SIT 218/738: Secure coding

**Distinction task 7.2D: Session management and CSRF attacks**

**Overview**

The updated 08-session-management app blocks the CSRF attacks by comparing the HTTP referrer header value. Report the response received when the CSRF attack is launched and discuss the logic behind the prevention. Also discuss the circumstances when this mitigation method will not be effective.

Catch the error that was reported by the web app when CSRF attack failed using a @ExceptionHandler and return a custom error message instead of the default 500 response page. Also log the error at the highest level.

Session management in the web app also has another issue where in once the user is logged into the web app, the authenticated URL can be copied in another new Firefox browser and the authenticated page can be displayed even when the user logged off in one of them. Instead add a logoff handle in the workout.jsp and manage it in the LoginController where you invalidate the user session so that I is no longer active in the second browser.

**Submission Requirements:**

Submit one PDF file containing the following information:

1. Screenshot of error page.
2. A paragraph reflecting on the prevention logic and when this mitigation method will fail.

**Submission Due**

The due for each task has been stated via its OnTrack task information dashboard.