XCTF bug wp

原创

Garybr0 于 2021-01-15 16:38:01 发布 73 收藏

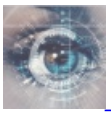
分类专栏： CTF writeup 文件上传 文章标签： XCTF bug 越权

本文链接：https://blog.csdn.net/weixin_45253216/article/details/112673040

CTF writeup 同时被 2 个专栏收录

16 篇文章 0 订阅

订阅专栏



文件上传

2 篇文章 0 订阅

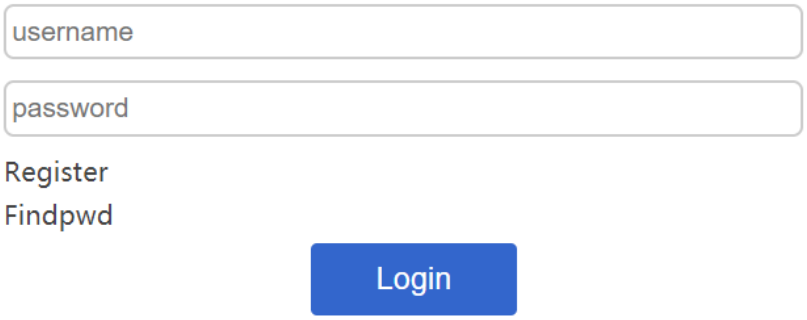
订阅专栏

~~网安菜鸡今天又来划水子~~

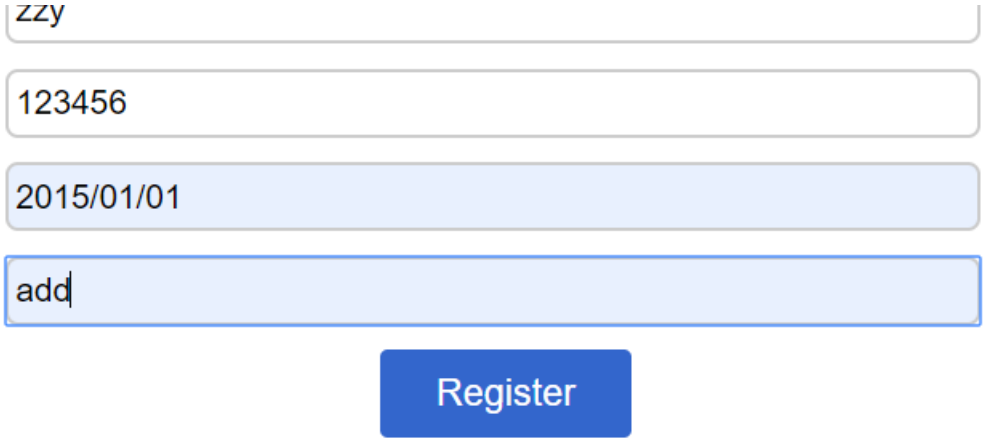
CTF题目属于萌新入门级，写下WP仅供自己总结练习，大佬请自行绕路，另外如果有师傅愿意有**每日轻松一笑**环结，还望不吝赐教。【狗头】

