Cross-Site Request Forgery (CSRF) Prevention in PHP

- CSRF is a type of attack that occurs when a malicious web site, email, blog, instant message, or program causes a user's web browser to perform an unwanted action on a trusted site when the user is authenticated. A CSRF attack works because browser requests automatically include all cookies including session cookies. Therefore, if the user is authenticated to the site, the site cannot distinguish between legitimate requests and forged requests.

Prevention:

- A hidden token used in an input form to let server verify that the requested client is legit, if this CSRF Token not included in input form and validated correctly, an attacker can forge requests on behalf of the real client.

To learn how to protect your PHP App/Site against CSRF, watch this video
https://www.youtube.com/watch?v=8MksjpfDvRw

If you are using a PHP framework, CSRF token should/will be implemented and validated automatically in the framework.

Toolkit Scans if input form doesn’t have CSRF Token and Notifies Developer about it.

To learn more, go here:
https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html