

Finding GTN-002: Stored Cross Site Scripting (XSS)

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:

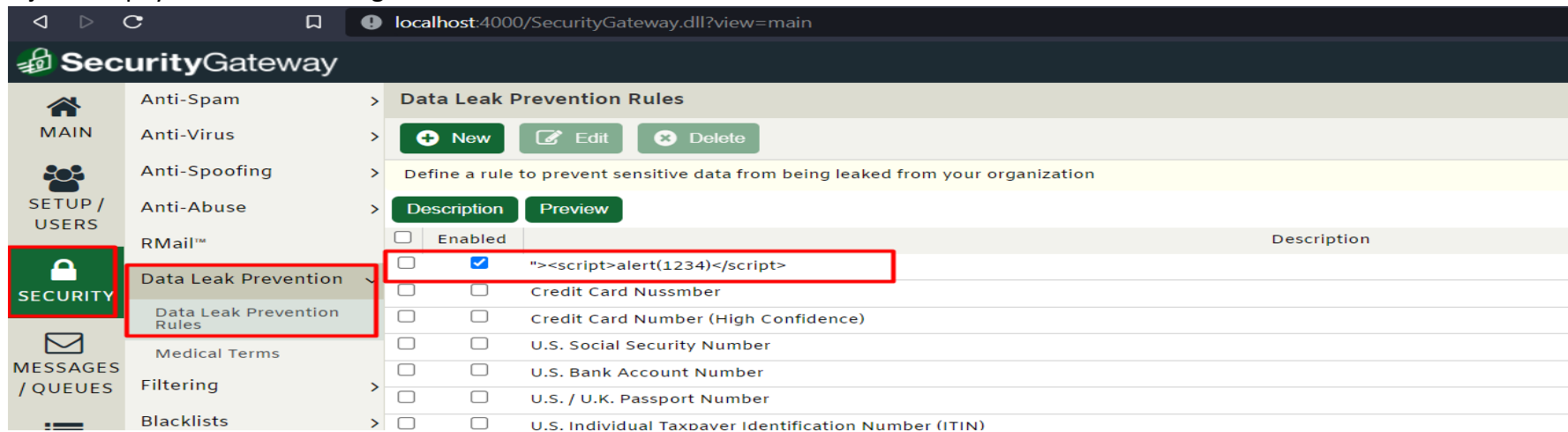
The payload `'"><script>alert(123)</script>'` was submitted with GET Request. The HTTP response appears to contain the output from the injected payload, indicating that the payload was executed successfully on the server.

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

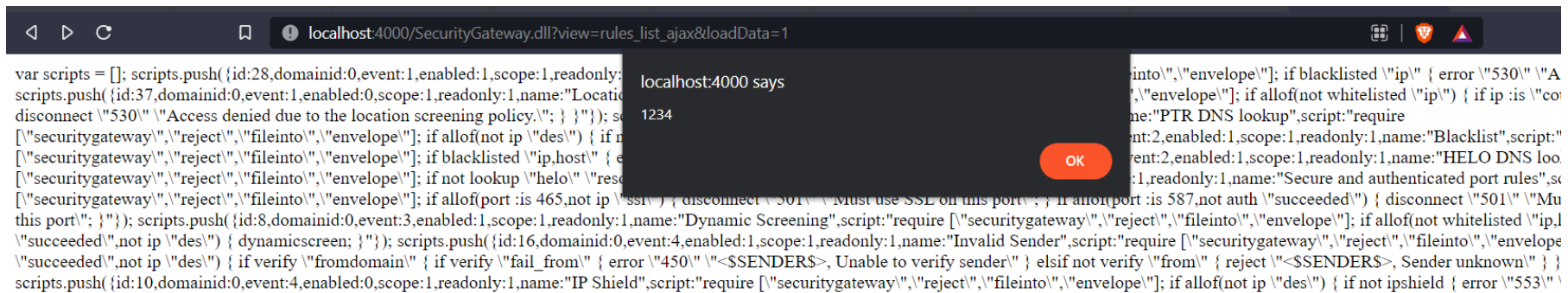


The screenshot shows the SecurityGateway web interface. The left sidebar has a 'SECURITY' menu item highlighted. The main content area displays 'Data Leak Prevention Rules' with a table of rules. One rule is highlighted with a red box, showing the payload `'"><script>alert(1234)</script>'` in the 'Description' column. The 'Enabled' checkbox for this rule is checked.

Description	Enabled
<code>'"><script>alert(1234)</script>'</code>	<input checked="" type="checkbox"/>
Credit Card Nussmber	<input type="checkbox"/>
Credit Card Number (High Confidence)	<input type="checkbox"/>
U.S. Social Security Number	<input type="checkbox"/>
U.S. Bank Account Number	<input type="checkbox"/>
U.S. / U.K. Passport Number	<input type="checkbox"/>
U.S. Individual Taxdaver Identification Number (ITIN)	<input type="checkbox"/>

Now visit

http://localhost:4000/SecurityGateway.dll?view=rules_list_ajax&loadData=1



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.