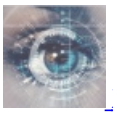
XCTF WEB backup

原创

YenKoc 于 2019-12-03 22:54:16 发布 93 收藏

分类专栏： XCTF 文章标签： XCTF

本文链接：https://blog.csdn.net/YenKoc/article/details/103378105



不用多说，肯定是扫描后台，目录看看能不能找到备份文件，（可恶我的御剑的字典太菜了，居然爆破不出来），建议大家装御剑高一些的版本，或者用**dirsearch**来扫描，都是不错的。

这里插个知识点，备份文件常见的后缀名：**.git .svn .swp .svn .~ .bak .bash_history**

0x01:

开始启动**dirsearch.py**脚本，开始扫描
dirsearch的语法为:**python dirsearch.py -u url -e* (-e**是表示扫描哪种类型的文件)

```
ython dirsearch.py -u http://111.198.29.45:55067/ -e*
```

```
[22:44:18] 403 -  293B  - /.htpasswds
[22:44:18] 403 -  291B  - /.htusers
[22:44:31] 200 -  438B  - /index.php
[22:44:31] 200 -  500B  - /index.php.bak
[22:44:31] 200 -  438B  - /index.php/login/
[22:44:37] 403 -  296B  - /server-status
[22:44:37] 403 -  297B  - /server-status/
```

它来了，我们想要的备份文件。**url**输入**index.php.bak**，会自动下载备份文件，里面有**flag**。

总结：后台扫描工具使用得当