**SQL Injection**

The most basic way to describe a database is a table (or tables) of data. Data in these tables are stored in a defined structure, utilizing indexing to facilitate highly efficient query performance.

SQL (Structured Query Language) is utilized for interacting with databases.

**How to inject SQL injection?**

Suppose an application allows users of a public web page to check their marketing preferences by entering their email addresses.

When a user searches for their preferences, their email address is inserted directly into the query; for example, if their email were test@email.com the SQL query would look like:

**SELECT \* FROM user\_preferences WHERE email = 'test@email.com';**

By injecting additional SQL code into the statement retrieving data, you can return a list of all email addresses that use this web page rather than just the details for your email.

**SELECT \* FROM user\_preferences WHERE email = ‘test@email.com’ OR ‘1’==’1’;**

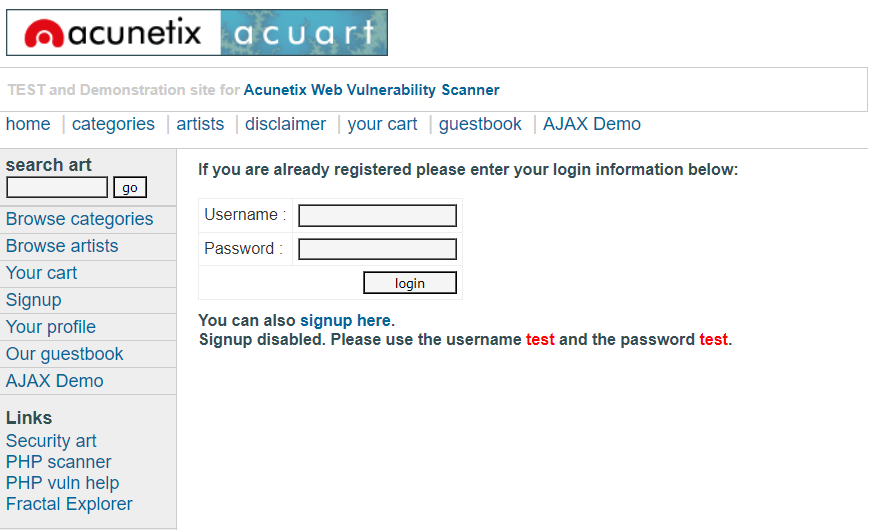
As the input is not sanitized, you can pass additional SQL code into this query above by closing off the string with a single apostrophe mark (') and entering your own SQL. Using Boolean logic, you want the statement to evaluate as accurate. This will allow you to return all rows instead of just one. An example of Boolean logic is OR 1=1 (since 1=1 is always authentic; all items will be returned).

Original user input: **test@email.com**

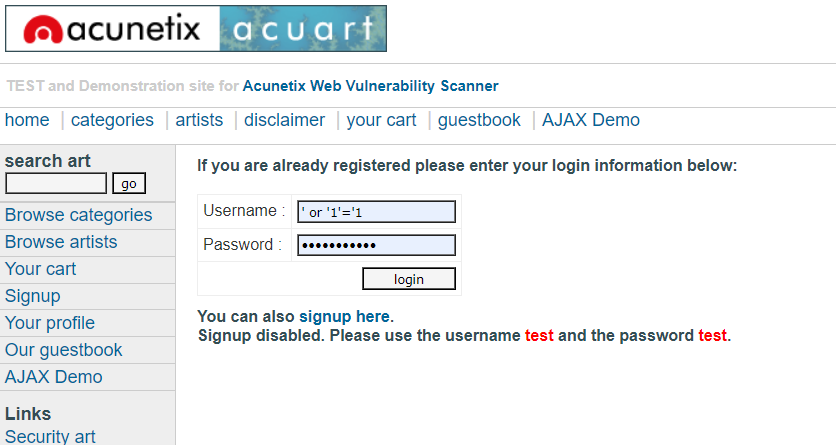
Malicious user input: **test@email.com’ OR ‘1’==’1**

