Security Best Practices

Last Modified on 10/13/2021 3:57 am EDT

It is critical that you maintain a secure environment. We recommend these best practices to maintain a secure environment.

- Configure HTTPS for all Cora SeQuence sites.
  - Administration
  - Flowtime
  - Other sites
- Do not disable or overwrite security elements that are part of the Cora SeQuence product, in its configuration files, such as EnableViewStateMac.
- Use OWASP Best Security Practices. This is particularly relevant if you write custom code and extend Cora SeQuence.
- Add validation to form input fields.
- Do not disable HTML encoding on the data you display to users.
- When you create forms, do not create security holes.
  For more information, see the OWASP documentation.
- If your forms access external systems, verify that these systems are secure, and the communication between Cora SeQuence and these systems is secure.
- Be mindful of cross-site scripting (XSS). If you want to display user input text as plain HTML (not in a text box), consider how to display the text without JavaScript or HTML tags.
- Do not rely on client-side checks and validations. Run the same checks and validations on the server side.
- For highly-secure environments, we recommend that you disable Form-based authentication. To disable Form-based authentication, remove the Form-based authentication provider from the providers list and disable anonymous access on the Administration and Process^{TOGO} sites.
- In both the Flowtime and Administration web.config files, make sure the `customErrors` property is set to On before going into production, .
- In the Flowtime web.config file, make sure that the `enableVersionHeader` property is set to false.
- Make sure to disable the reuse of session tokens across browsers or devices.
  For more information on reuse of session, read this article.