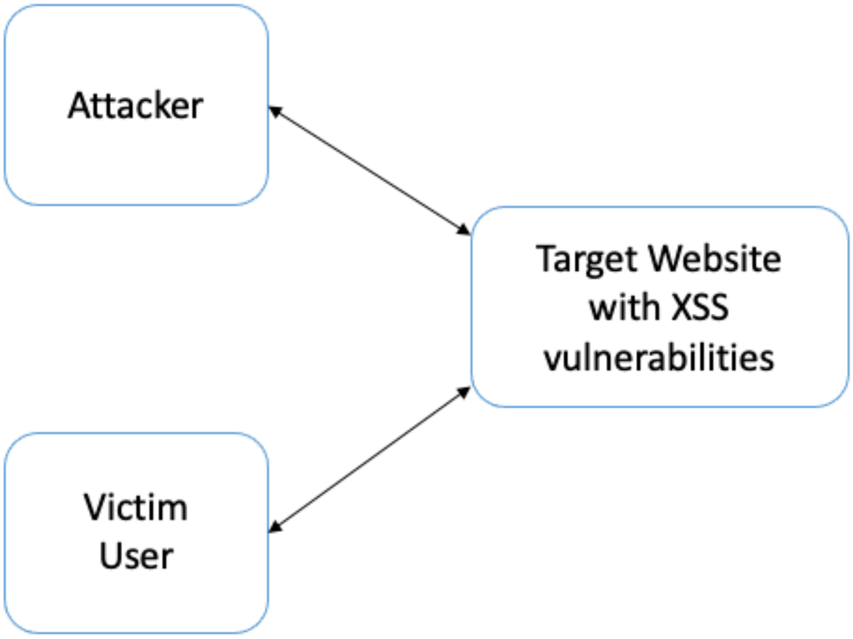
How Cross Site Scripting (XSS) attack works:

XSS attacks exploit "***the trust that a browser has in a website***".

The browser considers a website that it interacts with as trusted site and executes any code that it receives from that website. If the code received is malicious, it can do a lot of damage when run in the browser on the client side.

XSS attack is a form of a **code injection** attack on a website. SQL Injection attack is another example of code injection attack.



Countermeasures for CSRF Attacks:

1. **`Input validation/sanitization`**: The website will validate/sanitize the incoming data to make sure the data is not mixed with code (script code).
2. **`Output encoding`**: If the data has already made its way into the target website or to a persistent storage that a website uses, the website can encode any special script tags in the data before sending that data to the browser so the browser will just display the code as text instead of executing the code.

In XSS lab, the Elgg web application uses both these approaches to protect against XSS attacks.