题目

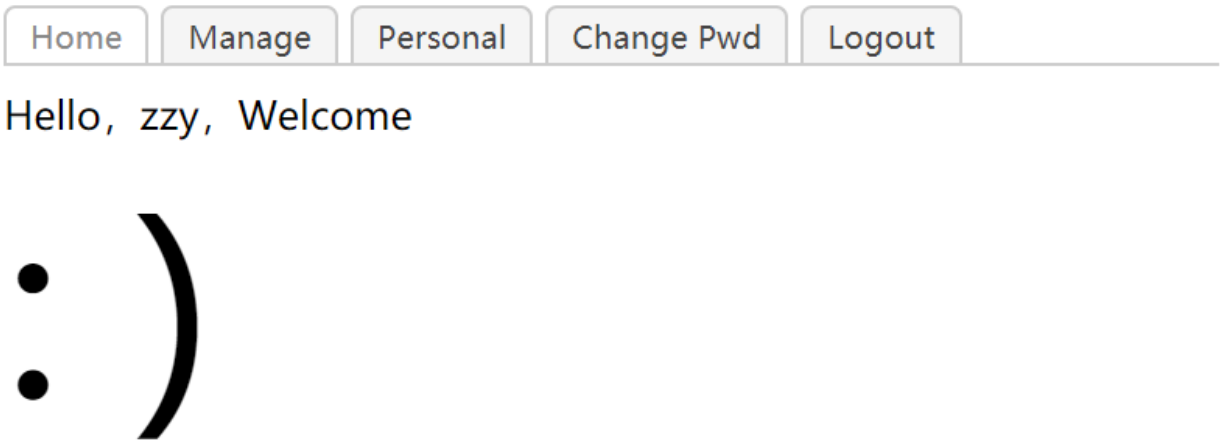
首先打开题目，是一个登陆注册框



有用户名和密码，没有用户名密码可以注册，忘记密码可以找回，先随便注册一个，看看是何方神圣。

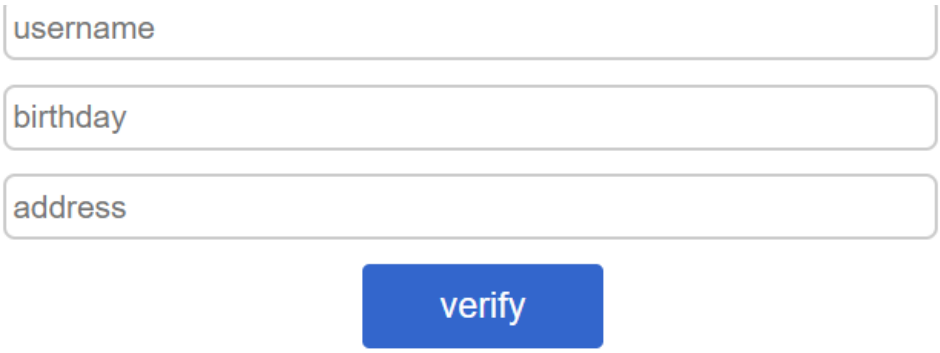


