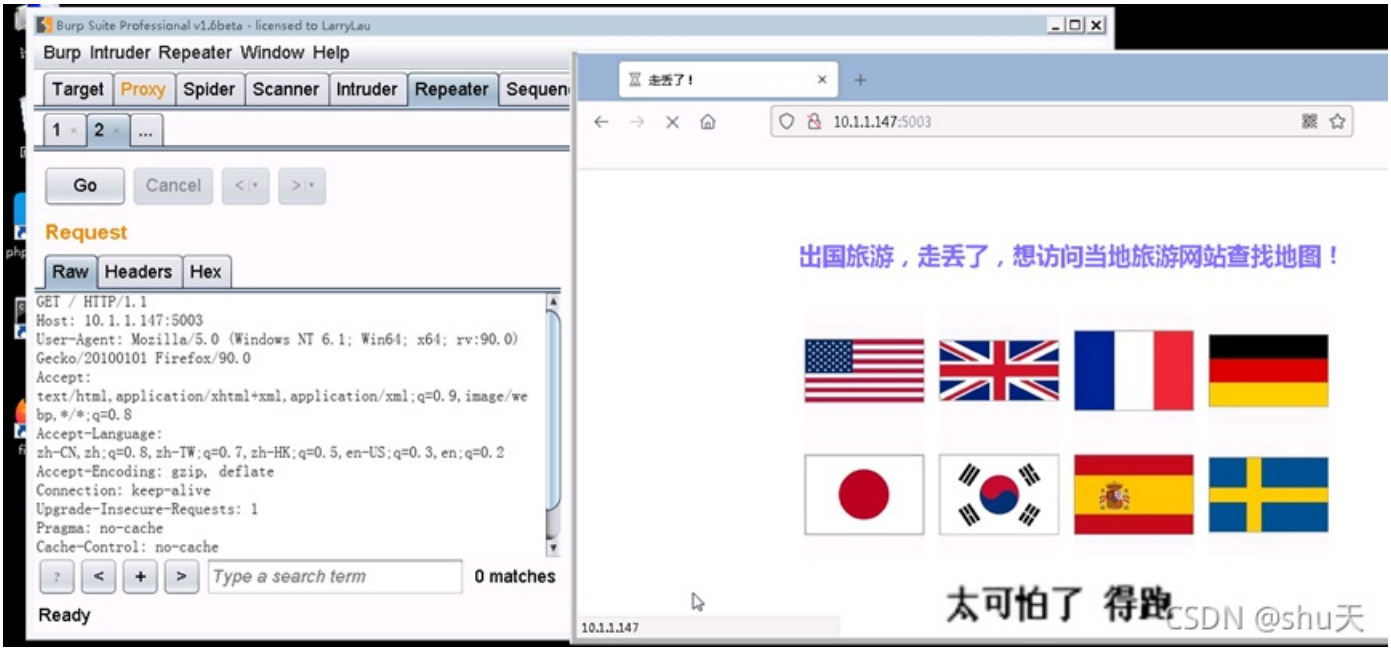
看到返回的Header里面有一个wozaizheli.php



这里有个js方法joy，鼠标移动到按钮，按钮就会消失，所以前端删去id=joy即可

过关

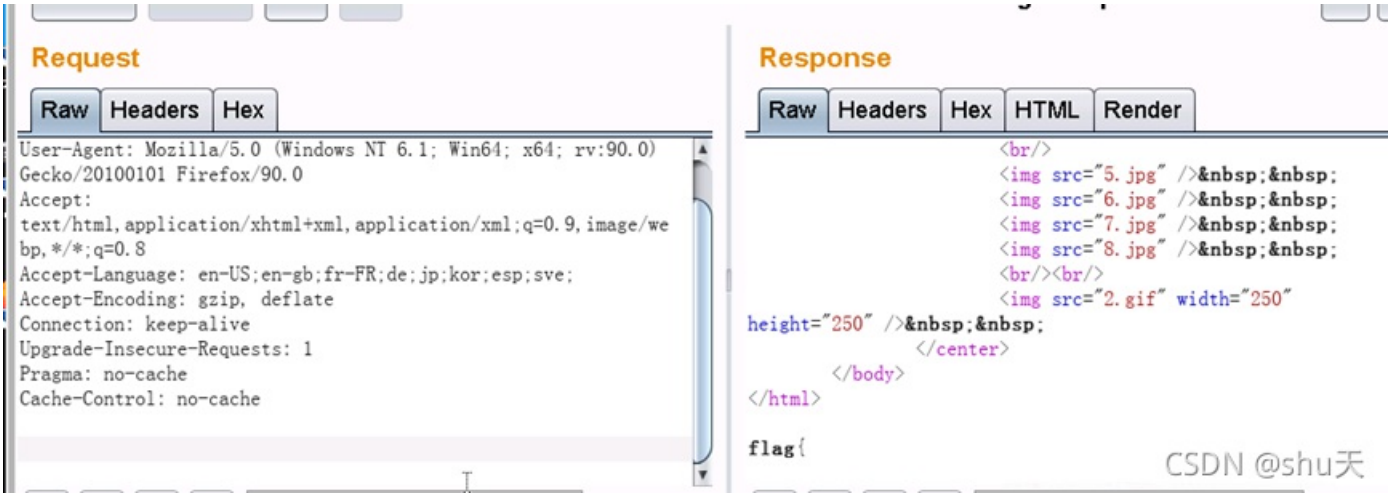
第三周 | 迷了路



抓包看header，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

根据页面各国国旗位置顺序，对应得出相应的accept-language代码：
美：en-us；
英：en-gb；
法：fr-FR；
德：de；
日：jp；
韩：kor；
西班牙：esp；
瑞典：sve；

Accept-Language: en-US;en-gb;fr-FRde;jp;kor;esp;sve;



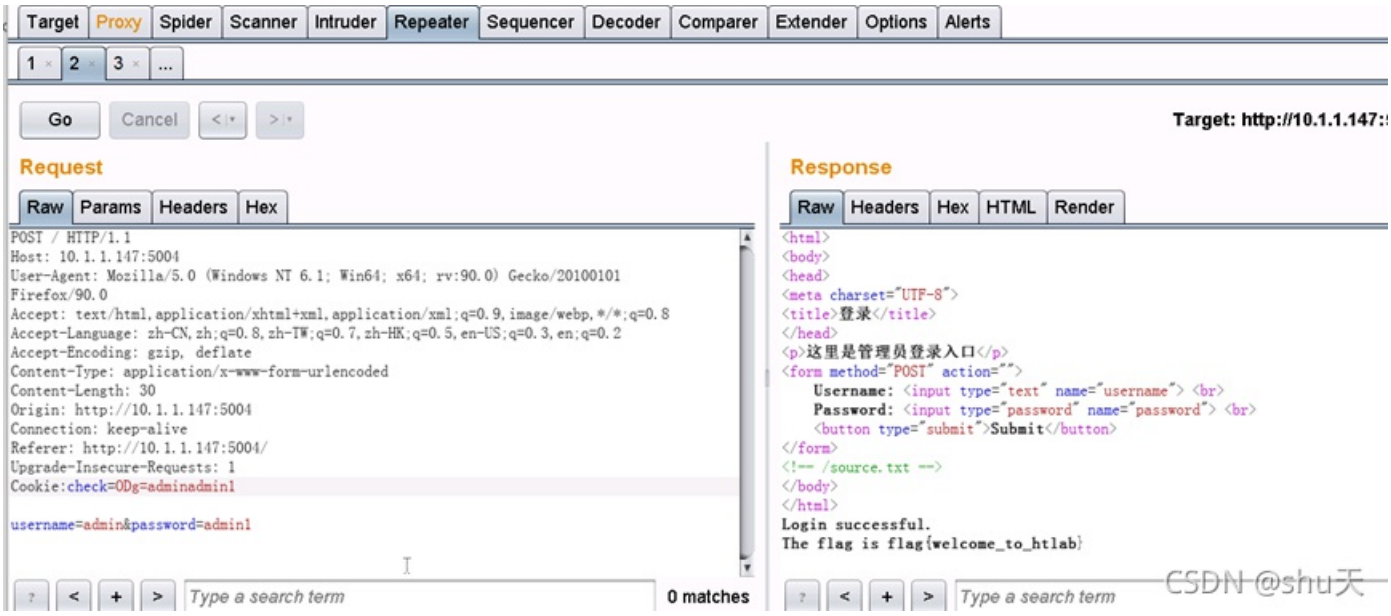
一个个改Accept-Language，得到flag
flag{Thisis_hetianlab@}

第四周 | Check your source code

<?php $flag = "XXXXXXXXXXXXXXXX"; $secret = "xx"; if(!isset($_POST["username"]) || !isset($_POST["password"])){ exit(); } $username = $_POST["username"]; $password = $_POST["password"]; if (!empty($_COOKIE["check"])) { if (urldecode($username) === "admin" && urldecode($password) != "admin") { if ($_COOKIE["check"] === base64_encode($secret) . urldecode($username . $password))) { echo "Login successful.\n"; die ("The flag is ". $flag); } else { die ("重新检查下你的cookie吧！ "); } } else { die ("你是不是管理员心里没点数吗？ "); } } setcookie("ahash", base64_encode($secret . urldecode("admin" . "admin")), time() + (60 * 60 * 24 * 7)); ?>

ahash = ODhhZG1pbmFkbWlu解密得到88adminadmin，88是$secret

根据代码构造cookie:check=ODg=adminadmin1，登陆



flag{welcome_to_htlab}