

**Assignment 1:**

Name : Muhammad Talha Yaseen (231450476)

Subject: Information Security

Section: A

Submitted To: Dr. Saad Bin Saleem

**Report on Website Attack Using SQL Injection**

**Introduction:**

During this exercise, I conducted an attack on a website using SQL injection technique with the help of SQLmap tool. The aim of the attack was to gain unauthorized access to the website's database and extract sensitive information. In this report, I will describe the steps taken during the attack and the results obtained.

**Attack Process:**

To begin the attack, I used SQLmap tool with the following command:

sqlmap -u testphp.vulnweb.com/artists.php?artist=1 –dbs

This command was used to identify the available databases on the website. The system displayed two databases, namely 'acuart' and 'information\_schema'. For further analysis, I decided to use 'acuart' and identified its tables using the following command:

sqlmap –u testphp.vulnweb.com/artists.php?artist=1 –D acuart –tables

This command helped me identify the 'products' table, which I then used to extract the data using the following command:

sqlmap –u testphp.vulnweb.com/artists.php?artist=1 –D acuart –T products –columns

The result was the list of all columns and their data types present in the 'products' table.

In addition to these commands, I also used two other commands during the attack:

sqlmap -u "http://testsite.com/login.php" --tor --tor-type=SOCKS5

This command was used to route the attack traffic through the Tor network, which provided an additional layer of anonymity.

sqlmap -u "http://testsite.com/login.php" --time-sec 15

This command was used to set the timeout for SQLmap to 15 seconds, which helped to speed up the attack process.

**Results:**

The attack was successful in identifying the databases and tables present on the website. By exploiting SQL injection vulnerability, I was able to extract sensitive information from the 'products' table. The extracted information included the list of all products and their details. The attack was performed with the intention of highlighting the vulnerabilities present in the website's database security.

**Conclusion:**

SQL injection attacks are a serious threat to the security of websites and databases. It is important for website owners to take necessary measures to protect their databases from such attacks. This report highlights the importance of regular security audits and vulnerability testing to ensure the safety of website databases.