

BUUCTF 后门查杀

原创

仲璧 于 2022-01-20 19:12:50 发布 3454 收藏 1

分类专栏: [CTF](#) 文章标签: [蓝桥杯](#) [职场和发展](#)

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/m0_49025459/article/details/122608121

版权



[CTF 专栏收录该内容](#)

47 篇文章 1 订阅

订阅专栏

题目

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吗? (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 @ 壬二舟

解压文件, 然后将解压后的文件用D盾打开扫描后门

D盾 v2.1.6.2 [测试版] http://www.d99net.net

ADV 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 扫描结束
检测文件数:462 发现可疑文件:6 用时:0.70秒

文件 (支持拖放目录和扫描)	级别	说明	大小	修改时间
c:\users\lenovo\desktop\ctf\后门查杀\html\d...	3	文件下载	147	2013-09-05 03:31:58
c:\users\lenovo\desktop\ctf\后门查杀\html\p...	1	phpinfo	22	2013-09-05 01:32:14
c:\users\lenovo\desktop\ctf\后门查杀\html\w...	3	可疑引用:["\$_GET[act].".php"]	41	2013-09-05 01:31:50
c:\users\lenovo\desktop\ctf\后门查杀\html\i...	5	已知后门	58057	2015-07-09 17:08:21
c:\users\lenovo\desktop\ctf\后门查杀\html\i...	1	[define] SITE_URL=>\$_SERVER[...]	2732	2013-08-29 02:26:46
c:\users\lenovo\desktop\ctf\后门查杀\html\i...	1	fwrite 参数:{\$file_config"/...}	7043	2013-08-30 05:17:44

主页 查杀 工具 规则 记录 选项

CSDN @ 壬二舟

邮件红色的 查看文件

```
include.php - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
define('IS_PHPINFO', (preg_match("/phpinfo/", $dis_func)) ? 1 : 0);

if (IS_GPC) {
    $_POST = s_array($_POST);
}
$P = $_POST;
unset($_POST);
/*===== 程序配置 =====*/

//echo encode_pass('angel');exit;
// 如果需要密码验证,请修改登陆密码,留空为不需要验证
$pass = '6ac45fb83b3bc355c024f5034b947dd3'; //angel

//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
// cookie 前缀
$cookiepre = "";
// cookie 作用域
$cookiedomain = "";
// cookie 作用路径
$cookiepath = '/';
// cookie 有效期
$cookielife = 86400;
```

第 1 行, 第 1 列 100% Windows (CRLF) ANSI @ 壬二舟

就能看见flag了

```
flag{6ac45fb83b3bc355c024f5034b947dd3}
```



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)