

BUUCTF 后门查杀 writeup

原创

碧羽o(*▽*)づ回雪  已于 2022-03-19 22:09:18 修改  199  收藏 2

分类专栏: [CTF writeup](#) 文章标签: [python](#)

于 2021-10-11 19:50:09 首次发布

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/zhangzhaolin12/article/details/120710263>

版权



[CTF writeup](#) 专栏收录该内容

16 篇文章 0 订阅

订阅专栏

后门查杀

1

小白的网站被小黑攻击了，并且上传了Webshell，你能帮小白找到这个后门么？(Webshell中的密码(md5)即为答案)。注意：得到的 flag 请包上 flag{} 提交

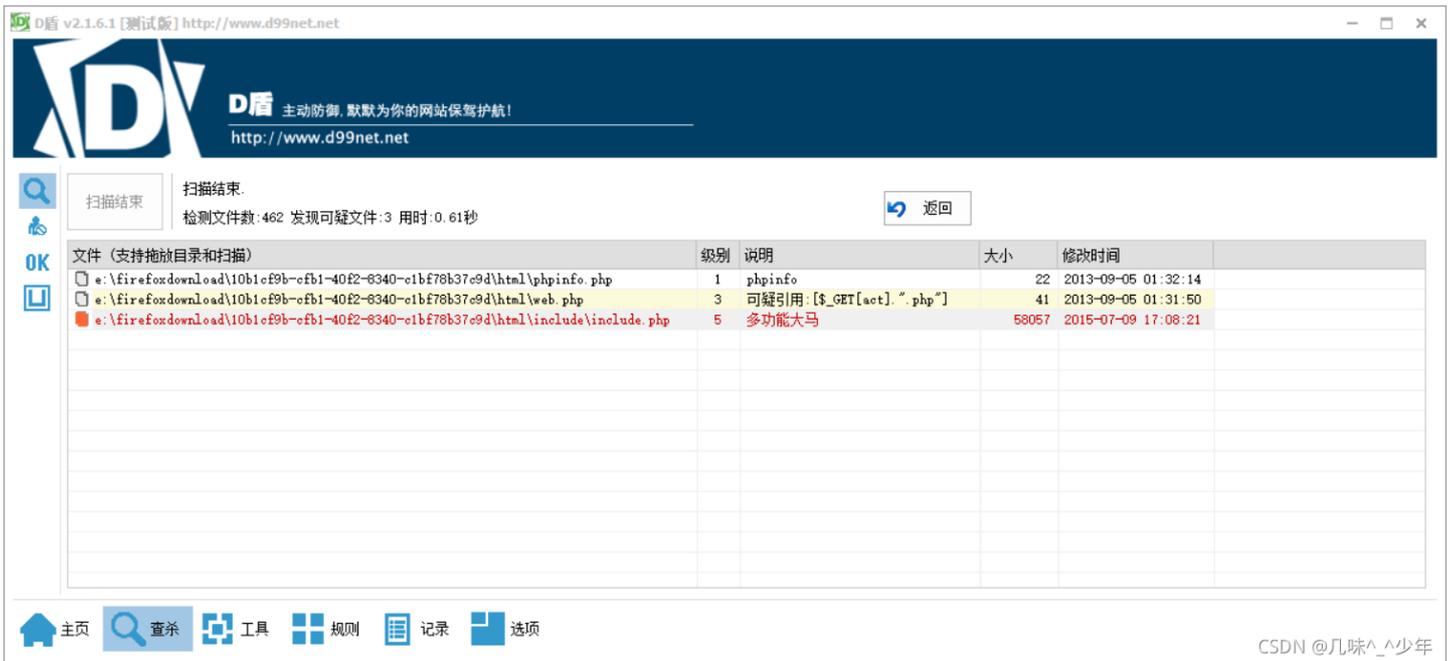
10b1cf9b-cf...

Flag

提交

CSDN @几味^少年

这里题目中说了，flag是密码，那就可以挨个找password这个关键字，但是真正的flag不是password，而是pass有一点点坑。使用D盾进行扫描文件夹，就可以找出网站的后门。



D盾 v2.1.6.1 [测试版] http://www.d99net.net

主动防御，默默为你的网站保驾护航！
http://www.d99net.net

扫描结束
检测文件数:462 发现可疑文件:3 用时:0.61秒

返回

文件 (支持拖放目录和扫描)	级别	说明	大小	修改时间
e:\firefoxdownload\10b1cf9b-cfb1-40f2-6340-c1bf78b37e9d\html\phpinfo.php	1	phpinfo	22	2013-09-05 01:32:14
e:\firefoxdownload\10b1cf9b-cfb1-40f2-6340-c1bf78b37e9d\html\web.php	3	可疑引用: [\$_GET[act]. ".php"]	41	2013-09-05 01:31:50
e:\firefoxdownload\10b1cf9b-cfb1-40f2-6340-c1bf78b37e9d\html\include\include.php	5	多功能大马	58057	2015-07-09 17:08:21

主页 查杀 工具 规则 记录 选项

CSDN @几味^少年

flag就在级别最高的那个文件里，这里有路径，找到这个文件，就可以得到flag。