1. set up

a. DVWA (Damn Vulnerable Web App)

If you already have the **Metasploitable 2** VM running, DVWA is pre-installed.

Accessing DVWA:

1. **Find the IP:** In your Metasploitable terminal, type `ifconfig` (e.g., `192.168.56.101`).
2. **Open Browser:** On your host machine (or Kali VM), go to `http://[IP-ADDRESS]/dvwa/`.
3. **Login:** Use `admin` / `password`.
4. **Initial Setup:** You **must** click the **"Setup / Reset DB"** button in the left menu and then click **"Create / Reset Database"** to make the app functional.

2. Document Vulnerabilities

A. Documenting SQL Injection (SQLi)

- **Vulnerability Name:** A03:2021-Injection (SQLi)
- **Location:** DVWA SQL Injection Tab (`/vulnerabilities/sqli/`)
- **Severity:** Critical, and Low
- **Description:** The application takes user input from the `id` field and inserts it directly into a database query without sanitization. This allows an attacker to manipulate the query logic.

Proof of Concept (Step-by-Step):

1. Navigate to the SQL Injection page in DVWA.
2. Input the payload: `1' OR '1'='1' #`
3. The backend executes: `SELECT first_name, last_name FROM users WHERE user_id = '1' OR '1'='1' #';`
4. **Result:** The application returns the full names of every user in the database.

B. Documenting Cross-Site Scripting (XSS)

- **Vulnerability Name:** A03:2021-Injection (Stored XSS)
- **Location:** DVWA XSS (Stored) Tab (`/vulnerabilities/xss_s/`)
- **Severity:** High
- **Description:** The application stores user-submitted comments in the database and displays them to other users without encoding the output. An attacker can inject malicious JavaScript.

Proof of Concept (Step-by-Step):

1. Navigate to the XSS (Stored) page.
2. In the "Message" field, enter: `<script>alert('Vulnerable_Session: ' + document.cookie)</script>`
3. **Result:** Every time a user (including admins) visits this page, their browser executes the script and shows a pop-up containing their session cookie.

C. Documenting the use of Burp Suite

- **Tool Role:** Intercepting Proxy & Analysis
- **Usage:** Burp Suite was used to capture, analyze, and modify traffic between the Kali Linux attacker machine and the Metasploitable target.

PROOF IN PDF's

1. SQL INJECTION (LOW,MEDUIM)
2. XSS
3. Brupsuite