

Buuctf 后门查杀

原创

Dexret 于 2021-11-18 20:56:43 发布 93 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/121409957>

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, 发现该文件为一个网站的源码, 结合题意让我们找出该网站的webshell

既然是找webshell, 那么直接用查杀软件D盾来扫描该网站源码

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\phpinfo.php	1	phpinfo	22	2013-09-05 01:32:14
c:\users\13631\desktop\html\web.php	3	可疑引用:[\$_GET[act].".php"]	41	2013-09-05 01:31:50
c:\users\13631\desktop\html\include\include...	5	多功能大马	58057	2015-07-09 17:08:21

成功找到一个多功能大马, 可以判断该木马为webshell

打开该目录下的网页源码include.php

名称	修改日期	类型	大小
smarty	2015/7/9 17:05	文件夹	
action.class.php	2013/9/1 6:15	PHP 文件	13 KB
download.class.php	2013/9/5 4:06	PHP 文件	2 KB
include.php	2015/7/9 17:08	PHP 文件	57 KB
init.php	2013/8/29 2:26	PHP 文件	3 KB
mysql.class.php	2013/9/5 4:49	PHP 文件	5 KB
upload.class.php	2013/9/5 0:51	PHP 文件	6 KB
upload.class.php.1	2013/9/5 0:28	1 文件	6 KB

总计 56.6 KB

CSDN @Dexret

对源码进行代码审计

```

$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 =====*/

Scharsetdb = array(

```

CSDN @Dexret

发现一段md5，结合题意说flag为md5

可以判断该题的flag为：

```
flag{6ac45fb83b3bc355c024f5034b947dd3}
```