Security report

Security breach	Covered?
Protection against malicious file uploads	No
Protection against Man-in-the-middle attacks	Yes
Protection against Link Injection Protection	Yes
Protection against Attribute autocomplete	Yes
Click hijacking protection	Yes

We protected against:

SQL Injection

Our application uses SQL queries that take user input. Therefore, to prevent any SQL injection we made the SQL code to have prepared statements.

Man In The Middle Attacks

We have secure login authorization by using Oauth2, relieving us from storing our credentials and passwords in the database. From the authorization server we retrieve access and Id tokens. We hash the access token and store it temporarily in our server and send it in the form of a cookie to the browser. In that way the user can authenticate to the resource server.

This is useful to prevent man in the middle attacks as the important information is not in plain text, readable by anyone who manages to listen in on the send and request.

Additionally, the access token has an expiry time of one hour, preventing attackers who compromised the token to continuously use the token information, if they managed to decode it as it will expire.

These credentials are further used to increase security by maintaining access restrictions for data confidentiality. Association members aren't able to access files belonging to other associations as their access rights are checked every time they try to access a file with their credentials in the database.

Attribute Autocomplete

For attribute autocompletion, there is one page where this issue is a concern, namely the login page. However, since we use Okta for our login we don’t need to implement any prevention methods ourselves, as this is managed by Okta.

Click Hijacking & Link injection

To resolve this issue we used methods that sanitized our input. The method prevents inline styling that could potentially hide malicious links. This is done through methods such as whitelisting characters. The input of new content to our system can only have certain characters that are specified by the system. Otherwise, an error occurs.