Security report

Security breach	Covered?
Protection against malicious file uploads	Yes
Protection against Man-in-the-middle attacks	Yes
Protection against Link Injection Protection	Yes
Protection against Attribute autocomplete	Yes
Click hijacking protection	Yes

Protection against malicious file uploads

If a file does not match a template describen on a server, the server returns "Not a valid simulation file". No Scripts can be executed since we are parsing the XML as SQL. Additionally nowhere in the frontend unfiltered html is added to the DOM, only via react templates, which filters it

Protection against Man-in-the-middle attacks

We have a HTTPS certificate. This means that whenever a user accesses our web application, they can look at the certificate and assure that the response was the one our server sent.

Protection against Link Injection Protection

Every api endpoint in the Application requires an authentication token. If a user tries to access any of the project links without a token, they will be redirected to a login page or no information will be sent.

Protection against Attribute autocomplete

Autocomplete is explicitly set to “off” on the website login/registration page.

Click hijacking protection

A user can never post anything on the web application. the user can only upload files (see malicious file uploads), or a user can view stored data. This means it is not possible for a user to post an element that could potentially hijack clicks.