

S3- Db02

Sander van Deurzen

**XSS(Cross Side Scripting)**

18-02-2022

**Introductie**

**Wat is Cross Site Scripting?**

*Cross Side Scripting is de naam van een fout in de beveiliging van een*[webapplicatie](https://nl.wikipedia.org/wiki/Webapplicatie)*. Het probleem wordt veroorzaakt doordat de invoer die de webapplicatie ontvangt (zoals*[cookie](https://nl.wikipedia.org/wiki/Cookie_(internet)),[url](https://nl.wikipedia.org/wiki/Url), *request parameters) niet juist wordt verwerkt en hierdoor in de uitvoer terechtkomt naar de eindgebruiker. Via deze bug in de website kan er kwaadaardige code (*[JavaScript](https://nl.wikipedia.org/wiki/JavaScript), [VBScript](https://nl.wikipedia.org/wiki/VBScript), [ActiveX](https://nl.wikipedia.org/wiki/ActiveX), [HTML](https://nl.wikipedia.org/wiki/HTML), [Flash](https://nl.wikipedia.org/wiki/Adobe_Flash)*etc.) geïnjecteerd worden. Hiermee kunnen onder meer sessiecookies worden bekeken, sessie van een gebruiker worden overgenomen, functionaliteit van een website worden verrijkt of onbedoelde acties voor een gebruiker worden* uitgevoerd*. https://nl.wikipedia.org/wiki/Cross-site\_scripting*

Met een XSS aanval kan je kleine aanvallen doen, zoals de kleur van je website achtergrond aanpassen of een javascript alert creëren, alleen kan je ook met XSS aanvallen iemand zijn database platleggen doormiddel van 1 query in een tekstveld. Dat maakt het super belangrijk om hier beveiligd voor te zijn. En daaruit komt de vraag:

***Hoe kan ik mijn website beveiligen tegenover XSS aanvallen?***

**Soorten XSS**

**Als je over XSS spreekt, spreek je niet gelijk over een algemeen onderwerp. We spreken van 3 verschillende soorten XSS aanvallen;**

**-Reflected XSS Attack:**

Stored XSS also known as persistent XSS occurs when user input is stored on the target server such as database/message forum/comment field etc. Then the victim is able to retrieve the stored data from the web application.

**- Stored XSS Attack:**

Stored XSS also known as persistent XSS occurs when user input is stored on the target server such as database/message forum/comment field etc. Then the victim is able to retrieve the stored data from the web application.

**- DOM Based XSS Attack:**

DOM Based XSS is a form of XSS when the source of the data is in the DOM, the sink is also in the DOM, and the data flow never leaves the browser.

**Wat kan ik tegen een XSS Doen?**

**Gelukkig is Cross side scripting makkelijk te beveiligen. Populaire webframeworks zoals Laravel heeft ingebouwde beveiliging tegenover XSS aanvallen.**

**- Alle niet vertrouwde gegevens op basis van de HTML-Context, attribuut, Javascript, CSS of URL waarin de gegevens zijn geplaatst moeten uitgefilterd worden**

**Conclusie**

**Een XSS aanval wordt weinig aandacht aan gegeven bij beginnende ontwikkelaars terwijl die aanvallen cruciaal kunnen zijn voor hun webapplicaties.**