

2016华山杯 writeup

原创

Recar 于 2016-09-10 18:40:05 发布 1252 收藏

分类专栏: [CTF学习 小技巧](#)

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/qq_28295425/article/details/52496416

版权



[CTF学习 同时被 2 个专栏收录](#)

2 篇文章 0 订阅

订阅专栏



[小技巧](#)

39 篇文章 0 订阅

订阅专栏

web

1、签到

微信回复得到flag

2、打不过~

http://huashan.xdsec.cn/ctf_hs_00b.php

发现submit被禁止了, 更改为允许, type="submit". burp抓包。看到显示了一个str

The screenshot shows the Burp Suite interface with a request and response view. The request is a GET request to `/ctf_hs_00b.php?Password=1&submit=Submit`. The response is an HTML page with a form. A red arrow points to a Base64 encoded string in the response headers: `Str: @GH0HzU1NTc3HTdhMTQ4NTc4ZmQ4MjJhYVYwM0TYwNzk=`.

发现是base64, 解码得到字符串, 觉得应该是MD5, 在进行MD5解码, 得到flag

3、系统管理

是西普实验吧的原题。。。。好尴尬啊。上网搜了下

```
writeuphttp://www.cnblogs.com/puluotiya/p/5388910.html  
http://www.cnblogs.com/zaki-Gui/p/5717958.html
```

注意的是用户名要是MD5值为0exx的然后密码为数组:

```
a:2:{s:4:"user";b:1;s:4:"pass";b:1;}
```

提交, 得到flag。

4、简单js, , 不是我做的, 队友做的。。等学会了在补充~

5、弹弹弹! xss, 我xss不行, 比完队友开车带我xss

6、233

坑了我好久的题

JSFUCK运行出来显示乱码。。我凌乱了。问了下朋友, 我没懂。。去百度了下。是编码问题ANSI->Unicode。一句话加密。转为16进制。出来 `%<e exucetr qeeuts"(@eys0t3g"t%)>` 这个我当时想这个怎么的还要怎么编码啊。研究了好久。突然朋友告诉我两两互换。。我想骂人。我怎么没发现。。。。

7、无间道。上传文件。神队友做的。

Forensics

1、蒲公英的约定

我到现在都不知道这些题给的提示怎么用。。。。

我用的Stegsolve, 走了几个发现二维码, 并且颜色是反的, 队友把颜色改了回来。。我服。扫码得类似base64编码。不行, 那么上base32。成功得到flag

2、什么鬼

这个吧, 得到图片, 这个大一定有文件, 重命名为rar, 有密码, 爆破。得到图片。那个, 我直接PS图片了。得到flag。。。我们队今天做了这么几道题。就两个人。我相信以后会更好。

collapsar

FlappyPig的writeup

<http://bobao.360.cn/learning/detail/3019.html>

官方writeup

链接: <https://pan.baidu.com/s/1bRS9mY> 密码: x32g

题目打包下载

<https://yunpan.cn/ckyrKxHJDPAIN> (提取码: bbaF)