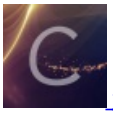
实验吧web几题writeup

原创

Daniel-0 于 2017-04-01 18:05:04 发布 512 收藏
分类专栏： writeup

本文链接：https://blog.csdn.net/D_pokemon/article/details/68946524

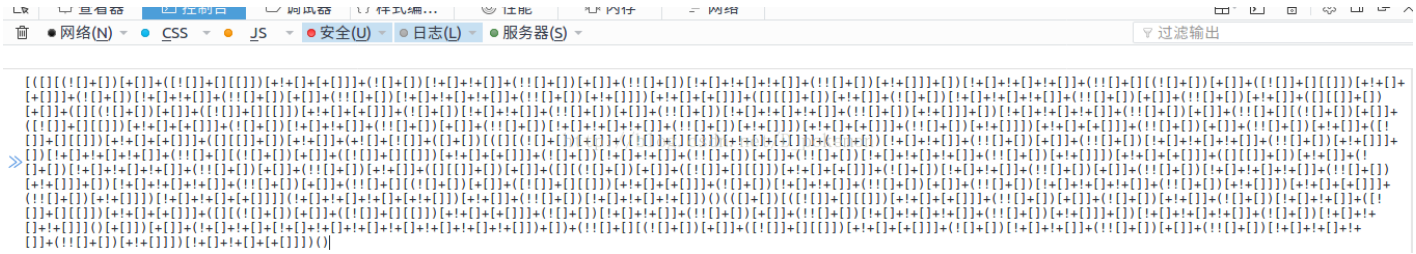

writeup 专栏收录该内容
17 篇文章 0 订阅
订阅专栏

01：

what a fuck!这是什么鬼东西?

解题链接：http://ctf5.shiyanbar.com/DUTCTF/1.html 通过

打开链接做题，发现是一串js，按下F12，打开控制台，复制所有的编码到控制台，回车即可拿到flag。

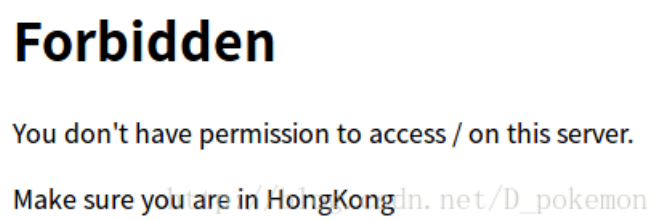


02：

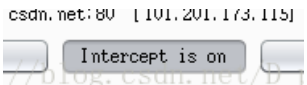
不要相信此题有提示描述哦!

解题链接：http://ctf5.shiyanbar.com/basic/header/ 通过

打开题目链接做题。



题目说：make sure you are in hongkong ， 这题应该要用到burp，首先配置浏览器的代理，打开burp。



保证intercept is on,然后刷新一下网页，再打开burp。看到获取的信息，因为题目说make sure you are in hongkong，所以修改一下accept language。

```
Accept-Language: zh-hk,zh;
```

然后点击GO ，拿到flag。

```
r><br>KEY:12
```

03:

catch! catch! catch! 嘿嘿，不多说了，再说剧透了

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

题目描述catch，catch，想到应该还是抓包，打开题目链接做题。

Input your pass key: 334444 提交查询

先随便输入一个key，会提示你check failed，同样配置代理，看到burp获取的内容，

```
nnection: keep-ali
grade-Insecure-Requ
ntent-Type: applica
ntent-Length: 15

ss_key=334444
```

会显示你刚刚提交的key，点击GO，

```
Pragma: no-cacne
Content-Row: MTQ5MTA0MDE4Ng==
Content-Length: 14
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Check Failed!
```

同样看到 check failed，同时看到上面的content-row，选择这个内容提交。

```
pass_key=MTQ5MTA0MDE4Ng==
```

然后继续点击GO。看到flag。

```
KEY: #WWW
```

只截图一部分flag，自己动手做吧。