# The Cross-site Scripting (XSS)

The Cross-site Scripting is a strike in the licensed websites or a web applications in the client’s side that the attacker can execute codes through their browsers. The attacker will find a weak spot in the website then this will be an opportunity to them to insert malicious scripts in the browser. This scripts are carried mostly in the structure of javascript codes. It is necessary in XSS vulnerabilities a collaboration with the user to provoke the weak spot of the site. The attacker posts the malicious scripts in the website. If a user inputs any form of data in the site then the browser executes the embedded codes and the user information will be directly transported to the attacker. Then the attacker can administer codes that can control the data that are stored in the system. The attacker can use these information as a threat to the user.

There are three types of Cross-site scripting vulnerability. The first vulnerability is the stored, it occurs when the payload is saved in the computer of the user then this will be a part of the webpage that can execute the malicious pages. The reflected is also a type of the XSS vulnerability this happens when the attacker send a malicious script to the user. This script is a component of the request delivered to the server and then it throws back the HTTP Response that compromises the script from the HTTP request.The last vulnerability is the DOM-based XSS, it happens when the webpage consists a script that composes user provided data to the DOM.

## Prevention

Cookies can be stolen via javascript. To avoid cookies from being stolen by cyber criminals, you can Most of the commonly used browsers allow the user to turn off third party or turn off the the cookies entirely. Be cautious when visiting untrusted websites. These websites are commonly not secure, which means that information theft can commonly happen when visiting untrusted websites. Be aware of the websites and ads you are visiting and clicking. Do not just click ads because ads normally redirects the user to other malicious websites.

## Example

* Cookie theft

Cookies are small pieces of data that are stored in the user’s browser that contains information about the user’s interaction with the website. Cookies can also contain user’s username and password or other important information about the user using javascript. Untrusted websites and banner ads can plant third party cookies on the user’s browser that steals cookie information from the user and send those data to cyber criminals.

* Redirect user to malicious website

Malicious script can be inserted to a website that can redirect the user to malicious websites like phishing websites which aims to steal users personal information. Stolen information can be used for malicious activities and this can even be used to gain something from the user for example stealing money if bank account was stolen, blackmailing to gain money.