Cryptography and Network Security Lab 12

Perform Reflected Cross-Site Scripting (XSS) Attack on the vulnerable web application. Set the security level "Low, Medium, High" to inject malicious scripts into the web application.

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site.

Reflected XSS attack: A reflected XSS (or also called a non-persistent XSS attack) is a specific type of XSS whose malicious script bounces off of another website to the victim's browser. It is passed in the query, typically, in the URL. It makes exploitation as easy as tricking a user to click on a link.

In this lab we will do the following:

- Set security level low in DVWA and perform the reflected XSS attack
- Set security level Medium and inject the attack vector to retrieve the session ID.
- Set security level High and inject the malicious vectors to perform reflected XSS.

Resources:

- ✓ **https://www.youtube.com/watch?v=J7fVOyhIX1c**