# XCTF web bug

原创

H4ppyD0g 于 2019-09-06 22:12:26 发布 242 收藏


注册后登陆，发现有manage，点击一下，说不是管理员，没有权限，那就得想办法获得管理员权限

退出，回到登录界面，点击Findpwd

输入信息后第二步就可以直接修改密码了。这个时候用burpsuite抓包，把user改成admin就可以把admin改成想要的密码。

登录admin，再点击manage，ip不允许，修改XFF头为127.0.0.1可以访问。

在网页源代码中发现传参，把do设为upload，可以上传文件

用`<script language="php"> ... php code... </script>`内容，jpg后缀名在本地绕过，bp改后缀名为php5即可看到flag

---

自己的理解是文件上传成功后，就会出现相应的反应，而这个题最后考的是文件绕过上传，所以相应的反应就是给出flag。

再一个就是为什么直接上传.php就不行，而在bp改包就可以，可能是因为上传时会先在本地进行检测，如果没有问题才会提交给浏览器。所以一开始是jpg格式文件在本地检测没有问题，会发送给服务器，在发送之前并且本地检测之后用bp改包就可以实现绕过了。嗯，应该是这个样子。