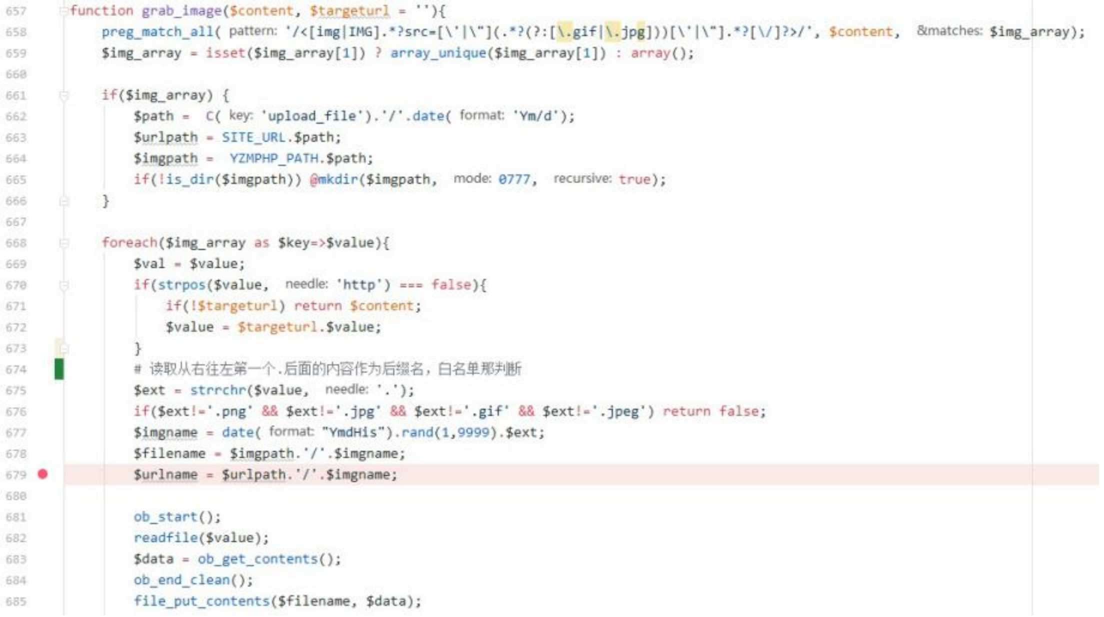
New issue Jump to bottom

A SSRF in yzmcms v5.5 management #44

Closed **mntn0x** opened this issue on Mar 27, 2020 · 1 comment

mntn0x commented on Mar 27, 2020

后台编辑文章处，最下方选项 将远程文件保存到本地 ，漏洞代码在yzmphp/core/function/global.func.php#grab_image()



```
function grab_image($content, $targeturl = ''){
    preg_match_all( pattern: '/<[img|IMG].*?src=[\'|\"](.*?(?:[\.gif|\.jpg]))[\'|\"].*?[\/]?>/', $content,  &matches: $img_array);
    $img_array = isset($img_array[1]) ? array_unique($img_array[1]) : array();

    if($img_array) {
        $path =  C( key: 'upload_file').'/'.date( format: 'Ym/d');
        $urlpath = SITE_URL.$path;
        $imgpath =  YZMPHP_PATH.$path;
        if(!is_dir($imgpath)) @mkdir($imgpath,  mode: 0777,  recursive: true);
    }

    foreach($img_array as $key=>$value){
        $val = $value;
        if(strpos($value,  needle: 'http') === false){
            if(!$targeturl) return $content;
            $value = $targeturl.$value;
        }
        # 读取从右往左第一个.后面的内容作为后缀名，白名单那判断
        $ext = strrchr($value,  needle: '.');
        if($ext!='.png' && $ext!='.jpg' && $ext!='.gif' && $ext!='.jpeg') return false;
        $imgname = date( format: "YmdHis").rand(1,9999).$ext;
        $filename = $imgpath.'/'.$imgname;
        $urlname = $urlpath.'/'.$imgname;

        ob_start();
        readfile($value);
        $data = ob_get_contents();
        ob_end_clean();
        file_put_contents($filename, $data);
```

当修改文章或者添加文章时选择了将远程文件加载到本地，则会进入grab_image函数，正则匹配文章内容中的img标签，提取出链接保存在$val=$value，然后通过 `strpos` 判断链接中是否有http，如果没有则直接返回（说明这不是外网图片链接）。
接着从右往左读取第一个点号作为分割，得到后缀名，然后白名单校验后缀，此处的后缀名可以通过 `1.php?2.jpg` 来绕过。接着出现漏洞点

