REST API XSRF Authentication

Last Modified on 04/15/2020 5:17 am EDT

A Cross-site request forgery (CSRF or XSRF) attack tricks a user into submitting an unintended web request by an event as simple as clicking an image. This request may contain URL parameters, cookies, and other user related information that web application may use to authenticate the users and perform actions on their behalf. The actions triggered from such malicious web requests can allow the attackers to modify and steal important information, or manipulate session data by changing the passwords on the web application.

Cora SeQuence is also vulnerable to such XSRF attacks, and to prevent these Cora SeQuence allows XSRF authentication of the POST, PUT, DELETE, and PATCH REST API requests sent to the system.

This XSRF authentication of REST API is configurable. You can enable or disable the feature in the web.config file (code sample shown below).

The feature is disabled by default. To enable this feature, set the value of *enabled* and *enablesOnServices* parameters in the above code to *True*.

To authenticate the REST API request, you include the XSRF token in the request header. The REST API exposes an endpoint that handles the XSRF token requests.

The generated token is then added to the request header:

- Header name: X-SqXsrfToken
- Value: generated token value

Methods

Supported	Not supported
• POST • PUT • DELETE • PATCH	• GET • HEAD • OPTIONS • TRACE

URL

https://localhost:1919/auth/v1/token

Example of token request

```
$.ajax({
        type: "POST",
        url: "http://localhost:1919/auth/v1/token",
        contentType: "application/json; charset=utf-8",
        dataType: "json",
        cache: false,
        async: false,
   });
```