| **Course Name:** | **Information Security (116U01L602)** | **Semester:** | **VI** |
| --- | --- | --- | --- |
| **Date of Performance:** | **13 / 03/ 2025** | **DIV/ Batch No:** | **C3** |
| **Student Name:** | **Romil Lodaya** | **Roll No:** | **16010122096** |

| **Title:Introduction to Open Web Application Security Project and implementation**  **of XSS.** |
| --- |

| **Objectives:** |
| --- |
| 1. Understanding Cross-site scripting (XSS). 2. Understanding and exploring the concept of DVWA. 3. Exploration of vulnerabilities for web based applications through XSS attack using DVWA. |

| **Expected Outcome of Experiment:** |
| --- |
| **CO3-Identify and analyze web attacks** |

| **Books/ Journals/ Websites referred:** |
| --- |
| * <http://www.dvwa.co.uk/> * <https://ensurtec.com/dvwa-part-2-exploiting-cross-site-scripting-xss-vulnerabilities/> * https://[www.youtube.com/watch?v=ivvTrTie16I](http://www.youtube.com/watch?v=ivvTrTie16I) * https://www.youtube.com/watch?v=1WFEVpyhRRQ |

| **Pre Lab/ Prior Concepts:** |
| --- |
| 1. Basic understanding of web technologies (HTML, CSS, JavaScript). 2. Familiarity with client-server architecture. 3. Knowledge of HTTP requests and responses. 4. Basics of web security principles and vulnerabilities. |

| **New Concepts to be learned:** |
| --- |
|  **OWASP Overview:**   * Purpose and goals of OWASP. * OWASP Top 10 vulnerabilities. * Importance of web application security.    **Cross-Site Scripting (XSS):**   * What is XSS? * Types of XSS attacks (Stored, Reflected, DOM-based). * How attackers exploit XSS vulnerabilities.    **XSS Attack Implementation:**   * Setting up a vulnerable web application. * Injecting malicious scripts. * Capturing user data through XSS.    **XSS Prevention Techniques:**   * Input validation and sanitization. * Content Security Policy (CSP). * HTTP-only cookies and secure headers.    **Practical Tools and Environment:**   * Using OWASP ZAP (Zed Attack Proxy). * Burp Suite for vulnerability testing. * Setting up a sandbox environment for testing. |

| **Abstract:** |
| --- |
| The main goals of DVWA are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.  We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA, it is not our responsibility, it is the responsibility of the person/s who uploaded and installed it. |

| **Related Theory:** |
| --- |
| OWASP (Open Web Application Security Project) is a non-profit organization that focuses on improving software security. OWASP's mission is to make software security visible so that individuals and organizations can make informed decisions about true software risks.  The OWASP Top 10 is a regularly updated document that lists the top 10 most critical web application security risks. The document is widely used as a standard for evaluating the security of web applications. It includes risks such as injection attacks, cross-site scripting (XSS), broken authentication and session management, security misconfiguration, and insufficient logging and monitoring.  In addition to the OWASP Top 10, OWASP provides a wide range of resources for developers, security professionals, and organizations. These resources include guidelines, tools, and documentation to help improve the security of software applications. OWASP also organizes conferences, local chapter meetings, and training events to promote awareness and education on software security.  DVWA (Damn Vulnerable Web Application) is a web application that is deliberately designed to be vulnerable to a range of common web application attacks. It is intended to be used as a training tool for web developers and security professionals to learn and practice identifying and exploiting common web application vulnerabilities.  DVWA includes a variety of vulnerabilities, such as SQL injection, cross-site scripting (XSS), command injection, file inclusion vulnerabilities, and more. Users can select the level of difficulty and choose which vulnerabilities to practice exploiting.  Using DVWA can help developers and security professionals gain a better understanding of how web application attacks work, and how to prevent them. It can also be used to test web application security tools and techniques.  It is important to note that DVWA should only be used in a controlled, safe environment for educational purposes. Using it in any other way could result in security vulnerabilities in real-world applications. |

| **Implementation Details:** |
| --- |
| **Enlist all the Steps followed and various options explored** In this experiment, we will be do the following:  1. **XSS Attack 1: Hijacking the user’s session**  XSS Attack 2: Perform unauthorized activities.  1. **XSS Attack 3: Phishing to steal user credentials.**  XSS Attack 4: Capture the keystrokes by injecting a keylogger.  1. **XSS Attack 5: Stealing sensitive information.**   DVWA security set to low   Vulnerability -XSS Stored Exploit Since there is a limit of letters to add letters in the name field so add a alert. Session ID  Vulnerability - XSS Reflected Exploit    Display cookie session:  With medium security - input for name field restricted to 10  text field length = 100  Page source   with high security level also the character restriction is 10 .   With <script>alert(xss)</alert>    Since script tag does not change so using another tag <img>  Dvwa - cross site request forgery (CSRF)  Admin password changed from password to pass  XSS Reflected:    Received the dvwa xss reflected request with the name field as test        Here changed the name field from test to a script payload for displaying an alert: <script>alert(‘XSS\_ATTACK’)</script>    XSS Stored:      Received dvwa xss stored request with txtname test1    Received dvwa xss stored request with txtname test1        Here changed the txtname field from test1 to a script payload for displaying alert: <script>alert(‘XSS\_ATTACK’)</script> |

| **Conclusion:** |
| --- |
| We explored vulnerabilities for web based applications through XSS attacks using DVWA & Burpsuite. |