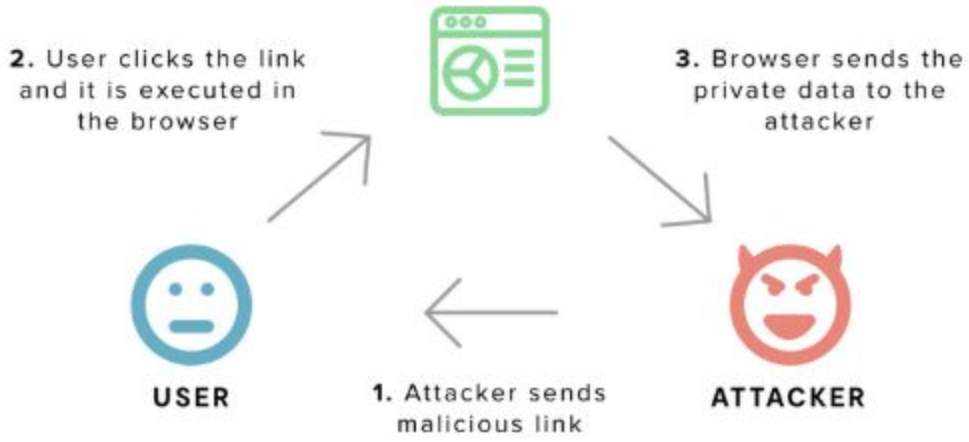
Week 12 A7-Cross-Site Scripting (XSS)

Explain the “sections” “Is the Application Vulnerable” and “How to Prevent” for the OWASP 2017 Risks: A7:

There are three kinds of XSS (Cross-Site Scripting):

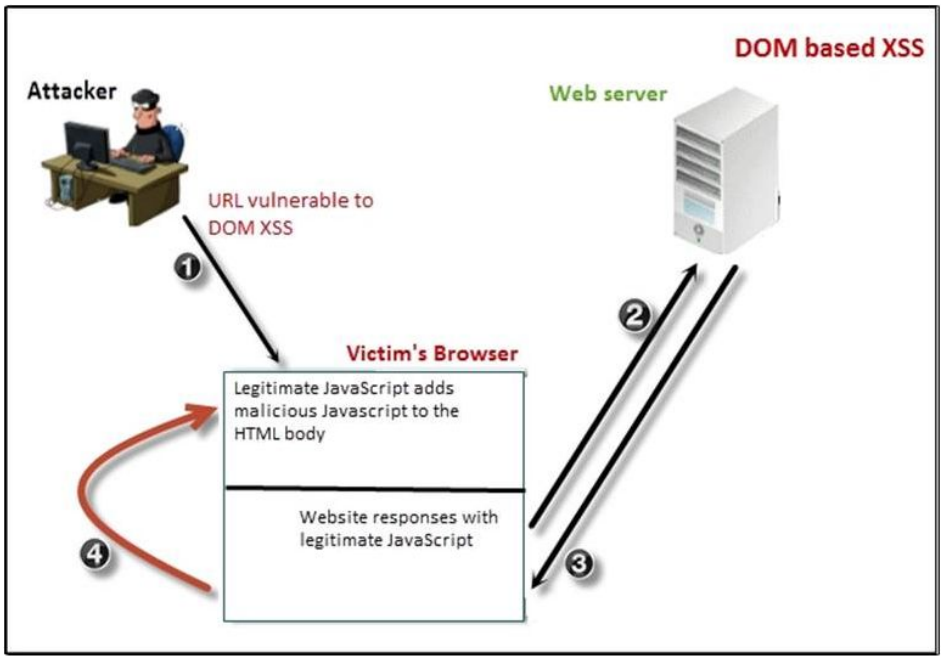
- **Reflected XSS: (ikke persistent XSS)**
  Reflected XSS is when a hacker has the opportunity to get a user to browser a malicious link. This is often done with emails and Social Engineering.



- **Stored XSS: (persistent XSS)**
  Stored XSS is when a hacker makes some HTML or JavaScript that is saved on a server which in turn can be used to run on other users. Often, it is some JavaScript code that is run without a user knowing. It can be a small HTML tag, that might run scripts from a hacker which miht copy a users session ID or cookies.

- **DOM XSS: (persistent XSS)**

  XSS-attack where the payload is deployed as a result of manipulating the DOM of the victims browser, so that the client side code runs in an modified way.



What kind of “indications” will an attacker look for in a WEB-page before testing whether the site is vulnerable to XSS-attacks?:
A hacker will often look after what functions the website has, and to see if there is a hole in where you can hide some html-tags which leads to links where you can hide scripts.

Explain and demonstrate ways to prevent XSS-attacks:
There is a good and easy way to prevent XSS attacks that everyone can do. Use libraries that are designed to prevent the XSS attacks. Owasp has a nice link to read up on some juicy tricks https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

Explain the terms *HTML Sanitizer* and *HTML Encoder* and their purposes

HTML Sanitizer

To sanitize HTML you begin a process in where you cross examine a list where you can see what tags are to be or not to be used, and you can remove and replace the tags needed

HTML Encoder
To convert some character outside of the normal 7-bit ASCII range, to a more standardized form.