OWASP 7 - Cross Site Scripting (XSS)

Cross-site scripting (XSS) is een fout in de beveilig van websites. Het zorgt ervoor dat websites - die normaliter wel betrouwbaar zouden zijn - onbetrouwbaar worden. Dit komt omdat de website XSS injectie toestaat.

Wat kun je met XSS injecties bereiken?

Het doel van XSS injecties is om permanente verandering aan te brengen aan een website. Een persoon met verkeerde intenties zou JavaScript code kunnen invoeren in een input field, waardoor deze mogelijk in een database tabel wordt opgeslagen. De opgeslagen JavaScript code zou uitgevoerd kunnen worden als de data uit de database tabel bijvoorbeeld gebruikt zou worden om data te tonen op de website. Zo zou de ontwikkelaar van XSS injecties ervoor kunnen zorgen dat de bezoeker van een website ge-redirect wordt naar een andere website.

XSS injectie opdracht

In deze les gaan we aan de hand van een simpele implementatie XSS injectie demonstreren. Let's start coding!

In deze les gaan we een input field binnen een form maken. Als het form af is gaan we met behulp van JavaScript wijzigingen aanbrengen in onze interface. Voor we XSS injectie kunnen toepassen, gaan we eerst het form maken. Dit doen we aan de hand van de volgende stappen:

1. Open de folder waar XAMPP in is opgeslagen en ga naar de htdocs -older. Maak een nieuwe map aan in deze en noem het XSS.
2. Maak een index.php file in de XSS-folder
3. Zorg ervoor dat de index.php file een HTML-skeleton bevat.
4. Maak een form aan in de body tag van index.php. Zorg ervoor dat dit form de index.php file aanroept.
5. Maak binnen het form een input field aan met een placeholder. De waarde hiervan stel je gelijk aan *Zoekopdracht*.
6. Zorg ervoor dat er een knop is naast de input field. We waarde van deze knop moet gelijk zijn aan *Zoek*.

7. Schrijf embedded php code in index.php. Deze code moet uitgevoerd worden zodra de gebruiker op de *zoek* knop drukt. Zorg ervoor dat je php code m.b.v. de isset functie checkt of er een waarde is ingevoerd in het input field. Als de check *true* is, zorg je ervoor dat je de volgende text print:

   De zoekopdracht is: $zoekopdracht
   Geen resultaat gevonden!

> **Opdracht 1:** Wat wordt er op de pagina getoond als je de volgende text invoert:
>
> Coole website <script>alert("XSS voorbeeld")</script>?

> **Opdracht 2:** Wat gebeurd er als je <font color="blue"> invoert?

> **Opdracht 3:** Hoe kun je XSS injecties voorkomen?

Revision #3
Created 2020-03-02 20:40:55 UTC
Updated 2020-03-09 17:42:58 UTC