




实验吧——WEB-猫抓老鼠

原创

小白白@  于 2019-03-30 16:21:37 发布  2627  收藏

分类专栏: [CTF](#)

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/weixin_44677409/article/details/88914301

版权



[CTF 专栏收录该内容](#)

23 篇文章 2 订阅

订阅专栏

猫抓老鼠

拿到题目，随便输了个123，显示"Check Failed!"。然后查看了一下源码，发现没什么线索。

Input your pass key:

开始抓个包看看：

<pre>POST /basic/catch/ HTTP/1.1 Host: ctf5.shiyanbar.com User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:66.0) Gecko/20100101 Firefox/66.0 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 Referer: http://ctf5.shiyanbar.com/basic/catch/ Content-Type: application/x-www-form-urlencoded Content-Length: 12 Connection: close Cookie: Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1553927142; Hm_lpv_34d6f7353ab0915a4c582e4516dffbc3=1553931744; Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*193895%2CnickName%3A%E5%B0%8F%E7%99%BD%E7%99%BD%40; PHPSESSID=698ma0m9gho3ej85foq4eknnl4 Upgrade-Insecure-Requests: 1 pass_key=123</pre>	<pre>HTTP/1.1 200 OK Date: Sat, 30 Mar 2019 08:08:22 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: MTU1MzkzMTc0Ng== Content-Length: 14 Connection: close Content-Type: text/html Check Failed!</pre>
--	---

在响应头信息中我们可以看到一行Content-Row的信息（至于这个字段是具体什么东西，也没有查到），一看就知道是经过base64加密的，然后去解码看看，得到一串数字1553931746，想着拿着个数字去试试，还是失败。后来发现不需要解码，直接输入密文就好了，也就是MTU1MzkzMTc0Ng==

<pre>POST /basic/catch/ HTTP/1.1 Host: ctf5.shiyanbar.com User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:66.0) Gecko/20100101 Firefox/66.0 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 Referer: http://ctf5.shiyanbar.com/basic/catch/ Content-Type: application/x-www-form-urlencoded Content-Length: 25 Connection: close Cookie: Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1553927142; Hm_lpv_34d6f7353ab0915a4c582e4516dffbc3=1553931744; Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*193895%2CnickName%3A%E5%B0%8F%E7%99%BD%E7%99%BD%40; PHPSESSID=698ma0m9gho3ej85foq4eknnl4 Upgrade-Insecure-Requests: 1 pass_key=MTU1MzkzMTc0Ng==</pre>	<pre>HTTP/1.1 200 OK Date: Sat, 30 Mar 2019 08:13:26 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: MTU1MzkzMTc0Ng== Content-Length: 21 Connection: close Content-Type: text/html KEY: #WWWnsf0cus_NET#</pre>
---	---

然后就拿到flag了，可是在最后提交的时候题目也没有给出什么格式，试了好几种格式最后才试出来直接提交KEY后面的值就好了

也就是

```
#WWWnsf0cus_NET#
```