What sort of DOM XSS (client XSS) mitigation techniques does EFT use?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT v7. and later

QUESTION

What sort of DOM XSS (client XSS) mitigation techniques does EFT use?

ANSWER

Document Object Model (DOM)-based Cross-Site Scripting (XSS) is a client (browser)-side injection issue in which the attack is injected into the application during runtime in the client (browser) directly.

To mitigate DOM XSS, EFT behaves per the following guidelines:

- Be careful with untrusted data: When forced to deal with untrusted data, EFT's web client only uses it for displayable text (rather than execution) and instead relies on EFT server for the rest of its data for execution, including templated Javascript.
- Use safe methods when dynamically rendering HTML: EFT's web client uses methods and practices recommended by OWASP for creating dynamic interfaces.
- Use caution when dealing with methods that implicitly eval() data and with eval() itself: EFT's web client uses OWASP-approved methods of parsing JSON payloads.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11477/What-sort-of-DOM-XSS-client-...