简单的CTF题

原创

即将成为大佬的菜鸡 于 2018-12-21 23:43:21 发布 2062 收藏 21

分类专栏： CTF 文章标签： 简单的ctf题目

本文链接：https://blog.csdn.net/weixin_44147777/article/details/85168392

我目前刷的题中的几个典型

题目来源：

学习平台

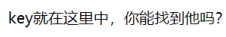
bugku

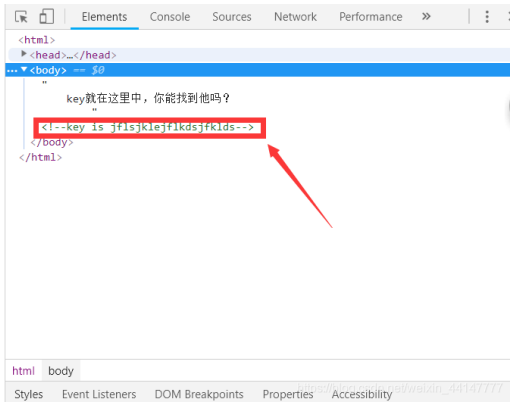
实验吧

菜鸡基础题

1.key

此题只需在点开链接后查看原码（按f12）即可得到key（火狐浏览器用firebug插件）

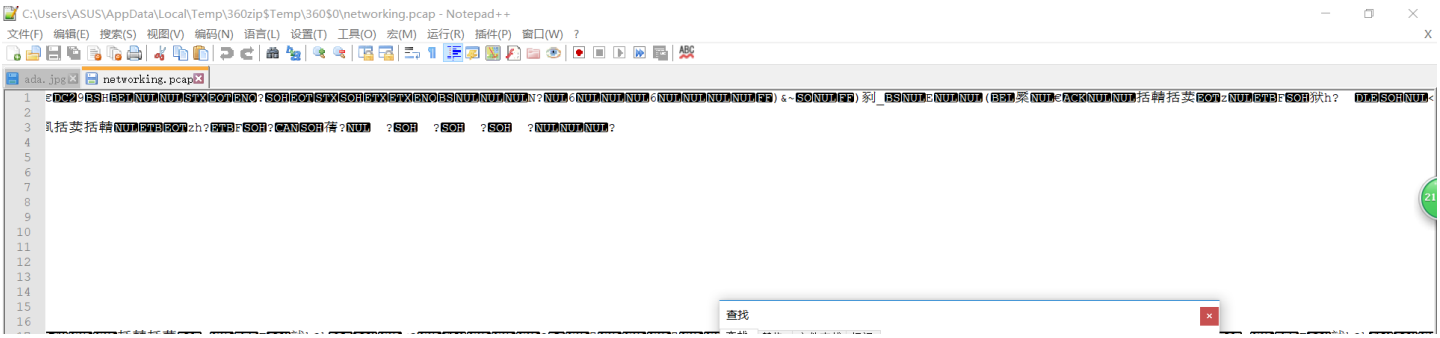


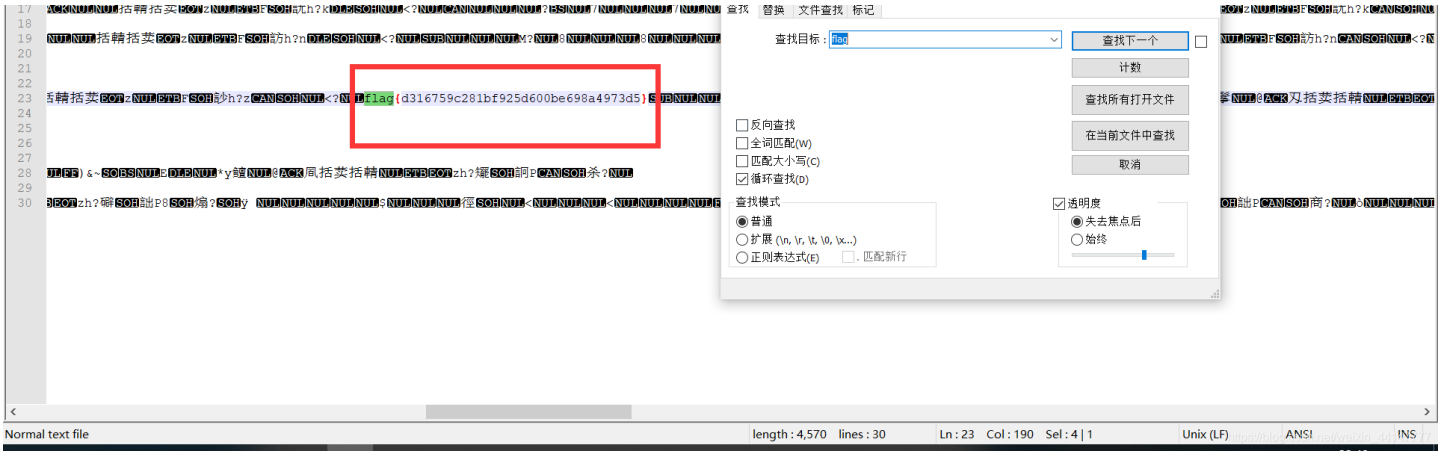


2.telnet

题目提示：flag{xxxxxxxxxx}

下载的zip文件中有个pcap文件，解压出来用nopated++打开，直接搜索“flag”即可。



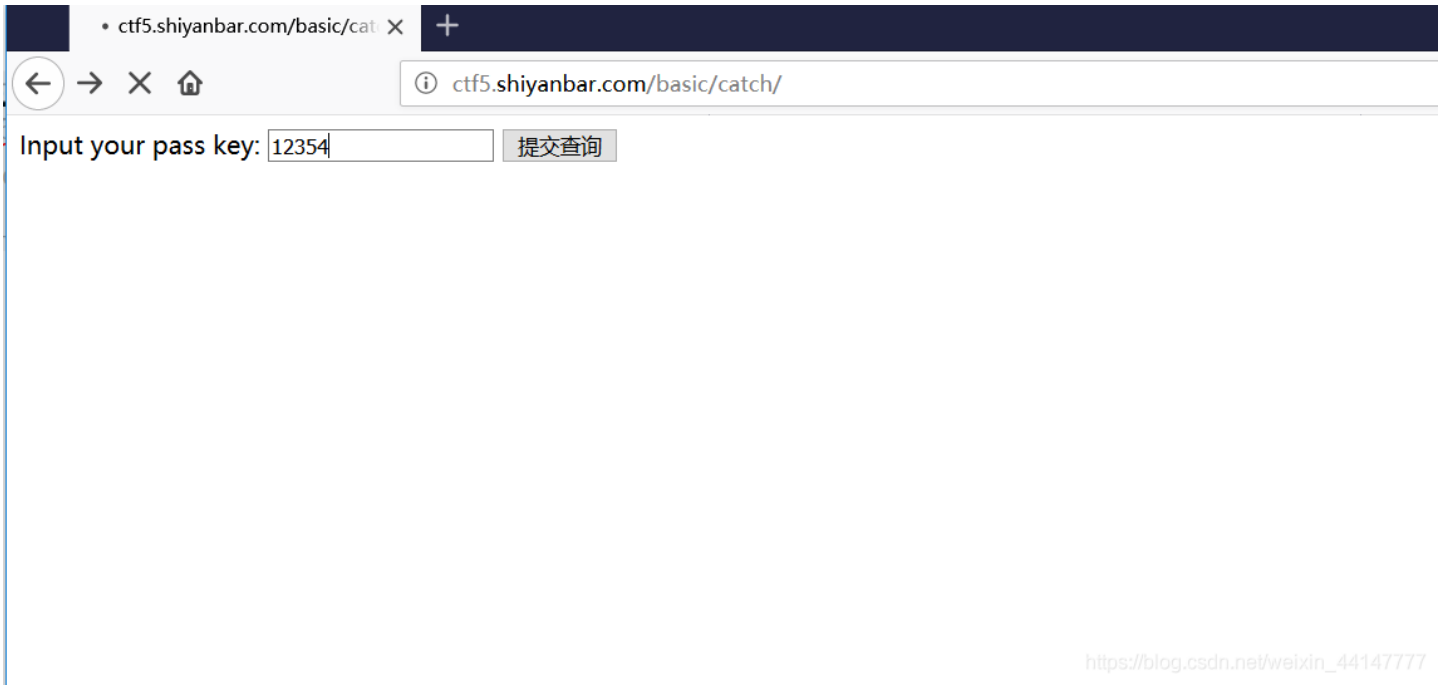


