

BUUCTF webshell后门

原创

仲璧 于 2022-04-17 21:27:19 发布 18 收藏 1

分类专栏: [CTF](#) 文章标签: [CTF](#)

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/124236928

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

×

webshell后门

1

朋友的网站被黑客上传了webshell后门, 他把网站打包备份了, 你能帮忙找到黑客的webshell在哪吗? (Webshell中的密码(md5)即为答案)。注意: 得到的 flag 请包上 flag{} 提交

827baa91-b...

Flag

提交

CSDN @仲璧

下载附件然后去D盾里扫一下

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:3002 发现可疑文件:5 用时:3.53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\827baa91-be16-43a4-...	2	干扰代码或注释过多	55926	2015-03-04 11:29:10
c:\users\lenovo\desktop\827baa91-be16-43a4-...	5	已知后门	58101	2015-08-24 16:06:52
c:\users\lenovo\desktop\827baa91-be16-43a4-...	5	已知后门	10285	2011-09-06 10:07:26
c:\users\lenovo\desktop\827baa91-be16-43a4-...	4	(内藏)Eval后门 {参数:\$_POST[...}	163948	2015-08-26 17:06:17
c:\users\lenovo\desktop\827baa91-be16-43a4-...	1	可疑echo	495	2012-04-19 15:42:32

主页 查杀 工具 规则 记录 选项

CSDN @仲璧

打开这些存在后门的文件看看

```

zp.php - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
define('IS_WIN', DIRECTORY_SEPARATOR == '\\');
define('IS_GPC', get_magic_quotes_gpc());
$dis_func = get_cfg_var('disable_functions');
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;
//angel = ba8e6c6f35a53933b871480bb9a9545c
// 如果需要密码验证,请修改登陆密码,留空为不需要验证
$pass = 'ba8e6c6f35a53933b871480bb9a9545c'; //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
$cooki_domain = "";
// cookie 作用路径

```

第 33 行, 第 49 列 100% Windows (CRLF) ANS

`$pass = 'ba8e6c6f35a53933b871480bb9a9545c'; //angel`

直接加上flag{}提交