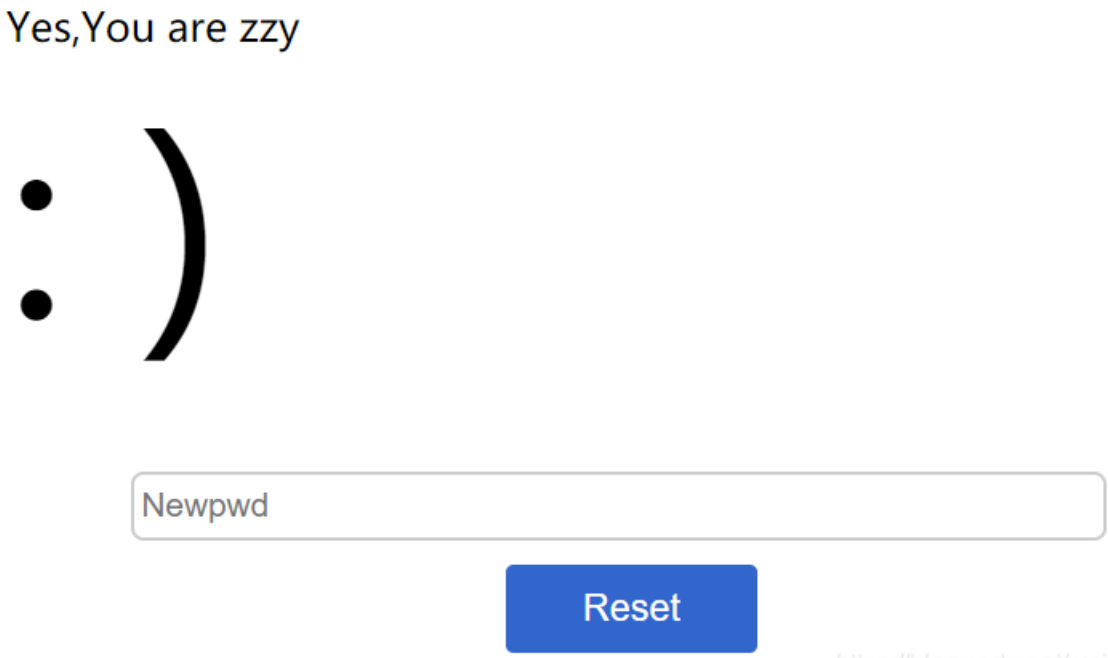
显示我们uid是5，emmm猜测一波咱们可能是第五个注册的用户。



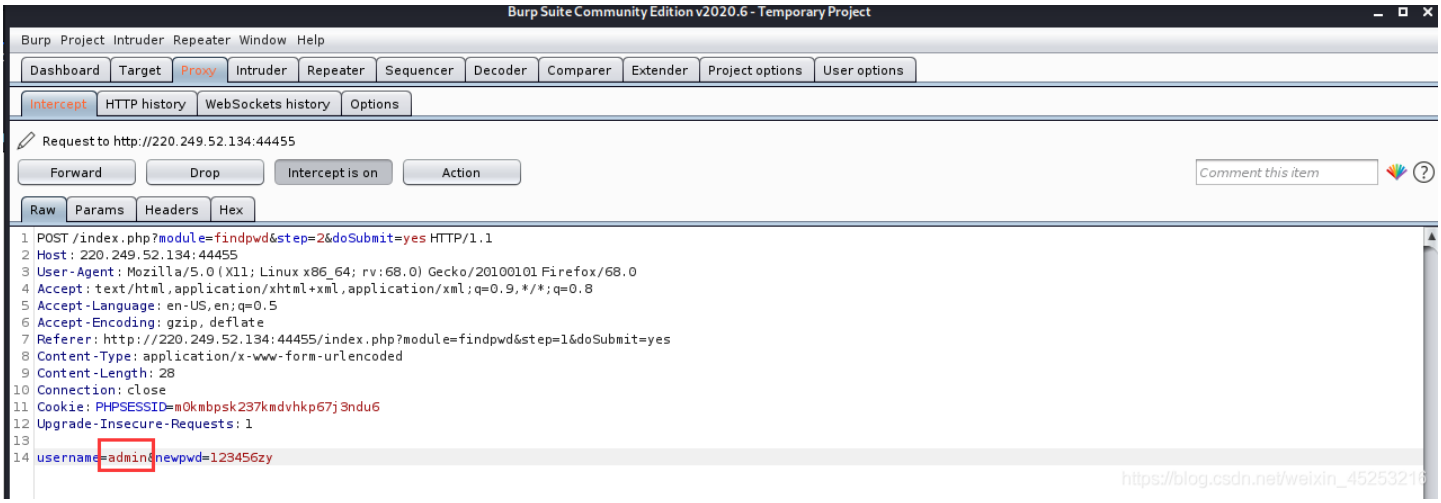
进来发现了几个供我们选择的选项，有管理，个人信息查看，修改密码，退出登录。
点了一圈发现manage需要admin权限