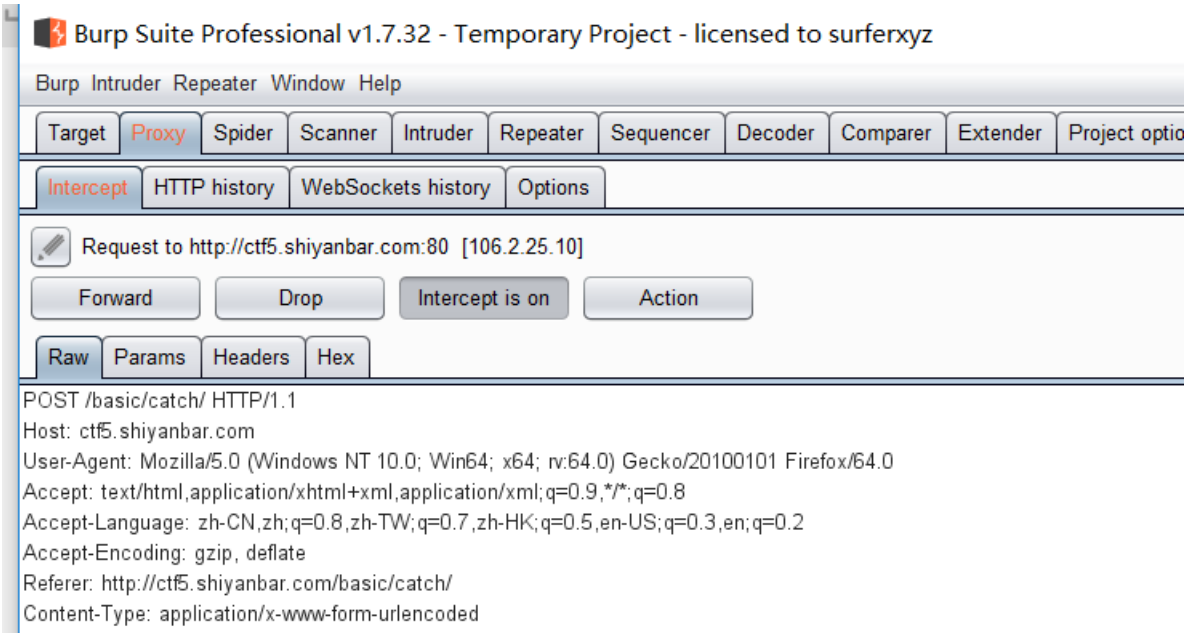
3.猫抓老鼠

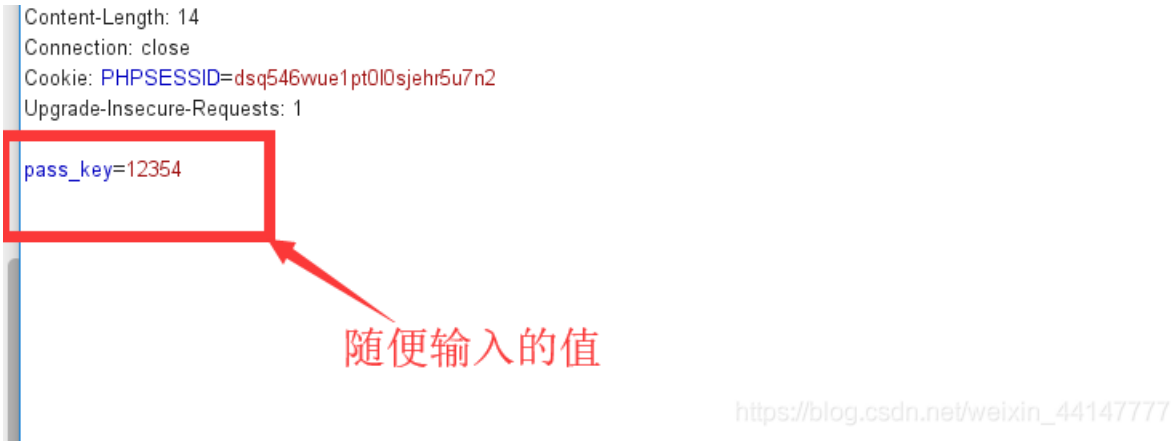
题目提示：catch！catch！catch！

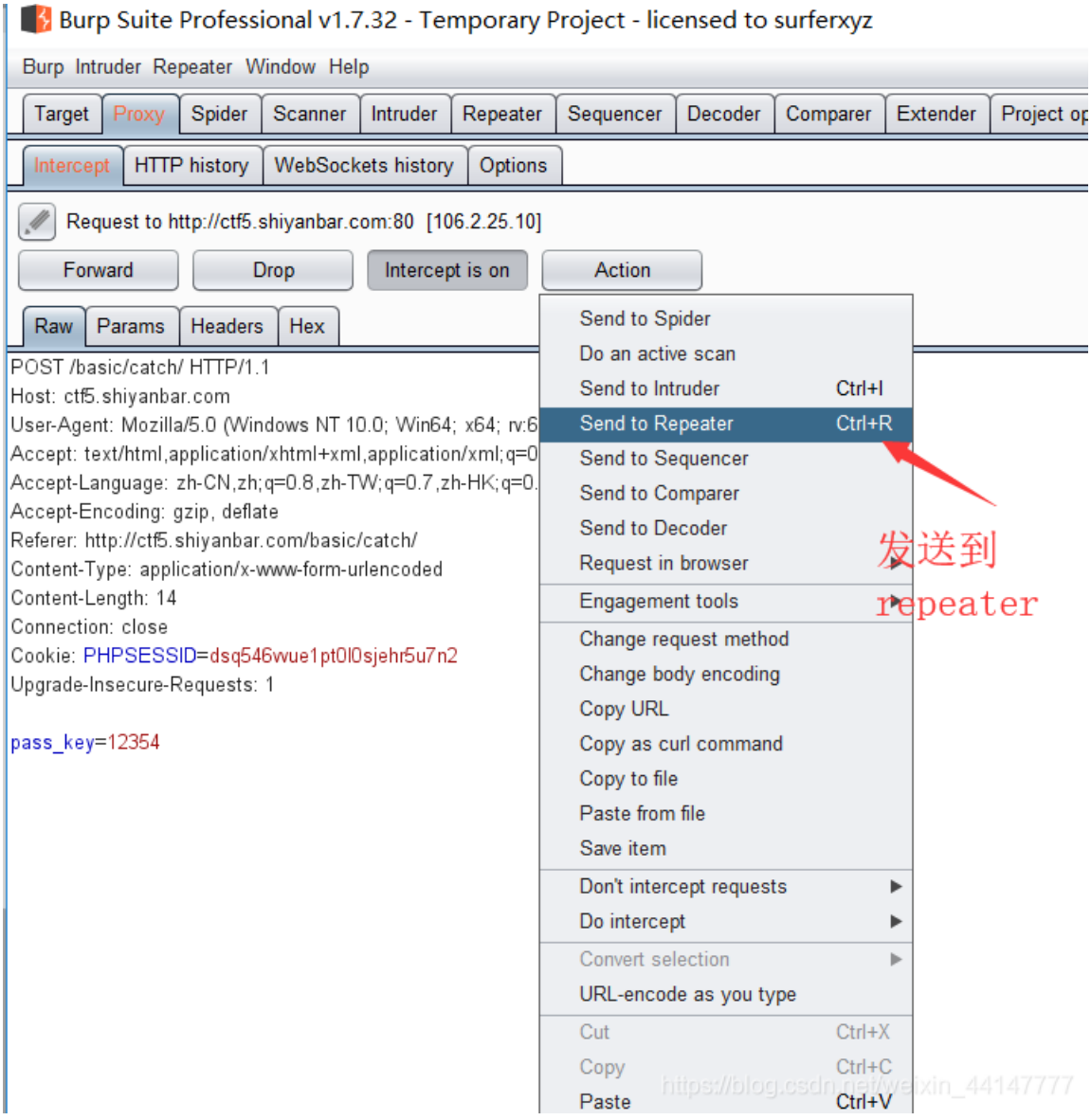
根据提示，选择抓包。

随便输入一串数字，开始抓包。

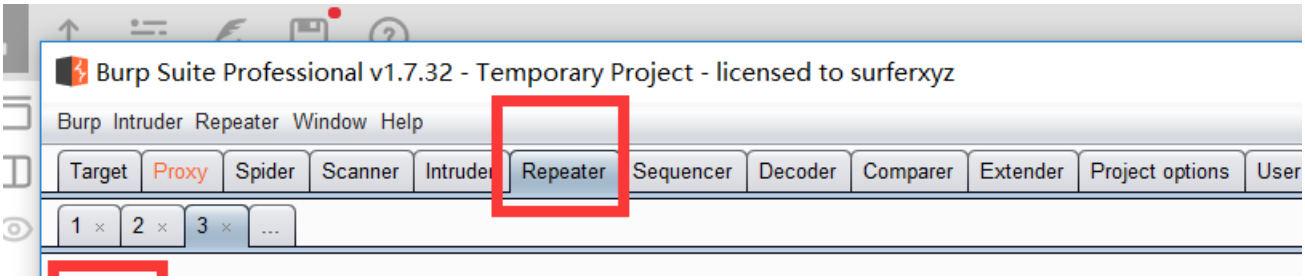


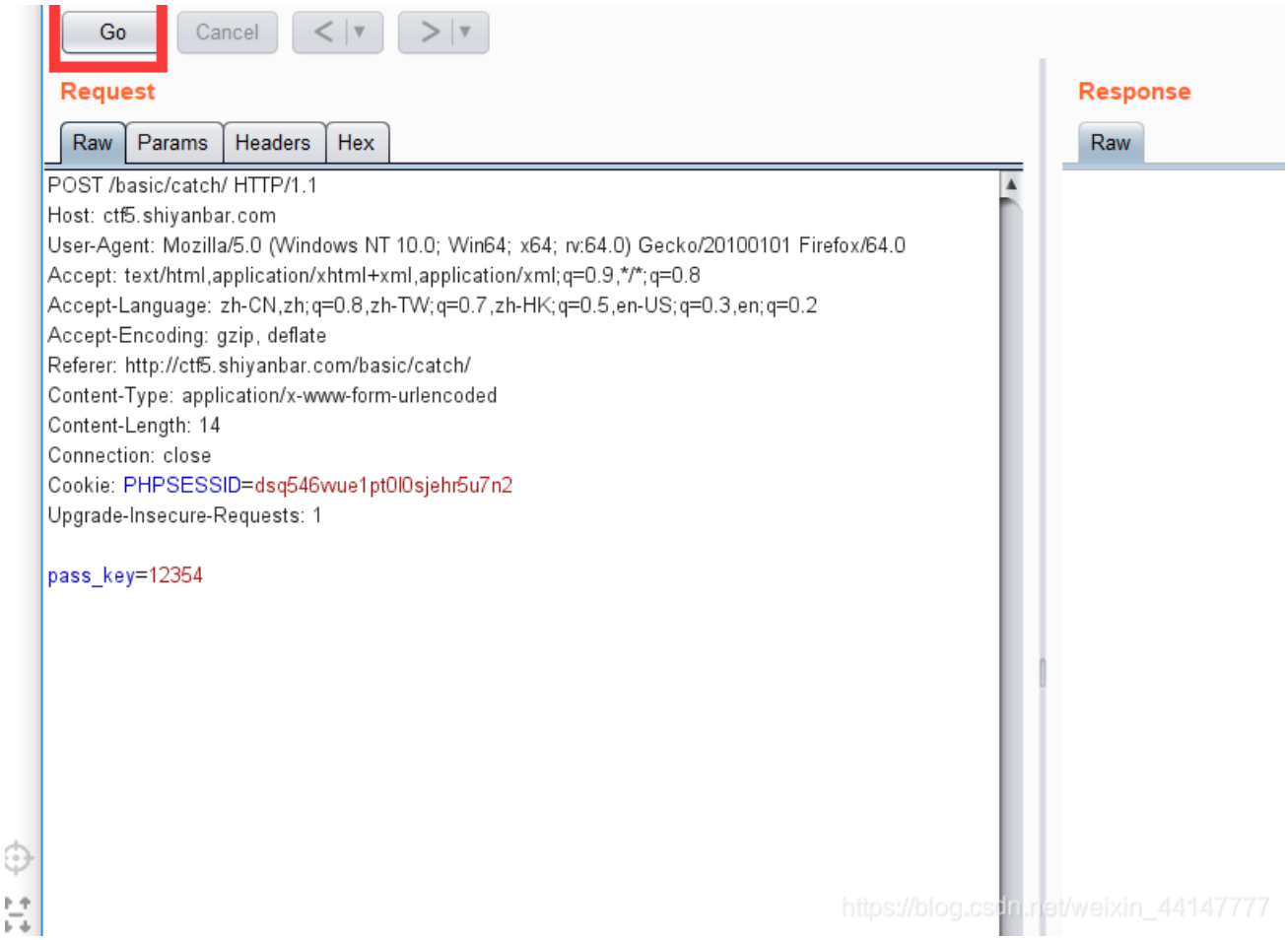


