

Pluck CMS 4.7.10 后台 文件包含+文件上传导致getshell代码分析

p014rB / 2019-10-18 09:32:05 / 浏览数 8210

0x01 漏洞描述

影响版本: Pluck CMS Pluck CMS <=4.7.10

官网地址: <http://www.pluck-cms.org/?file=home>

源码下载:<https://github.com/pluck-cms/pluck/releases>

0x02 漏洞分析

目前最新版本为4.7.10, 个人测试github上最旧的4.7.2版本仍然存在该漏洞, 框架本身语言选择模块数据注入导致的文件包含漏洞, 官方更新版本并没有对这部分代码进行修改, 可以认为是全版本通用的。该漏洞是在复现"我怎么这么帅"在先知发表的《Pluck CMS 4.7.10远程代码执行漏洞分析》之余审计其他代码发现的, 在此致谢。

v4.7.1分析

从入口文件admin.php查看:

```
145
146
147 //Page:Options:Language
148 case 'language':
149     $titelkop = $lang['language']['title'];
150     include_once ('data/inc/header.php');
151     include_once ('data/inc/language.php');
152     break;
```

查看language.php,满足指定的文件存在, 并传入的cont1参数和原本设置的\$langpref参数不等, 进入save_language(\$cont1)。

```
//Check if chosen language is valid, and then save data.
if (isset($_POST['save'], $cont1) && $cont1 != '0' && file_exists( filename: 'data/inc/lang/'.$cont1) && $cont1 != $langpref) {
    save_language($cont1);

    //Redirect user.
    show_error($lang['language']['saved'], level: 3);
    redirect( url: '?action=options', time: 2);
    include_once ('data/inc/footer.php');
    exit;
}
```

调用save_file方法。

```
function save_language($language) {
    save_file( file: 'data/settings/langpref.php', array('langpref' => $language), chmod: FALSE);
}
```

由于只有一个数据, 直接182写入php文件。

```

167 function save_file($file, $content, $chmod = 0777) {
168     $data = fopen($file, mode: 'w');
169
170     //If it's an array, we have to create the structure.
171     if (is_array($content) && !empty($content)) {
172         $final_content = '<?php'."\n";
173         foreach ($content as $var => $value) {
174             $final_content .= '$'.$var.' = \''.$value.'\';'."\n";
175         }
176         $final_content .= '??';
177
178         fputs($data, $final_content);
179     }
180
181     else
182         fputs($data, $content);
183
184     fclose($data);
185     if ($chmod != FALSE)
186         chmod($file, $chmod);
187 }

```



至此，langpref的值变成可控值，这个值对应的文件，用于控制网站的语言选择，会自动被全局php文件包含。可以包含上传功能点上传的图种文件解析其中的一句话导致getshell。文件上传功能点使用白名单，但是没有进行重命名，所以路径可以简单猜解。

```

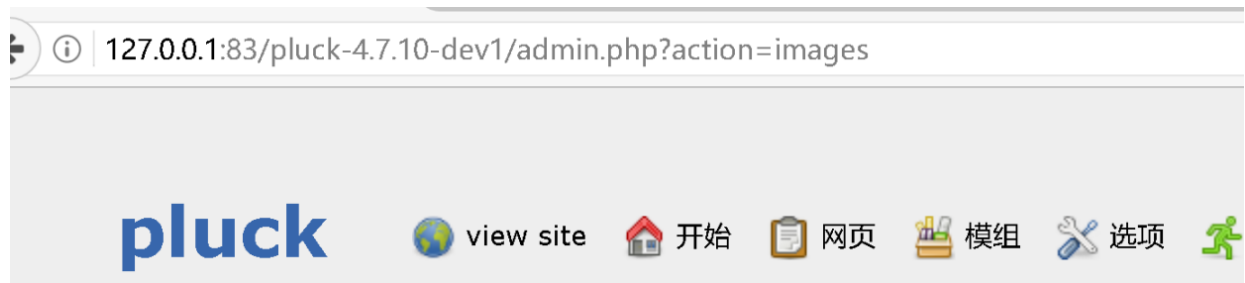
<?php
$langpref = '../ ../ ../images/wphp.jpg';
?>

```




0x03 漏洞复现

文件上传一个可以写一句话木马的php图种。

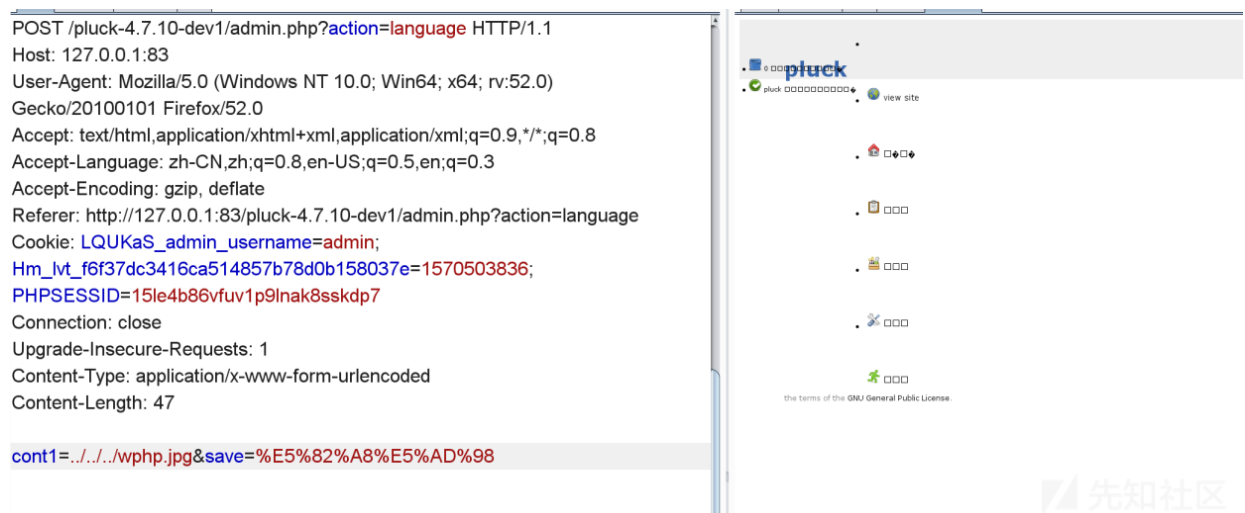


管理图片

这里你可以上载你的图片，以供日后加入网页中。图片支援 JPG, PNG 和 GIF



已上载的图片



上述参数保存于php文件:

\data\settings\langpref.php



由于该参数是网站语言控制的php文件，访问任意网页，包含langpref对应的文件。



p0l4rB

2019-11-01 09:49:02

@adda**** 之前有事，今天才看到非常抱歉。我测试了4.7.3，也是可以写入。如果是无法写入的话，猜测可能的问题是这个参数写入的条件是写入文件必须在是存在的（这个在上文中提到），我测试的数据包的那个图种是放在根目录下的。你可以检测一下你的/images/wphp.jpg文件是否存在，并将值改为../../images/wphp.jpg。

👍 0 回复Ta

登录 后跟帖