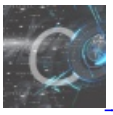
CTF之catch

原创

Unitue_逆流 于 2017-04-04 22:18:09 发布 817 收藏

分类专栏： Burp-Suite 文章标签： CTF

本文链接：https://blog.csdn.net/lijia111111/article/details/69216790

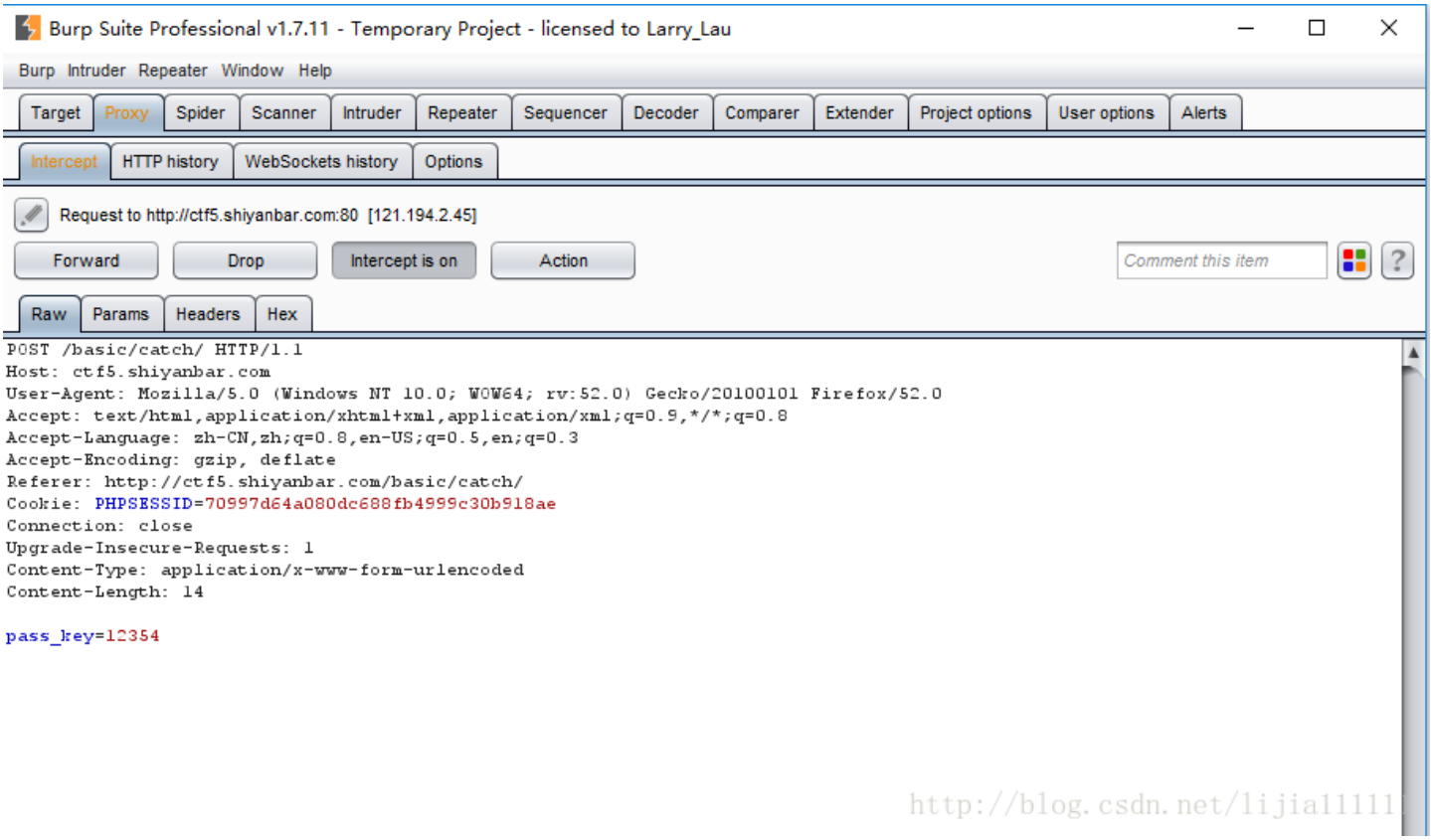

Burp-Suite 专栏收录该内容

3 篇文章 0 订阅

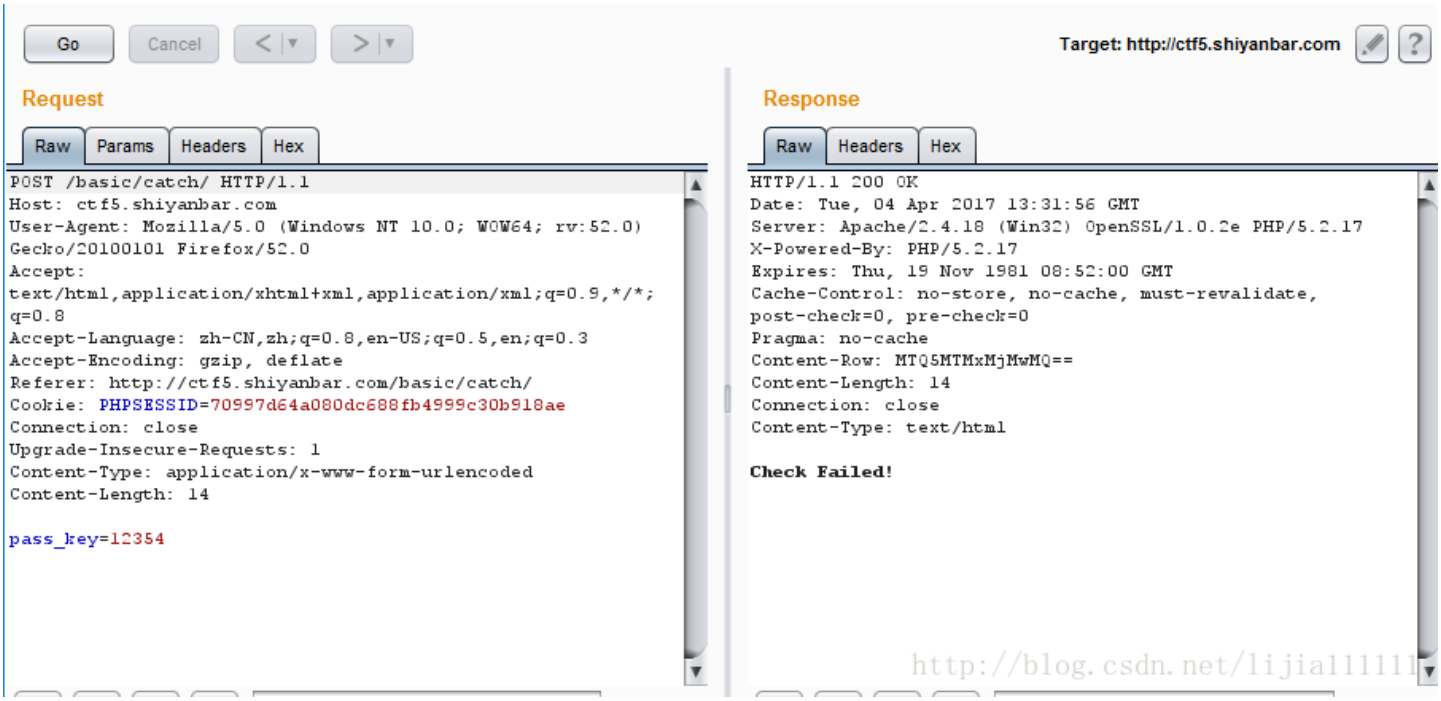
订阅专栏

随便输入一个密码

使用Burp进行抓包，如下：



将抓取的直接发送到repeater,点击go,得到Content-Row的值，直接复制后粘贴到key值，然后再次点击go，得到key值，如下图：



Go | Cancel | < | > | 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: PHPSESSID=70997d64a080dc688fb4999c30b918ae
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 14

pass_key=MTQ5MTMxMjMwMQ==
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Tue, 04 Apr 2017 13:31:56 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: MTQ5MTMxMjMwMQ==
Content-Length: 14
Connection: close
Content-Type: text/html

Check Failed!
```


Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Tue, 04 Apr 2017 13:34:04 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: MTQ5MTMxMjMwMQ==
Content-Length: 21
Connection: close
Content-Type: text/html

KEY: #WWWnsf0cus_NET#
```