

# buuctf 后门查杀

原创

x-x123 于 2021-09-27 23:22:33 发布 1402 收藏 1

分类专栏: [ctf buuctf](#) 文章标签: [web安全](#)

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/EasonCc/article/details/120519697>

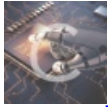
版权



ctf 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏



buuctf

2 篇文章 0 订阅

订阅专栏

题目 [解题快手榜](#) ×

## 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

CSDN @x-x123

## 1. 下载得到源码文件夹

名称	修改日期	类型	大小
admin	2015/7/9 17:05	文件夹	
cache	2015/7/9 17:05	文件夹	
data	2015/7/9 17:05	文件夹	
images	2015/7/9 17:05	文件夹	
include	2015/7/9 17:07	文件夹	
install	2015/7/9 17:05	文件夹	
languages	2015/7/9 17:05	文件夹	
theme	2015/7/9 17:05	文件夹	
upload	2021/9/13 9:23	文件夹	
.htaccess	2013/9/4 21:15	HTACCESS 文件	2 KB
article.php	2013/9/5 4:48	PHP 文件	2 KB

article_category.php	2013/9/1 6:16	PHP 文件	3 KB
attacktest.sql	2013/9/5 6:49	SQL 文件	121 KB
captcha.php	2013/8/29 2:26	PHP 文件	2 KB
download.php	2013/9/5 3:31	PHP 文件	1 KB
error.php	2013/9/5 4:58	PHP 文件	1 KB
favicon.ico	2013/8/31 0:23	图标	2 KB
index.php	2013/9/1 6:23	PHP 文件	3 KB
page.php	2013/9/1 6:12	PHP 文件	2 KB
phpinfo.php	2013/9/5 1:32	PHP 文件	1 KB
product.php	2013/9/1 6:12	PHP 文件	2 KB
product_category.php	2013/9/1 6:16	PHP 文件	3 KB
robots.txt	2013/8/24 8:50	文本文档	1 KB
sitemap.php	2013/6/30 10:39	PHP 文件	5 KB
web.php	2013/9/5 1:31	PHP 文件	1 KB

CSDN @x-x123

## 2. 直接使用D盾查杀后门



CSDN @x-x123

扫描位置	C:\Users\Ghost\Downloads\html					开始扫描
检测类型	全部文件	<input checked="" type="checkbox"/> 列出隐藏脚本	<input type="checkbox"/> 不显示低级别脚本(1级)	<input type="checkbox"/> 显示Zend加密	目录排除	选择目录...
文件	级别	说明	大小	修改时间	验证值	
<input type="checkbox"/> C:\Users\Ghost\Downloads\html\phpinfo.php	1	关键字: phpinfo()	22	2013-09-05 01:32:14	2EABF016	
<input type="checkbox"/> C:\Users\Ghost\Downloads\html\web.php	3	可疑引用: [\$_GET[act].".php"]	41	2013-09-05 01:31:50	7CAABF1E	
<input checked="" type="checkbox"/> C:\Users\Ghost\Downloads\html\include\include.php	5	多功能大马	58057	2015-07-09 17:08:21	AA216E4D	
<input type="checkbox"/> C:\Users\Ghost\Downloads\html\install\index.php	1	fwrite 参数: {\$file_config.. "\$p...	7043	2013-08-30 05:17:44	1938BD3A	

### 3.打开红色标注文件查找相关代码

```
25 unset($_POST);
26 /*===== 程序配置 =====*/
27
28 //echo encode_pass('angel');exit;
29 // 如果需要密码验证,请修改登陆密码,留空为不需要验证
30 $pass = '6ac45fb83b3bc355c024f5034b947dd3'; //angel
31
32 //如您对 cookie 作用范围有特殊要求,或登录不正常,请修改下面变量,
  否则请保持默认
33 // cookie 前缀
34 $cookiepre = '';
35 // cookie 作用域
```

CSDN @x-x123

如题所示pass后的MD5加上flag{}即为flag:

flag{6ac45fb83b3bc355c024f5034b947dd3}