Project: Security Chief

Tester: Tristan Koning

Datum: 12/12/2024

Doel: Ons project voor de Gemeente Heerlen maakt voor 90% van de interface gebruik van SSR (Server-Side Rendering). Dit betekent dat de gebruiker alles vertrouwt wat de server stuurt. Daarom moet ik controleren of ik ergens sanitization ben vergeten.

Hypothese

Door een van mijn account velden te vervangen door een XSS-payload kan ik een alert in mijn browser krijgen als de payload ergens wordt uitgevoerd. Als dat gebeurt, krijg ik een pop-up met de tekst waarin het nummer 1 staat.

Test methode

Ik heb in de JSON-array van de website mijn website vervangen door de XSS-payload ‘<script>alert(1)</script>’, zodat ik het zie als er ergens niet gesanitized is.

Test resultaat

Na alle pagina’s te hebben doorgelopen, heb ik geen alerts ontvangen. Dit betekent dat er in ieder geval geen XSS-fout zit in de code die de websites rendert. Ik was vooral bang dat de websites-array een probleem zou kunnen zijn, omdat je elk element één voor één moet saniteren met een loop, maar alles zag er goed uit.