

实验吧ctf web题猫捉老鼠

原创

ZweLL032 于 2017-03-16 23:05:45 发布 2427 收藏

文章标签: [web](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/ZweLL032/article/details/62470773>

版权

解题链接: <http://ctf5.shiyanbar.com/basic/catch/>

首先点进去



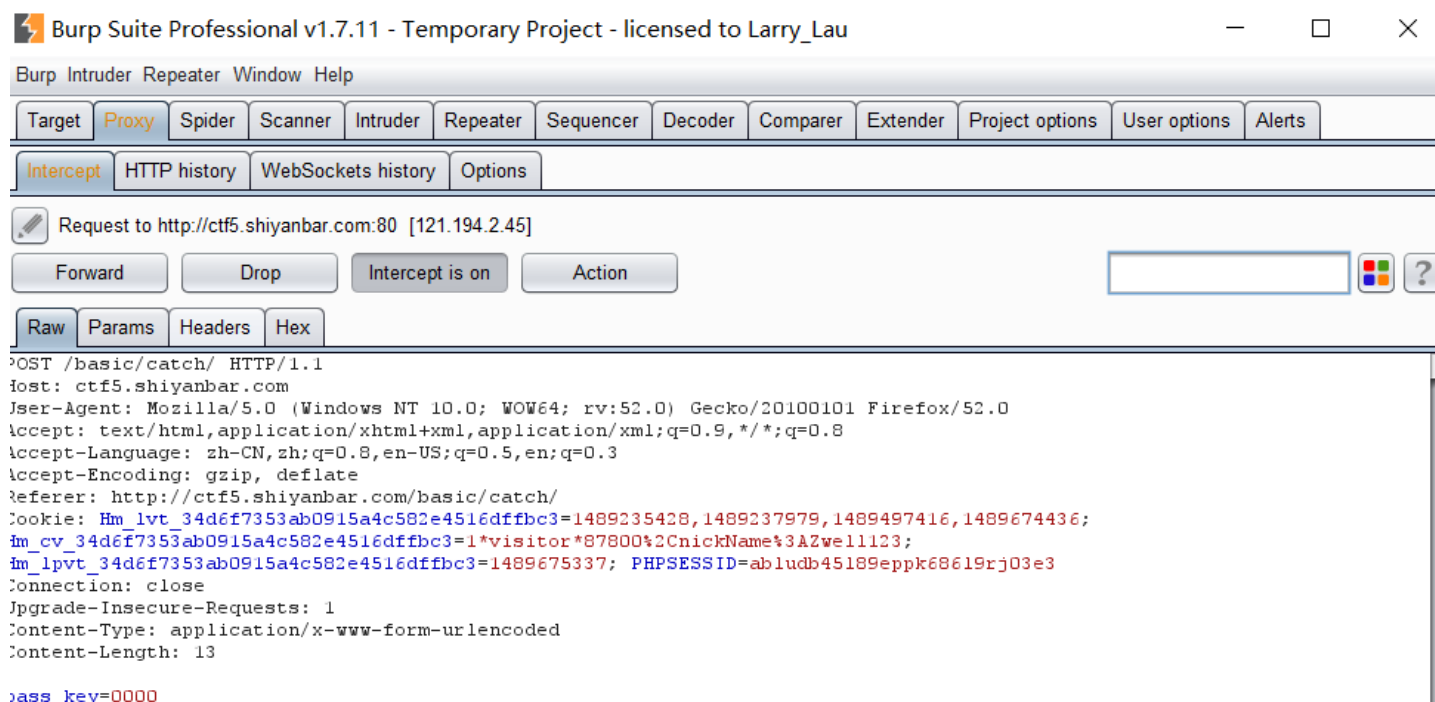
<http://blog.csdn.net/ZweLL032>

然后抓包 题目都提醒了catch catch 所以应该抓包首先随便提交0000进去 看到的结果是这个

Check Failed!

<http://blog.csdn.net/ZweLL032>

然后用Burpsuite抓包



然后发送到repeater

Burp Suite Professional v1.7.11 - Temporary Project - licensed to Larry_Lau

Target: http://ctf5.shiyanbar.com

Request

Raw Params Headers Hex

```
POST /basic/catch/ HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0)
Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/basic/catch/
Cookie:
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1489235428,1489237979,1489497416,1489674436;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*87800%2CnickName%3A2we11123;
Hm_lpv_34d6f7353ab0915a4c582e4516dffbc3=1489675337;
PHPSESSID=abludb45189eppk68619rj03e3
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 13

pass_key=0000
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Thu, 16 Mar 2017 15:01:01 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.2.17
X-Powered-By: PHP/5.2.17
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: MTQ4OTY3NTMzNw==
Content-Length: 14
Connection: close
Content-Type: text/html

Check Failed!
```

0 matches

Content-Type: text/html

KEY: #WWWnsf0cus_NET#

/blog.csdn.net/ZweLL032

首先看response回应 肯定是那个 好然后把它的值粘贴复制到pass_key得到这个结果
题方法就是这样

此题的解