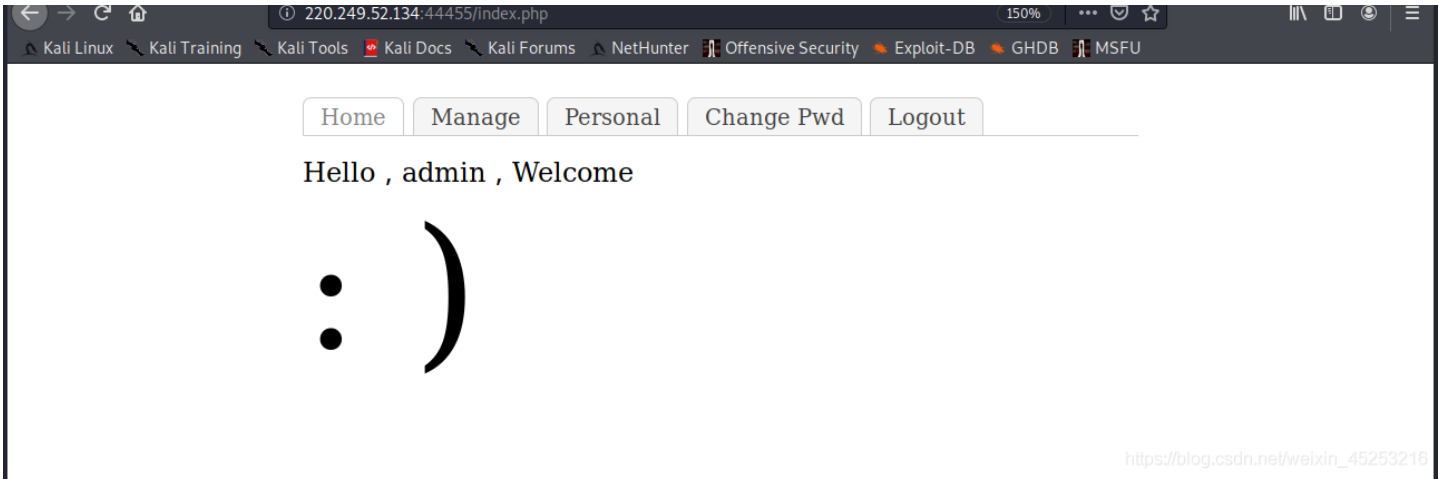
考虑怎么能拿到admin权限，思路1就是对账号admin进行密码爆破，但是实用性不高，考虑到本题有很多功能模块，所以想到了思路2，根据FindPwd进行admin密码重置。
这里找回密码的验证机制是，需要你输入生日和地址进行身份验证，验证通过后即可修改密码。