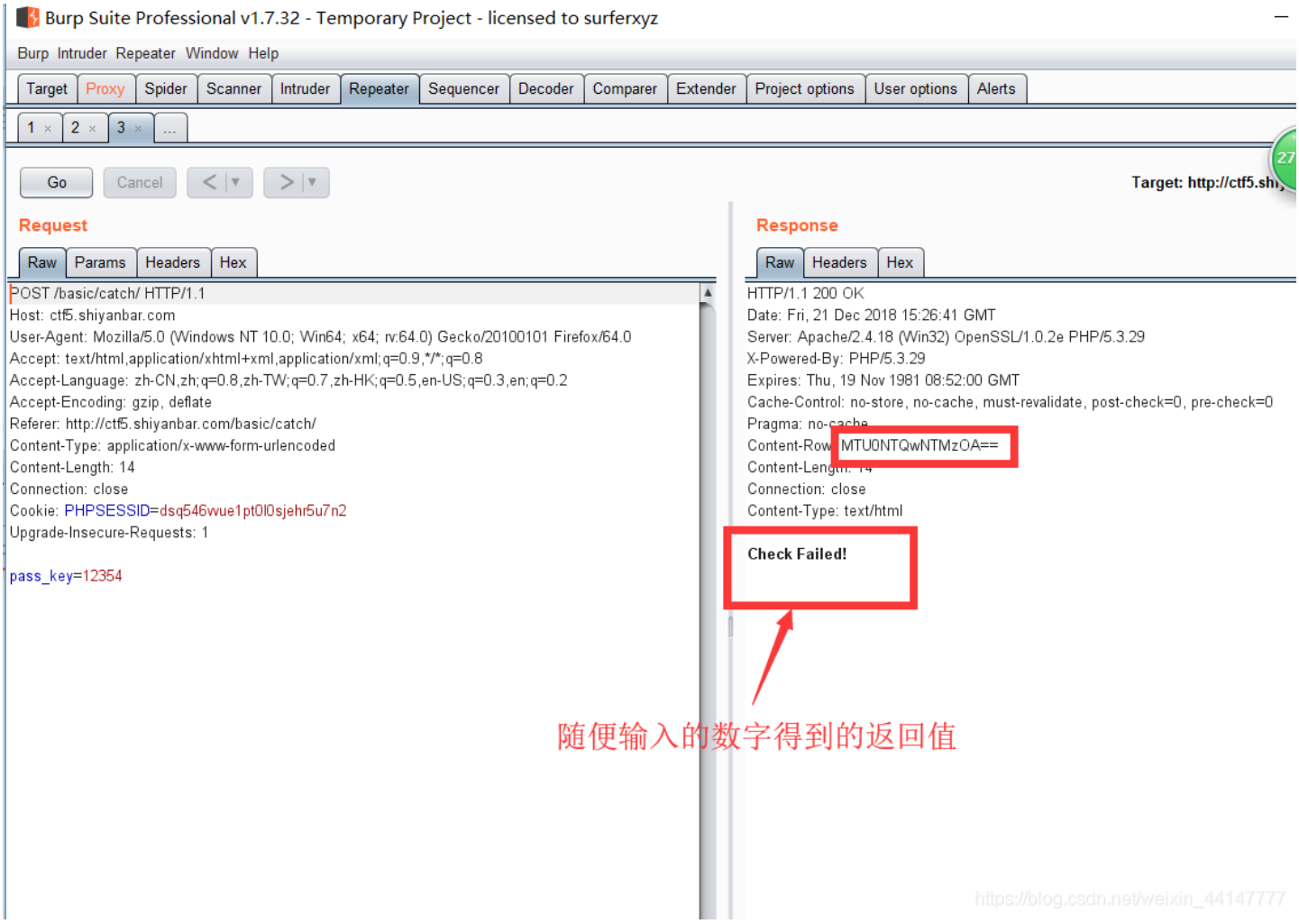




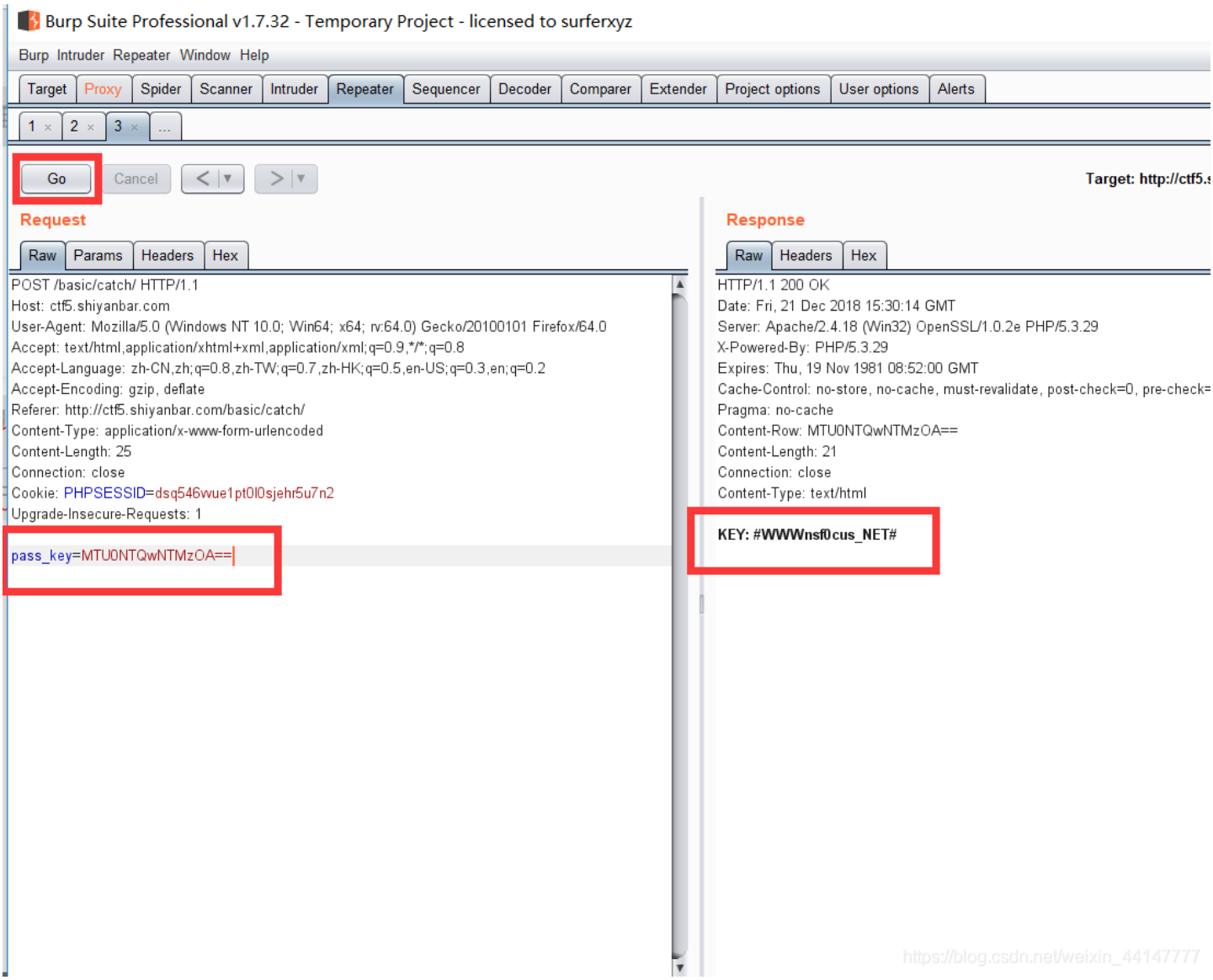
点开repeater，点go运行




Go
Cancel
Request
Raw
Params
Headers
Hex
POST /basic/catch/ HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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://ctf5.shiyanbar.com/basic/catch/
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
Connection: close
Cookie: PHPSESSID=dsq546wue1pt0l0sjehr5u7n2
Upgrade-Insecure-Requests: 1
pass_key=12354
Response
Raw
https://blog.csdn.net/weixin_44147777


Burp Suite Professional v1.7.32 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 3 ...
Go
Cancel
Target: http://ctf5.shi
Request
Raw Params Headers Hex
POST /basic/catch/ HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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://ctf5.shiyanbar.com/basic/catch/
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
Connection: close
Cookie: PHPSESSID=dsq546wue1pt0l0sjehr5u7n2
Upgrade-Insecure-Requests: 1
pass_key=12354
Response
Raw Headers Hex
HTTP/1.1 200 OK
Date: Fri, 21 Dec 2018 15:26:41 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Row MTU0NTQwNTMzOA==
Connection: close
Content-Type: text/html
Check Failed!
随便输入的数字得到的返回值
https://blog.csdn.net/weixin_44147777

将Content-Row的值输到pass_key=中，再次点go运行，便可得到key。



这些是目前我做的比较典型的题（当然我目前也做不出再难的）#手动狗头#，才刚刚入门请大佬们见谅(还有一些杂项的题之后在po）。