**Walkthrough of target site: login page (vulnweb.com)**

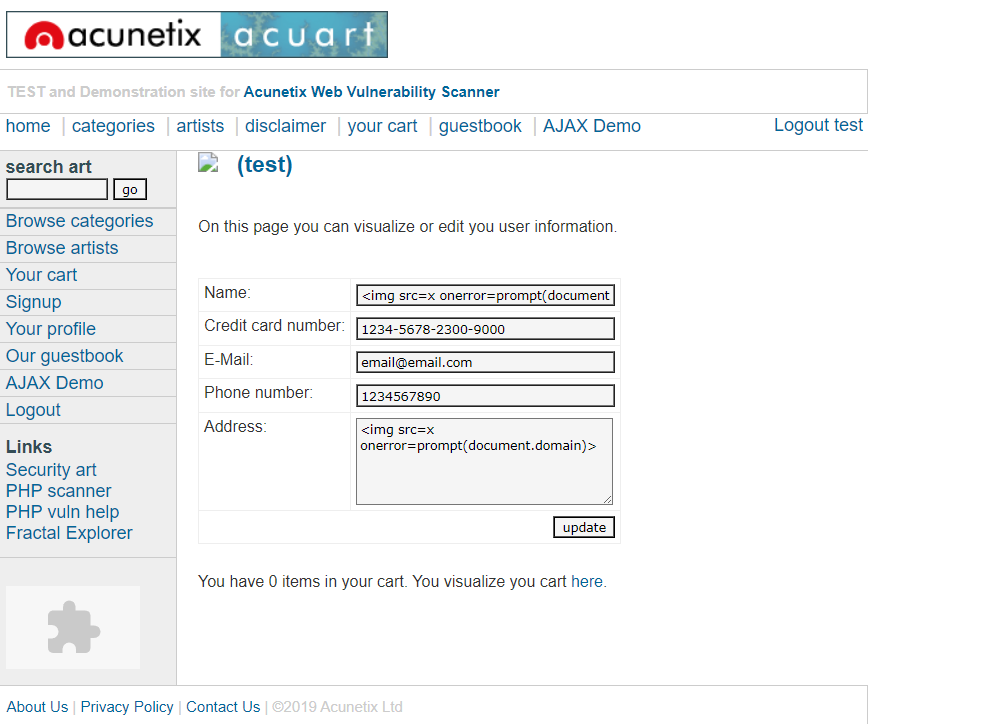
1. Go to the target URL: http://testphp.vulnweb.com/login.php

****

1. Write the command **‘ or ‘1’=’1** in both username and password field.

****

1. We can see we were successfully able to exploit and login in into the site using SQL injection.

****

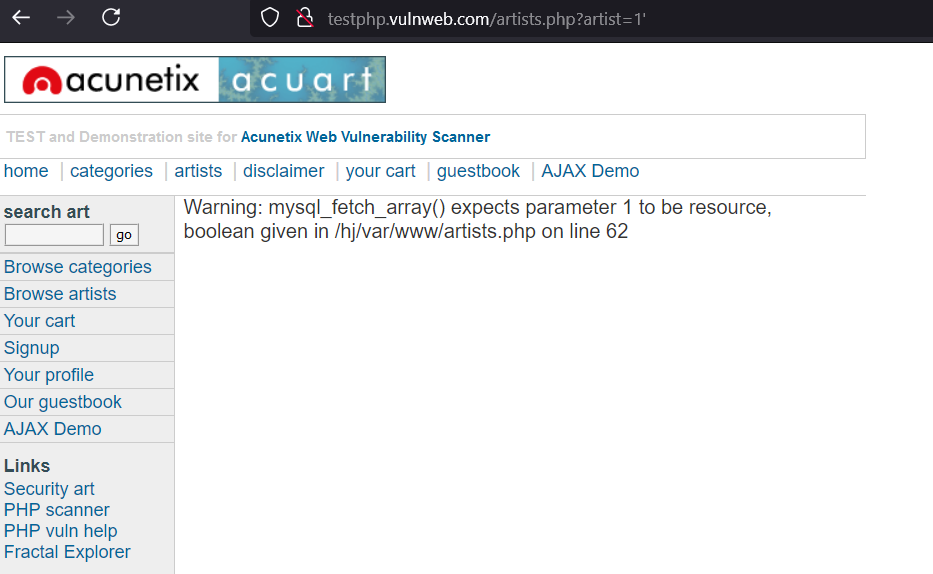
**Enumerating the database**

When exploiting SQL injection vulnerabilities, it's often necessary to find further information on the database itself, such as the type/version of the database software and the database structure (in terms of columns and tables contained within).

**Target URL:** [**http://testphp.vulnweb.com/artists.php?artist=1**](http://testphp.vulnweb.com/artists.php?artist=1)

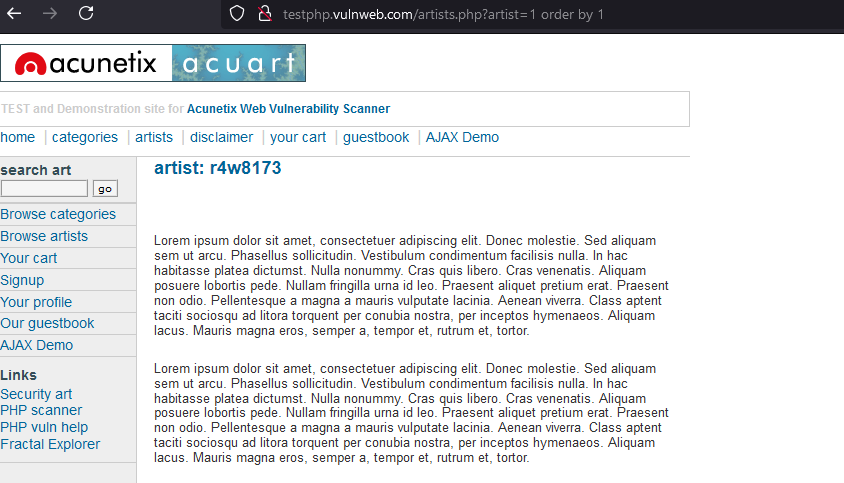
1. We broke the developers code and saw an error message which shows that SQL injection might be possible here.