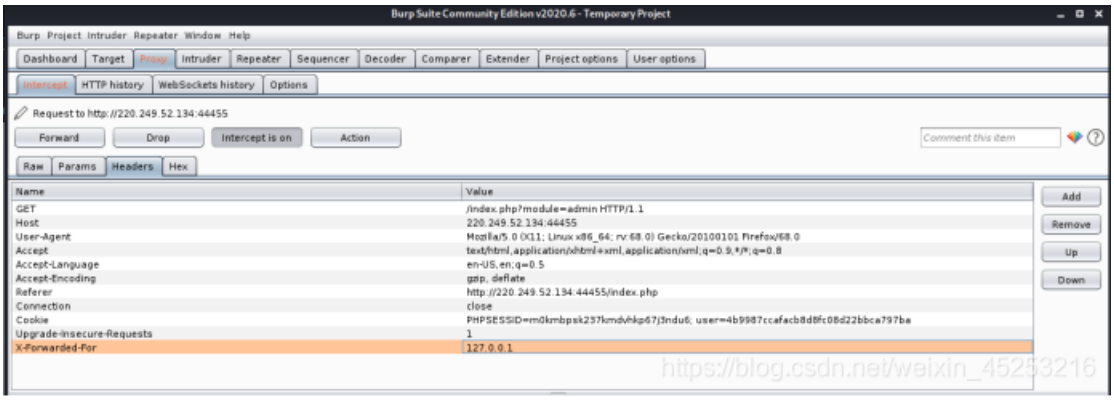


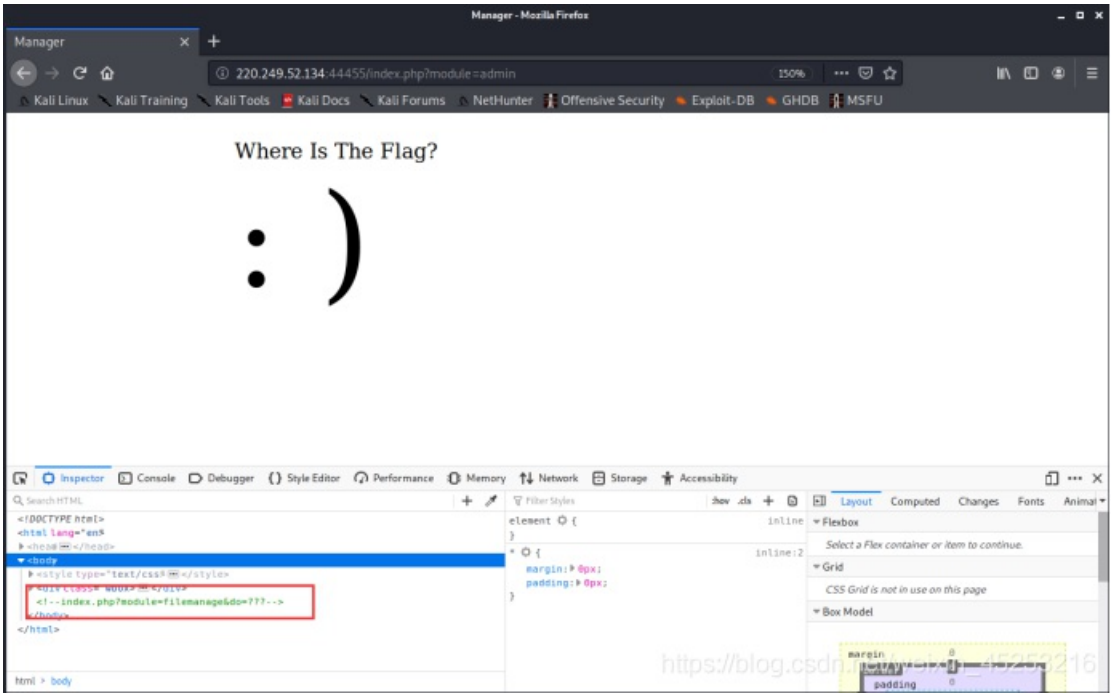
这里是有东西可以利用的，告诉我们yes你是zzy，然后就可以重置密码了，抓个包就能看到，发出的post表单时username=XXX，newpassword=XXX，我们可以把username改为admin。





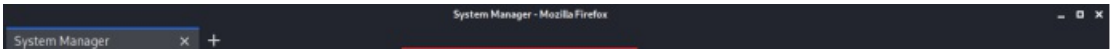
然后，我们就能以admin的身份登陆进来了。点击manage，提示IP地址有问题，还是抓包在http headers里添加XFF为本地ip127.0.0.1

