Finding GTN-003: HTTP Response splitting through 'format' parameter

Severity: High
Vendor of the product: MDaemon Technologies
Product: SecurityGateway for Email Servers
Version: v8.5.2 (64 bit)
Researcher: Pankaj Kumar Thakur (Green Tick Nepal Pvt. Ltd.)

Details of Vulnerability:

HTTP Response Splitting occurs when a web server fails to sanitize CR and LF characters before the data is included in outgoing HTTP headers.

To launch a successful exploit, the application must be vulnerable to the injection of Carriage Return (CR, ASCII 13, \r) and Line Feed (LF, ASCII 10, \n) characters, which are used in the HTTP protocol to terminate a line, into the response header. This technique is also referred to as "CRLF Injection in HTTP Headers", and it gives attackers control of the remaining headers and body of the response that the application will send.

Impact:

The vulnerability allows the attacker to set arbitrary headers, take control of the body, or break the response into two or more separate responses. Impacts depend on the technological stack, with outcomes including Cross-Site Scripting, Cookie Injection, CORS Headers Injection, CSP Bypass, Cache Poisoning attacks, and many others.

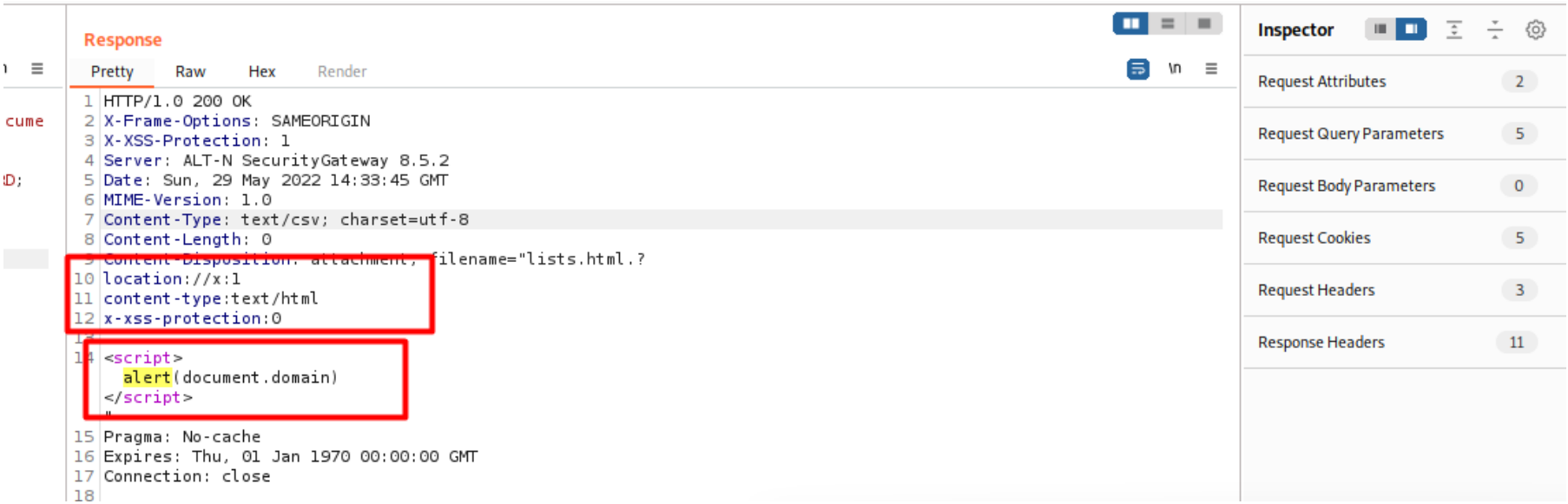
Evidence:

```
MIME-Version: 1.0
Content-Type: text/csv; charset=utf-8
Content-Length: 0
Content-Disposition: attachment; filename="lists.csv
set-cookie: mycookie=hacked"
Pragma: No-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Connection: close
```

Trying to chain with XSS vulnerability, XSS was unable to execute because file was downloading

Payload

/SecurityGateway.dll?view=download&data=lists.html&format=%3f%0D%0ALocation://x:1%0D%0AContent-Type:text/html%0D%0AX-XSS-Protection%3a0%0D%0A%0D%0A%3Cscript%3Ealert(document.domain)%3C/script%3E&blacklist=1&user=1



Suggested Remediation:

- As with other similar injection attacks, HTTP Response Splitting can be mitigated by performing appropriate server-side validation and escaping. The canonical ways are the following:
- Carefully validate and sanitize any user-provided content that might be used to compose response headers.
- Encode dangerous characters such as \r and \n.