Tom Follow

Jun 25 · 2 min read · Listen

Persistent Cross-site scripting leading to full account takeover on Galaxkey v5.6.11.4 and v5.6.11.5

CVE-2020–27509

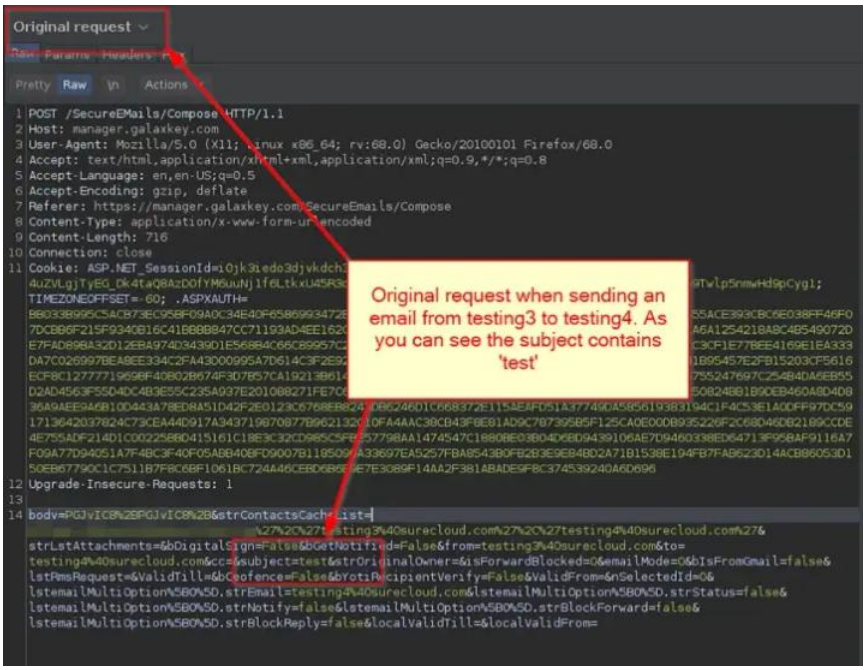
I am a Senior Cybersecurity Consultant for SureCloud Limited and whilst on an engagement discovered persistent cross-site scripting which led to full account takeover on Galaxkey's Secure Email platform. The vulnerable versions were 5.6.11.4 and 5.6.11.5.

Note: This has now been fixed by the security team at Galaxkey.

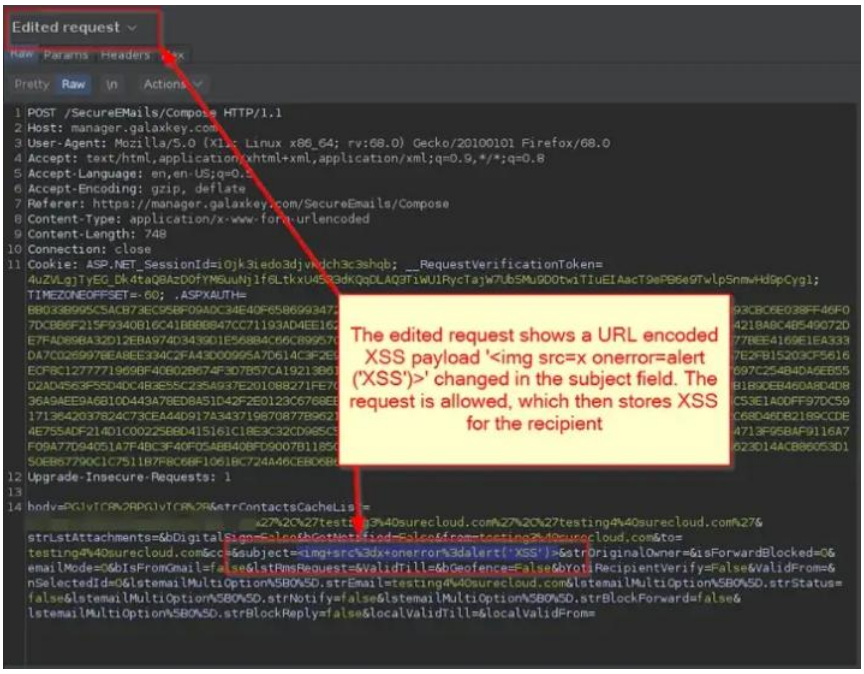
The vulnerability allowed an attacker to perform full account takeover by manipulating the HTTP POST request when sending an email by inserting a cross-site scripting payload into the 'subject' variable. The payload executed when the recipient logged into their mailbox, due to the lack of server-side sanitisation on this variable. The attack was leveraged to full account takeover due to the session cookie not having the HttpOnly flag set.

Proof-of-Concept

The HTTP POST request for sending an email is shown below, with the vulnerable subject variable high-lighted. We are currently logged in as testing3@surecloud.com

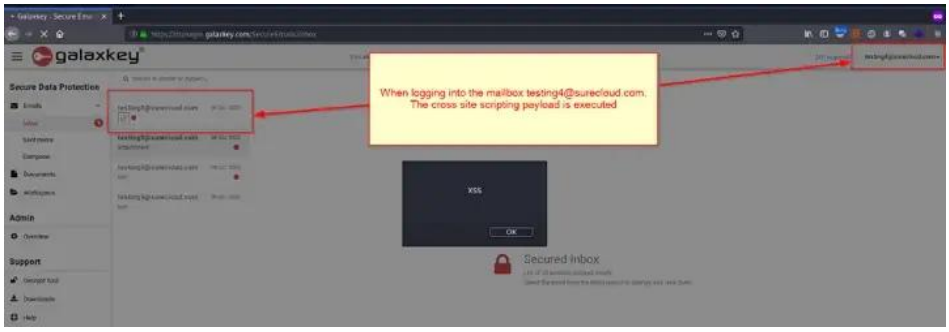


The HTTP POST request subject variable is modified to contain the URL encoded payload '<img src=x onerror=alert('XSS')>'



When the email is submitted and the recipient for example testing4@surecloud.com logs into their mailbox, the persistent cross-site scripting vulnerability is executed.

Note: For this Proof-of-Concept the payload has been changed to not contain the session information.



As the session cookie did not have the HttpOnly flag set it was possible to leverage the persistent cross-site scripting vulnerability to steal session information leading to full account takeover.