Security report- Team 4 GRYBB

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

Protection against malicious file uploads

Since our web application does not require the user to upload a file and does not have any option do so, there is no way for an attacker to upload a malicious file to our server

Protection against Man-in-the-middle attacks

No

Protection against Link Injection Protection

Wherever in the application user input is taken, it is extremely restricted. The user cannot enter any special characters in any of the input fields in the web application. Only characters from a-z(A-Z) and numbers 0-9 can be entered. This doesn’t allow the user to input malicious code in the website by using symbols like <,>,/, etc. to make the server mistake user input as code.

Protection against Attribute autocomplete

Wherever in the application user input is taken autocomplete has been set to off by using appropriate HTML code. The browser will not autocomplete user input fields for any user since the forms used in the web application do not allow the browser to do this. It tells the browser not to save data inputted by the user for later autocompletion on similar forms, though heuristics for complying vary by browser.It stops the browser from caching form data in the session history. When form data is cached in session history, the information filled in by the user is shown in the case where the user has submitted the form and clicked the Back button to go back to the original form page. Also, since user input is always validated , it is very difficult for an attacker to run malicious code on the website

Click hijacking protection

Clickjacking is a type of attack, where the attacker tricks the victim into performing a malicious action by hijacking their click. To prevent this, our web application makes use of the same origin policy which will allow the page to be displayed only in the frame of the same origin as the page itself.We have added security HTTP headers per server by declaring it directly on the whole server level and configuring apache.

<u>Additional security</u>

- Usage of prepared statements wherever possible to protect the website against sql injection.
- Implementation of a secure login system which makes it impossible to use the website without logging in successfully first.
- Usage of sessions : - A user will be logged out after a set amount of time forcing the user to log in again. This reduces the chances of unauthorized users to gain access to already logged in accounts