Uitwerking OWASP 7 - CROSS SITE SCRIPTING (XSS)

Cross-site scripting (XSS) is een fout in de beveilig van websites. 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:

Ingevoerde zoekterm: $zoekopdracht
Er zijn geen resultaten gevonden voor de ingevoerde zoekopdracht

Uitwerking bovenstaande stappen

```
<!DOCTYPE html>
<html>
<head>
	<title>Mooie demonstration</title>
</head>
<body>
	<h1>Voer je zoekopdracht hieronder in</h1>
```

```
<form action="index.php" method="get">
<input type="text" name="search" placeholder="Zoekterm invoeren " />
<input type="submit" name="submit" value="Zoek">
</form>

<?php
if (isset($_GET["search"])) {
echo "Ingevoerde zoekterm: " . $_GET["search"] . "<br/>";
echo "Er zijn geen resultaten gevonden voor de ingevoerde zoekopdracht!";
}
?>
</body>
</html>
```

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

De pagina toont de text *Ingevoerde zoekterm: Coole website*. De script tags en de JavaScript functie tonen niet. Deze zorgen er wel voor dat er een pop-up box met de text *XSS voorbeeld* verschijnt.

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

De text *Er zijn geen resultaten gevonden voor de ingevoerde zoekopdracht* kleurt blauw.

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

XSS injecties kun je voorkomen door de user input te beperken tot een bepaalde tekenreeks. Bijvoorbeeld alleen letters en getallen. Dit resultaat zou je bereiken door Regular Expressions (RegEx) toe te passen.

Revision #3
Created 2020-03-09 20:53:22 UTC
Updated 2020-04-14 11:08:28 UTC