

BUUCTF——后门查杀1

原创

山东网安菜鸡  已于 2022-04-03 10:11:28 修改  135  收藏

分类专栏: [CTF](#) 文章标签: [CTF misc 杂项题 BUUCTF](#)

于 2022-04-03 09:03:21 首次发布

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/YZ913/article/details/123932530>

版权



[CTF 专栏收录该内容](#)

7 篇文章 0 订阅

订阅专栏

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

CSDN @山东网安菜鸡

题文件:

链接: <https://pan.baidu.com/s/1dLcG4Uflo6wn9DCJqganNw?pwd=m9v8>

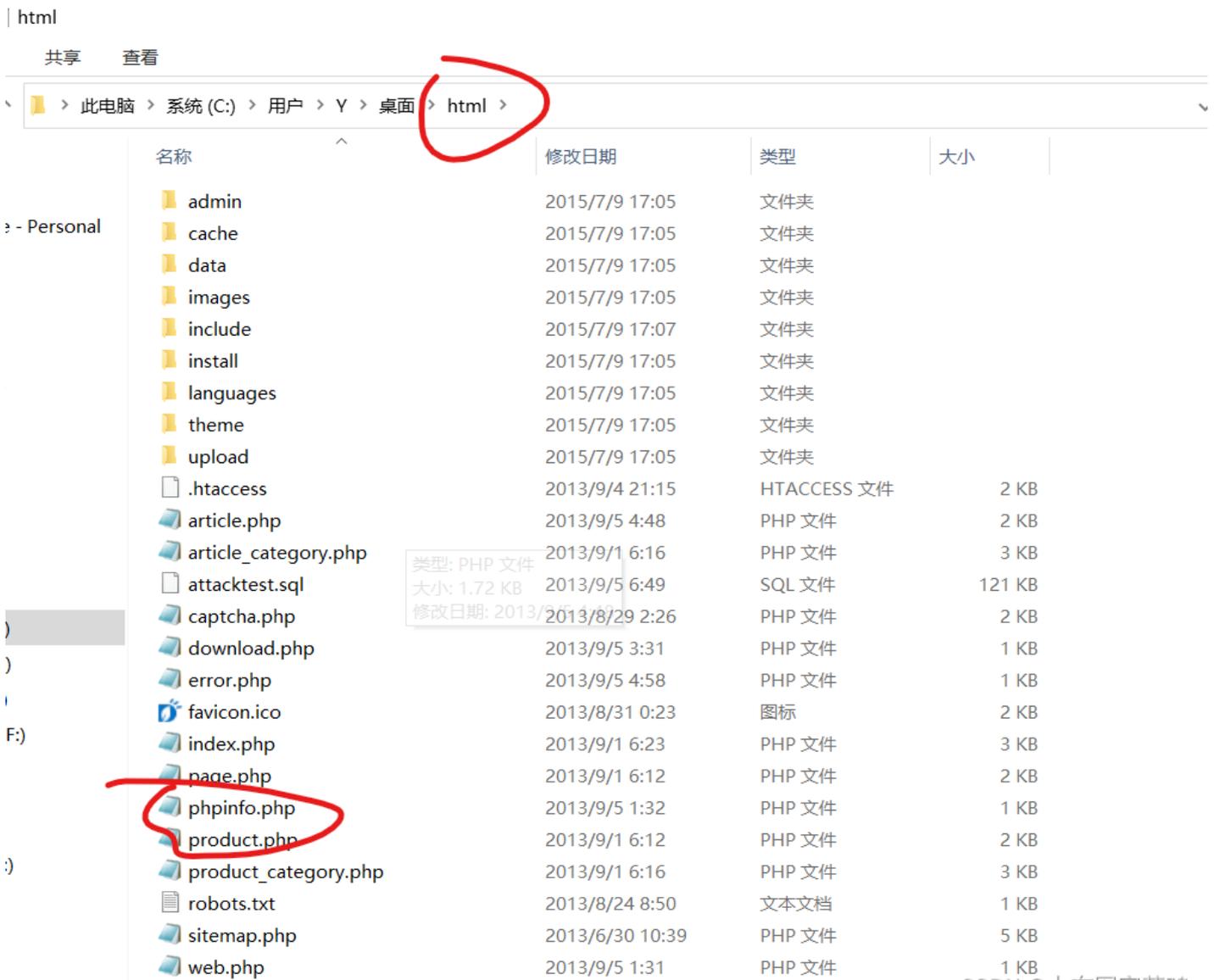
提取码: m9v8

--来自百度网盘超级会员V1的分享

[BUUCTF——webshell后门1_山东网安菜鸡的博客-CSDN博客h](#)

后门查杀和webshell后门1这两道题差不多一样

下载文件查看是一个html的文件夹



CSDN @山东网安菜鸡

根据题目以及一些文件来看，猜测可能是php语言

存在一句话木马、php危险函数？

用火绒等一些安全软件扫描文件夹，扫描有无危险文件



CSDN @山东网安菜鸡

发现有危险文件，打开查看一下内容

```
include.php - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
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,
// 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;

/*===== 配置结束 =====*/
```

发现有一个md5的加密文件

md5是由0~9和a~f之内的数字以及字母组成

提交试试,发现成功

This is flag:

flag{6ac45fb83b3bc355c024f5034b947dd3}