**testphp.vulnweb.com/artists.php?artist=1'**



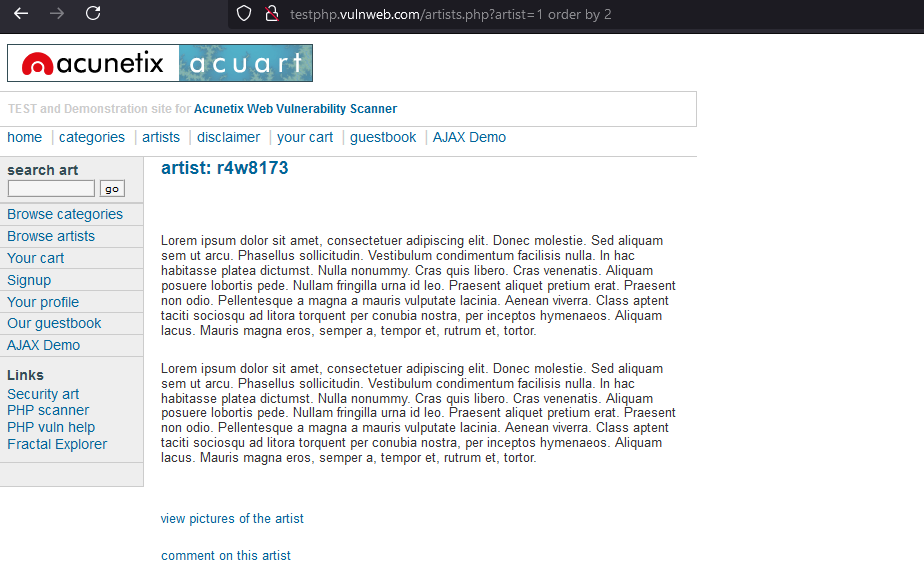
1. In order to query the database on any of this information, you must first find out how many columns the original table being queried has.

[**http://testphp.vulnweb.com/artists.php?artist=1%20order%20by%201**](http://testphp.vulnweb.com/artists.php?artist=1%20order%20by%201)



1. The number in this query can then be incremented until you are met with an error. This error means you've gone too far and that the actual number of columns is the number entered before an error is thrown. Here we increase the order by 1.

**http://testphp.vulnweb.com/artists.php?artist=1%20order%20by%202**



1. We increase one more.

[**http://testphp.vulnweb.com/artists.php?artist=1%20order%20by%203**](http://testphp.vulnweb.com/artists.php?artist=1%20order%20by%203)



1. Here we got thrown an error meaning that we have just cross the actual number of columns. So, we can conclude that the no. of column in the table is 3.

**http://testphp.vulnweb.com/artists.php?artist=1%20order%20by%204**



1. The SQL UNION operator combines the result sets of two or more SELECT statements into a single result set, eliminating duplicate rows. In order for a UNION query to work, there must be an equal number of columns in each of the SELECT statements, and the corresponding columns in each query must have the same data type.

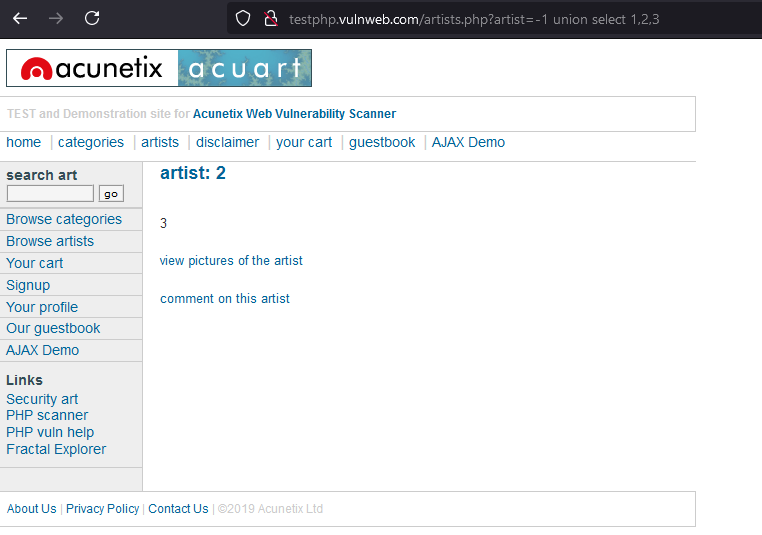
**http://testphp.vulnweb.com/artists.php?artist=1%20union%20select%201,2,3**



1. Make the first SQL query invalid by moving the pointer to the undefined row i.e. -1.

Here we used a negative number as we know that row cannot be negative.

[**http://testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,2,3**](http://testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,2,3)



1. The queries and data that can be discovered vary according to the software the database is built upon. For example, the syntax for finding the database for a few popular database types are listed below:

Microsoft/MySQL SELECT @@version

Oracle DB SELECT \* FROM v$version

PostgreSQL SELECT version()

@@version can be replaced with a number of different commands, depending on what you want to retrieve from the database; for example, @@hostname or @@datadir.

[**http://testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,database(),version()**](http://testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,database(),version())

