Flexera SPS Producer portal – Retest Report 20 Feb 2023

Please see the details related to new vulnerability identified during the retest.

VULNERABILITIES	SEVERITY	Retest Status
Missing Multi-factor Authentication	HIGH	Resolved
Missing SSO Integration	HIGH	Resolved
Unvalidated Redirects	MEDIUM	NEW /OPEN

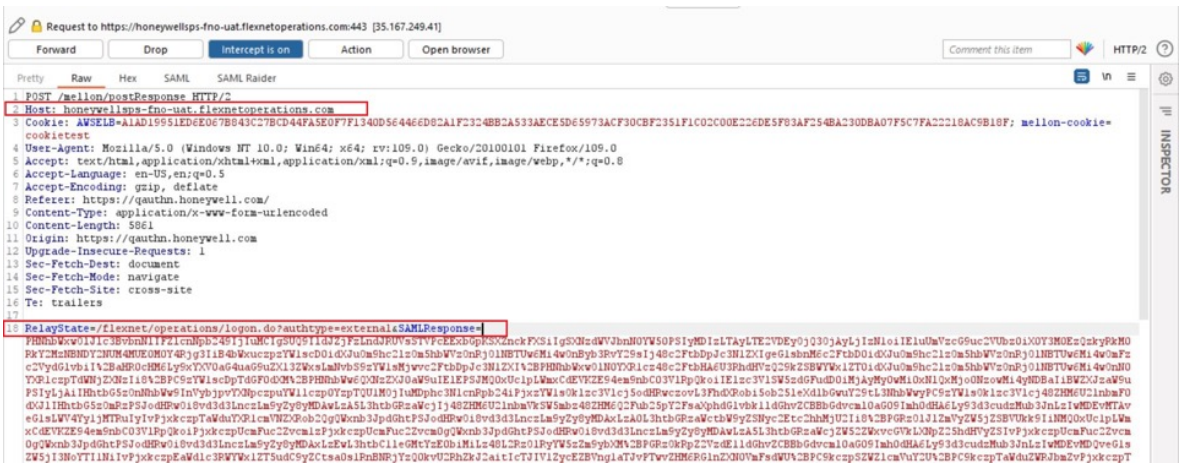
Unvalidated Redirects - MEDIUM

Observation:
Noted that an attacker can redirect the users to a malicious URL (e.g. bing.com) as the destination URL.

Recommendation:
- Avoid using redirects and forwards.
- If used, do not allow the URL as user input for the destination
- If user input cannot be avoided, ensure that the supplied value is valid, appropriate for the application, and is authorized for the user.
- Sanitize input by creating a list of trusted URLs (lists of hosts or a regex).
- Force all redirects to first go through a page notifying users that they are leaving your site and have them click a link to confirm.

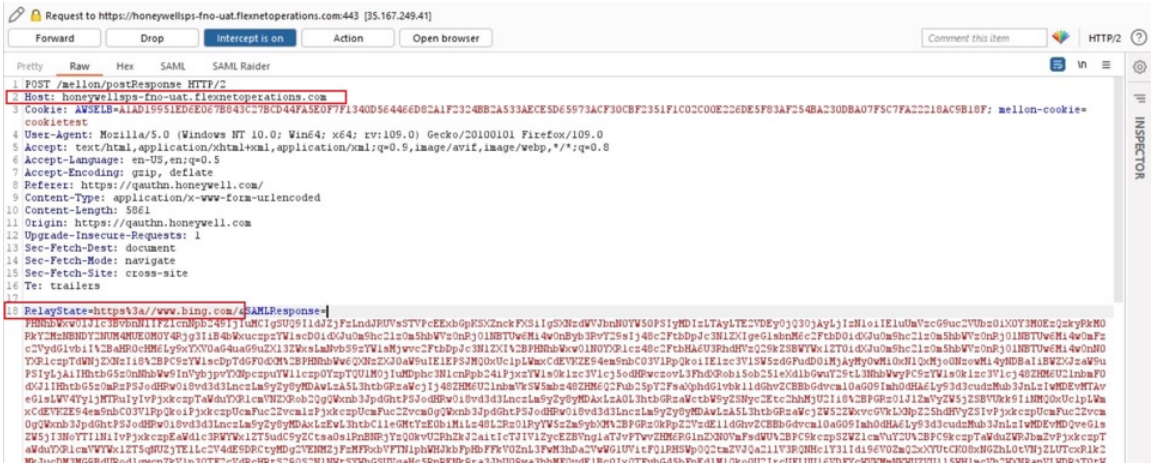
Steps to Reproduce:
1. After submitting credentials, intercept the request and approve MFA.
2. Change the ReplayState path to any desired URL and forward the request.
3. Observe the response, the user is redirected to a malicious/test URL, e.g., as bing.com.

Proof of Concept:
Below figure shows an intercepted request of ReplayState path.



Proof of Concept:

Below figure shows a malformed request with the attacker site's URL changed (e.g.; bing.com)



Below figure shows a malformed URL that is redirected to the attacker's website (e.g; bing.com)