Finding GTN-006: Stored Cross Site Scripting (XSS) at ‘data_leak_list_ajax’ endpoint

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:

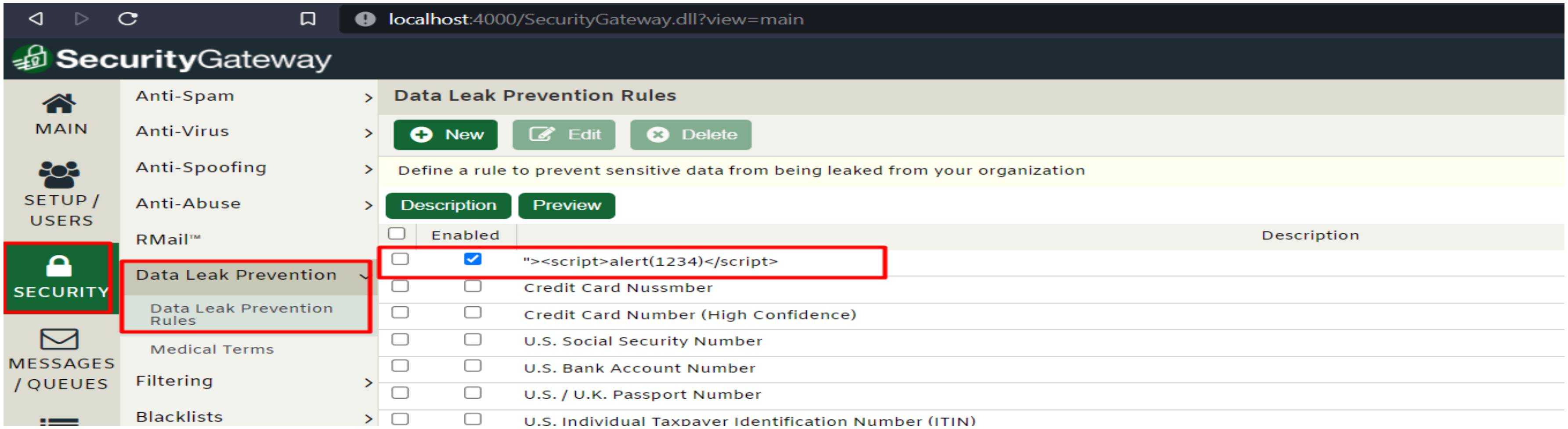
The payload ‘”><script>alert(123)</script>’ was submitted with GET Request. The HTTP response appears to contain the output from the injected payload, indicating that the payload was executed successfully on the server.

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:

Inject XSS payload while creating rule



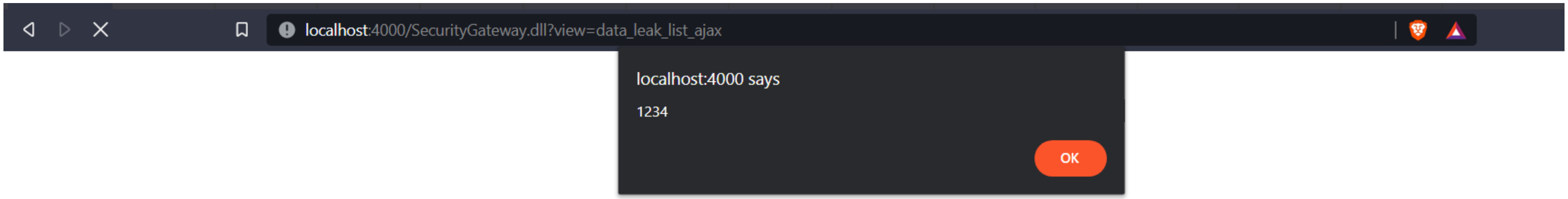
Data Leak Prevention Rules

Define a rule to prevent sensitive data from being leaked from your organization

□	Enabled	Description
□	☑	"><script>alert(1234)</script>
□	□	Credit Card Nussmber
□	□	Credit Card Number (High Confidence)
□	□	U.S. Social Security Number
□	□	U.S. Bank Account Number
□	□	U.S. / U.K. Passport Number
□	□	U.S. Individual Taxpayer Identification Number (ITIN)

Now visit

http://localhost:4000/SecurityGateway.dll?view=data_leak_list_ajax



localhost:4000 says

1234

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.