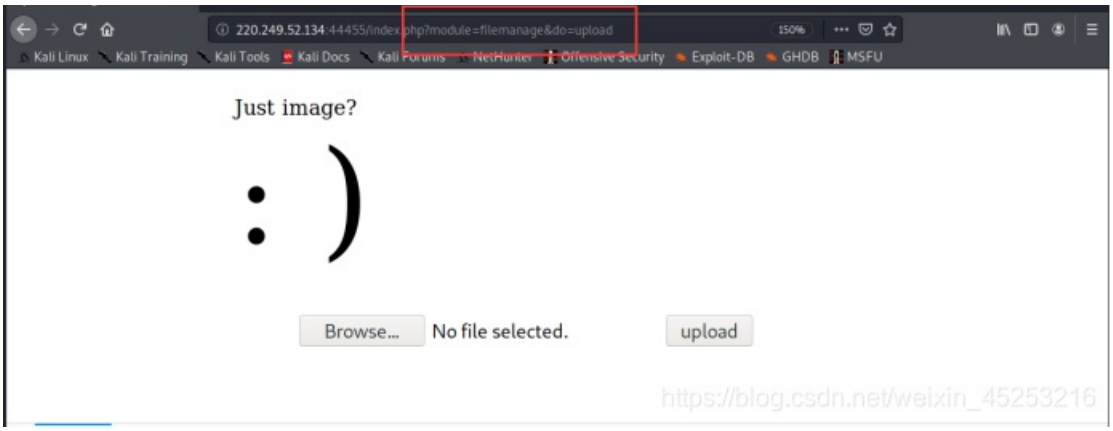




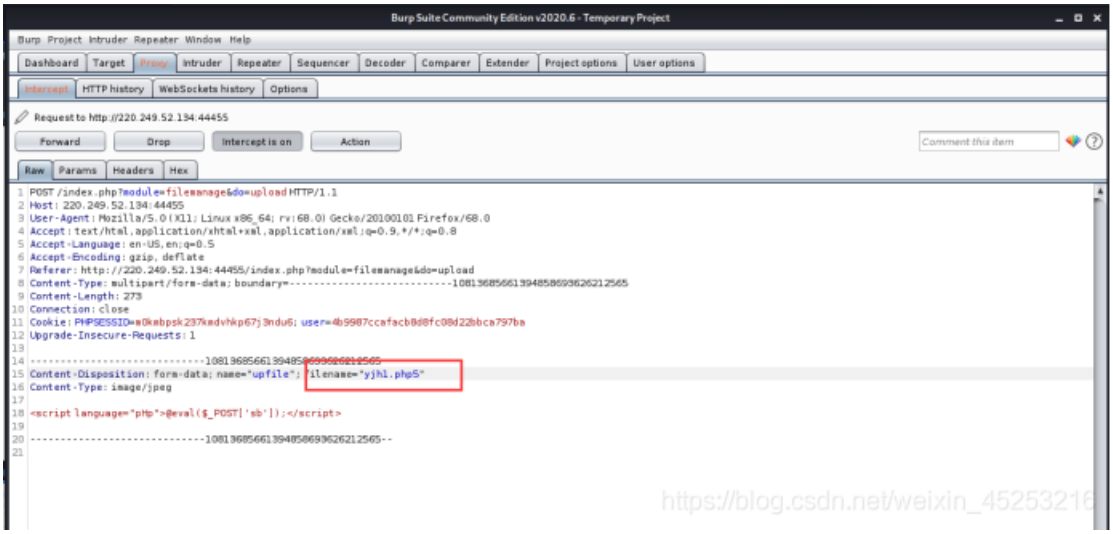
进来后F12看到页面注释提示，?model=filemanage&do=???

功能是文件管理，并且给了一个接口，~~自己当然想不出来啥~~，在大佬的提示下，一个就意识到是文件上传，于是do=upload，就看到了文件上传的页面

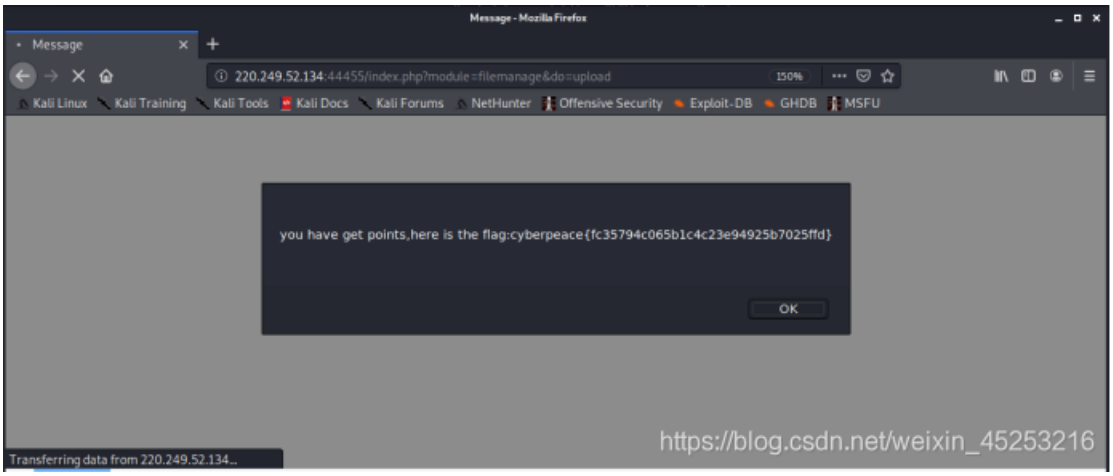




非常非常非常熟悉的一个界面，估计就是传个一句话木马，然后查看网页文件目录结构就能找到flag。
提示Just image？应该是前端做了过滤，所以写完一句话后把文件改为jpg格式，然后bp抓包再改回来。

