Cross-Site Request Forgery

.NET

Client-Side validation gives users instant feedback on the information they submitted to a web page. Server-Side validation is also necessary because information arriving from the network should never be trusted .

HTTPS://WWW.C-SHARPCORNER.COM/ARTICLE/CUSTOM-DATA-ANNOTATION-VALIDATION-IN-MVC/

Over-Posting

https://docs.microsoft.com/en-us/aspnet/mvc/overview/getting-started/getting-started-with-ef-using-mvc/implementing-basic-crud-functionality-with-the-entity-framework-in-asp-net-mvc-application#overpost

Cross-Site Request Forgery(CSRF)

https://en.wikipedia.org/wiki/Cross-site_request_forgery

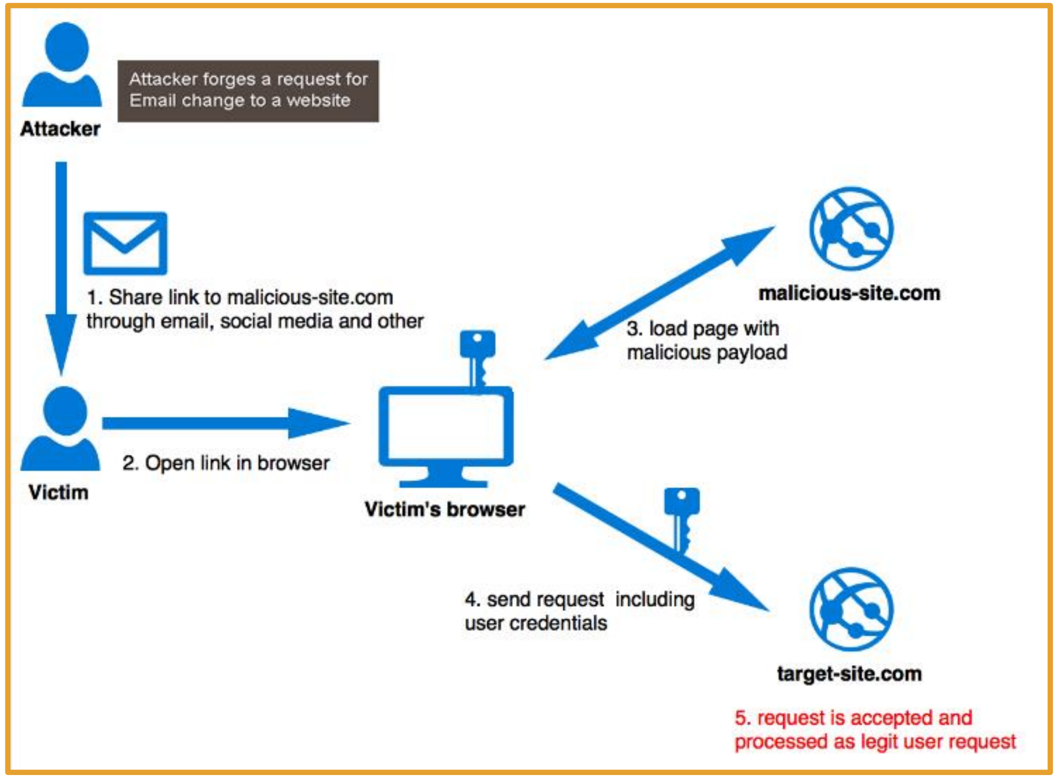
CSRF is a type of attack where unauthorized commands are transmitted from a user that the web application trusts.

A malicious website can transmit commands by using:

- specially-crafted image tags,
- hidden forms,
- *JavaScript XMLHttpRequests.*

All the above can work without the user's interaction or even knowledge. *CSRF* exploits the trust that a site has in a user's browser.

In a *CSRF* attack actions can be performed on the website that can include inadvertent client or server data leakage, change of session state, or manipulation of an end user's account.



Attacker
Attacker forges a request for Email change to a website
1. Share link to malicious-site.com through email, social media and other
malicious-site.com
3. load page with malicious payload
Victim
2. Open link in browser
Victim's browser
4. send request including user credentials
target-site.com
5. request is accepted and processed as legit user request

CSRF (Cross Site Request Forgery)

https://docs.microsoft.com/en-us/aspnet/mvc/overview/security/xsrfcsrf-prevention-in-aspnet-mvc-and-web-pages

Create secure login

https://docs.microsoft.com/en-us/aspnet/mvc/overview/security/create-an-aspnet-mvc-5-web-app-with-email-confirmation-and-password-reset