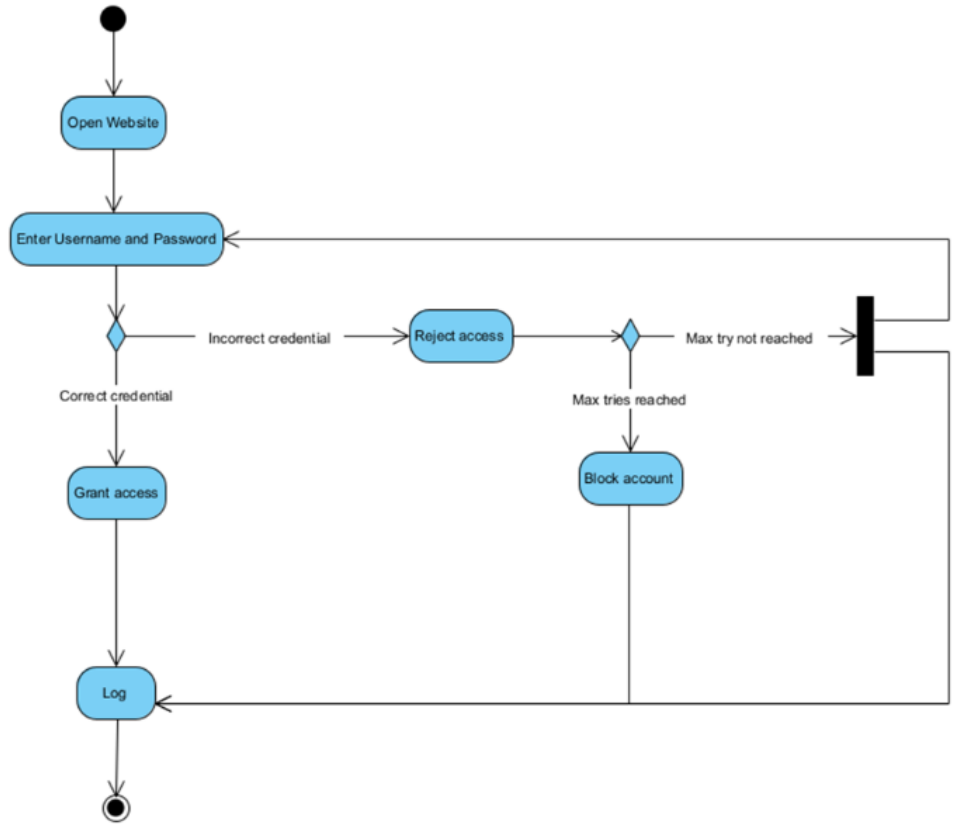
Security logging and monitoring failures are one of the top 10 web application security concerns, according to the Open Web Application Security Project (OWASP) This category is designed to assist in the detection, escalation, and response to active breaches. Breach detection is unachievable without logging and monitoring (OWASP, 2021).

Insufficient logging, detection, and monitoring mainly occurs any time when auditable events, such as logins, failed logins, and high-value transactions, are not logged, warnings and errors generate no or inadequate log messages, logs of applications are not monitored for suspicious activity, appropriate alerting thresholds and response escalation processes are not in place or effective, etc. (OWASP, 2021).

The process of logging into a system is illustrated in the UML activity diagram below. If a user tries multiple username and password combinations and the application does not log these events with adequate detail and these logs are not monitored, this may lead to further breaches or allow a breach to go undetected (OWASP,2021).

Further to reading peers post I can agree that “One way to lower the chance of data breaches is to know first whether the data breach is happening.”



References:

OWASP Top 10 (2021) OWASP top ten. Available from: **https://owasp.org/www-project-top-ten/** [Accessed 25 Mar 2022]