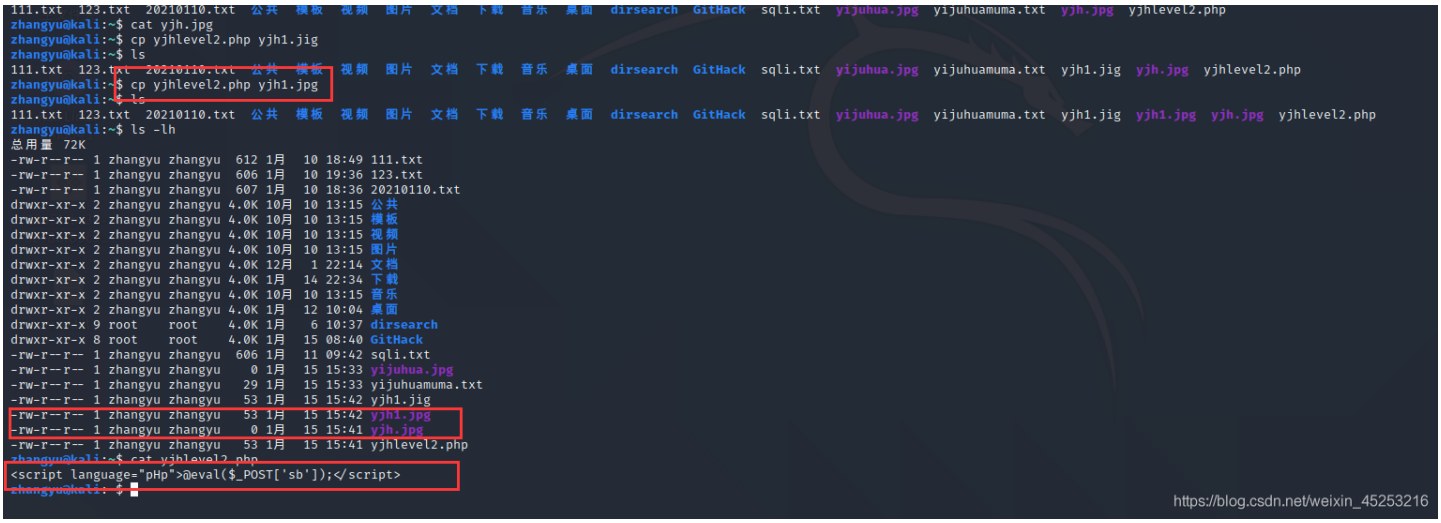


emm想复杂了，直接传完一句话，flag就被alert了。



具体有一个细节就是，一句话的写法，还有文件格式要写.php4或者是.php5，否则页面会提示你上传的是一个php文件。

```
zhangyu@kali:~$ ls
111.txt  123.txt  20210110.txt  公共  模板  视频  图片  文档  下载  音乐  桌面  dirsearch  GitHack  sqli.txt
zhangyu@kali:~$ touch yijuhuamuma.txt
zhangyu@kali:~$ ls
111.txt  123.txt  20210110.txt  公共  模板  视频  图片  文档  下载  音乐  桌面  dirsearch  GitHack  sqli.txt  yijuhuamuma.txt
zhangyu@kali:~$ vim yijuhuamuma.txt
zhangyu@kali:~$ cat yijuhuamuma.txt
<?php @eval($_POST['sb']);?>
zhangyu@kali:~$ touch yijuhuamuma.txt yijuhua.jpg
zhangyu@kali:~$ vim yijuhuamuma.txt
zhangyu@kali:~$ touch yjhlevel2.php
zhangyu@kali:~$ vim yjhlevel2.php
zhangyu@kali:~$ ls
111.txt  123.txt  20210110.txt  公共  模板  视频  图片  文档  下载  音乐  桌面  dirsearch  GitHack  sqli.txt  yijuhua.jpg  yijuhuamuma.txt  yjhlevel2.php
zhangyu@kali:~$ touch yjhlevel2.php yjh.jpg
zhangyu@kali:~$ ls
```



常规写法会被检测到是php文件，这里采用第二种写法yjhlevel2.php。将文件以不同格式保存要用cp命令，如果像我之前憨憨的用touch，肯定是不行的，大家看到touch后的文件时0KB也就是新建了一个空文件，并不是文件以另外格式保存的操作。

有一个疑问，为什么文件后缀名，.php4或者.php5就可以，但是.php就不行？