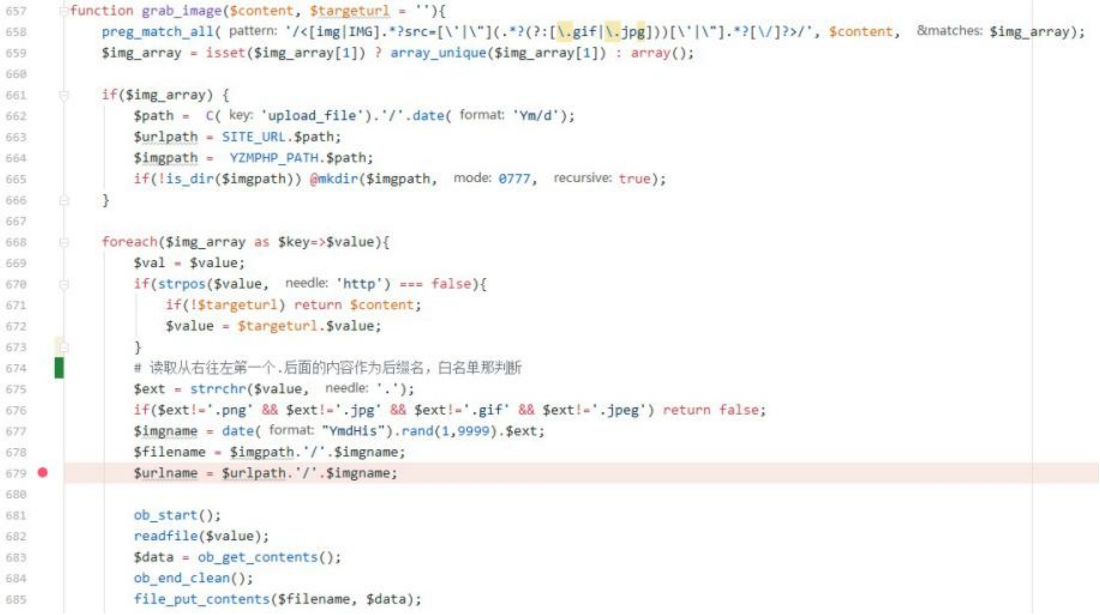
```
ob_start();
readfile($value);
$data = ob_get_contents();
ob_end_clean();
file_put_contents($filename, $data);
```

`readfile` 读取文件内容，然后保存到jpg文件。如果 `readfile` 读取文件有warning或者error，就会跳转到错误处理函数。
payload：

```
<img src="http://127.0.0.1:80/2.jpg" width="100" height="100"/>
```

可通过此处探测内网端口及ip。
同时，此处也是一个文件读取漏洞，只是读取php文件有可能会报错，尝试读取config.php，因为YZMPHP_PATH变量没有声明而报错。

Edit the background, the bottom option 将远程文件保存到本地 , Vulnerable code:



```
function grab_image($content, $targeturl = ''){
    preg_match_all( pattern: '/<[img|IMG].*?src=[\'|\"](.*?(?:[\.gif|\.jpg]))[\'|\"].*?[\/]?>/', $content,  &matches: $img_array);
    $img_array = isset($img_array[1]) ? array_unique($img_array[1]) : array();

    if($img_array) {
        $path =  C( key: 'upload_file').'/'.date( format: 'Ym/d');
        $urlpath = SITE_URL.$path;
        $imgpath =  YZMPHP_PATH.$path;
        if(!is_dir($imgpath)) @mkdir($imgpath,  mode: 0777,  recursive: true);
    }

    foreach($img_array as $key=>$value){
        $val = $value;
        if(strpos($value,  needle: 'http') === false){
            if(!$targeturl) return $content;
            $value = $targeturl.$value;
        }
        # 读取从右往左第一个.后面的内容作为后缀名，白名单那判断
        $ext = strrchr($value,  needle: '.');
        if($ext!='.png' && $ext!='.jpg' && $ext!='.gif' && $ext!='.jpeg') return false;
        $imgname = date( format: "YmdHis").rand(1,9999).$ext;
        $filename = $imgpath.'/'.$imgname;
        $urlname = $urlpath.'/'.$imgname;

        ob_start();
        readfile($value);
        $data = ob_get_contents();
        ob_end_clean();
        file_put_contents($filename, $data);
```

When modifying an article or adding an article, you chose to load a remote file locally,It will enter the functiongrab_image() , which matches the img tag in the article content, extracts the link and saves it in $ val = $ value, and then uses `strpos` to determine whether there is http in the link. If not, it returns directly (indicating that this is not an external network image link).
Then read the first dot from right to left as the segmentation to get the suffix name, and then check the suffix on the white list. The suffix name here can be bypassed by `1.php? 2.jpg` . Then there are vulnerabilities

```
ob_start();
readfile($value);
$data = ob_get_contents();
ob_end_clean();
file_put_contents($filename, $data);
```

`readfile` reads the file content and saves it to a jpg file. If `readfile` reads a file with warning or error, it will jump to the error handling function.
payload:

```
<img src="http://127.0.0.1:80/2.jpg" width="100" height="100"/>
```

You can probe the intranet port and ip here.
At the same time, here is also a file reading vulnerability, but reading php files may report an error. Try reading config.php because the YZMPHP_PATH variable is not declared and an error is reported.

yzmcms commented on Mar 28, 2020 Owner

已收到反馈，下一个版本修复

mntn0x closed this as completed on Mar 29, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants