**Instal·lació i Pràctica amb OWASP WebGoat**

**1. Objectius de la Pràctica**

* Aprendre a instal·lar i executar OWASP WebGoat en un entorn Kali Linux.
* Familiaritzar-se amb la interfície i el conjunt de lliçons que proporciona WebGoat.
* Treballar sobre vulnerabilitats específiques guiades per les lliçons (SQL Injection, XSS, CSRF, etc.).
* Comprendre les tècniques d’explotació i proposar solucions de seguretat.

**2. Instal·lació de WebGoat i WebWolf**

1. Descarregar WebGoat i WebWolf (versió exemple):

**cd /opt**

**sudo wget https://github.com/WebGoat/WebGoat/releases/download/v8.2.2/webgoat-server-8.2.2.jar**

**sudo wget https://github.com/WebGoat/WebGoat/releases/download/v8.2.2/webwolf-8.2.2.jar**

Executar WebGoat:

**java -jar webgoat-server-8.2.2.jar**

**3. Accedir a WebGoat**

* Obriu el navegador i aneu a **http://localhost:8080/WebGoat**
* Registreu un nou compte o inicieu sessió amb credencials ja existents.
* Un cop a dins, observeu les lliçons disponibles.

**4. Lliçons i Vulnerabilitats**

Seleccioneu algunes lliçons per practicar:

* SQL Injection (Basics): Introduïu consultes malicioses per obtenir dades sensibles.
* Cross-Site Scripting (Stored/Reflected): Injecteu <script>alert('XSS')</script> i analitzeu el resultat.
* CSRF (Cross Site Request Forgery): Enteneu com es pot forçar un usuari a realitzar accions sense el seu consentiment.
* Insecure Direct Object References (IDOR): Manipuleu IDs a la URL per accedir a recursos no autoritzats.
* Command Injection: Intenteu injectar comandes del sistema a través de paràmetres a l’aplicació.

**5. Anàlisi i Reflexió**

* Documenteu els passos seguits, les injeccions provades i els resultats obtinguts.
* Reflexioneu sobre les mesures de seguretat:
  + Per SQL Injection: consultes preparades, validació de dades.
  + Per XSS: escapament de sortida, filtres d’entrada, CSP.
  + Per CSRF: ús de tokens anti-CSRF.
  + Per IDOR: controls d’accés robustos.
  + Per Command Injection: validació estricta d’entrada i limitació de comandes.

**7. Lliurament**

* Un document on es descriguin les lliçons treballades, els atacs realitzats i les defenses recomanades.