

# Buuctf webshell后门

原创

Dexret 于 2021-11-19 00:35:20 发布 301 收藏

分类专栏: [Buuctf Misc](#) 文章标签: [安全 php](#)

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/Dexret/article/details/121411647>

版权



[Buuctf Misc](#) 专栏收录该内容

47 篇文章 0 订阅

订阅专栏

下载该文件, 发现该文件为一整个网站的源码

结合题意, 该题需要我们找到该文件的webshell文件, 且flag值为md5值

直接使用D盾扫描该网页源码

文件 (支持拖放目录和扫描)	级别	说明	大小	修改时间
c:\users\13631\desktop\html\do\qq_login.php	1	[可疑]file_get_contents 参数...	5159	2013-04-15 09:55:51
c:\users\13631\desktop\html\member\zp.php	5	多功能大马	58101	2015-08-24 16:06:52
c:\users\13631\desktop\html\hack\upgrade\ad...	5	已知后门	10285	2011-09-06 10:07:26
c:\users\13631\desktop\html\upload_files\ar...	4	(内藏)Eval后门 {参数:\$_POST[...}	163948	2015-08-26 17:06:17

发现有多功能大马, 和一个已知后门, 打开文件所在位置, 用notepad++打开该网页源码

```
C:\Users\13631\Desktop\html\member\zp.php - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
xp.php
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 $dis_func = get_cfg_var('disable_functions');
19 define('IS_PHPINFO', (!ereg("phpinfo",$dis_func)) ? 1 : 0);
20
21 if( IS_GPC ) {
22     $_POST = s_array($_POST);
23 }
24 $_P = $_POST;
25 unset($_POST);
26 /*===== 程序配置 =====*/
27
28 //echo encode_pass('angel');exit;
29 //angel = ba8e6c6f35a53933b871480bb9a9545c
30 // 如果需要密码验证,请修改登陆密码,留空为不需要验证
31 $pass = 'ba8e6c6f35a53933b871480bb9a9545c'; //angel
32
33 //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
34 // cookie 前缀
35 $cookiepre = '';
36 // cookie 作用域
37 $cookiedomain = '';
38 // cookie 作用路径
39 $cookiepath = '/';
PHP Hypertext Preprocessor file length: 58,351 lines: 1,616 Ln: 31 Col: 43 Sel: 32 | 1 Windows (CR LF) GB2312 (Simplified) CHS
```

发现一段md5的值，判断该值为该题的flag值，尝试后发现能够提交

所以该题的flag为

```
flag{ba8e6c6f35a53933b871480bb9a9545c}
```