Onderzoek story 4: Veilige website voor financiële transacties

Bij deze userstory heb ik samen met Erkan onderzocht wat belangrijk is voor de veiligheid van een pagina en welke dingen toepasbaar zijn voor onze website.

• HTML injection tegenhouden door middel van het blokkeren van tekst input met html tags

Het is belangrijk dat de site tegen HTML-injectie is beschermd. HTML-injectie is op schadelijke invoervelden van de site werkende HTML-code invoeren. Als de site niet beschermd is tegen HTML-injectie, kunnen mensen HTML code naar de website sturen.

Dit kan heel erg slecht zijn, door HTML-injectie kan je bijvoorbeeld de design van de website veranderen, of gegevens van gebruikers stelen.

• SQL injection tegenhouden

SQL-injectie houdt in dat je doormiddel van het invoeren van SQL-code in een invoerveld het SQL-database kan manipuleren. Als jouw website hier niet tegen beschermd is, kunnen belangrijke tabellen worden aangepast of verwijdert.

• XSS-aanvallen tegenhouden

XSS-Aanvallen is het injecteren van javascript code op een pagina van een website. Als dit succesvol gaat, wordt elke keer het geïnjecteerde javascript uitgevoerd als je naar de gehackte pagina gaat. Online hebben we al een tool gevonden genaamd: “Xenotix XSS Exploit Framework”. Met deze tool kan je testen of je site beschermd is tegen dit soort aanvallen.

• Dubbele Checks: checks in de database zelf en in de code van de website.

Ook is het heel belangrijke dat er niet alleen een check wordt uitgevoerd op de code van de site. Je zou als gebruiker de check in de site kunnen omzeilen, waardoor je foute data kunt invoeren in de database. Als je dezelfde check ook hebt in de database zelf, dan in het onmogelijk om foute data in de database in te voeren.

# Bronnen

<https://www.creativebloq.com/web-design/website-security-tips-protect-your-site-7122853>

<https://xenotix.in/>

<https://www.softwaretestinghelp.com/html-injection-tutorial/>