CYBR 3510 "Systems Security"

SQL Injection Exploitation

Please read the document of SQL injection Exploitation.pdf and using the <http://testphp.vulnweb.com/index.php> website to complete this lab.

Please record the injected sql statement and the screenshot of obtained results in each step.

1. Identify the SQL vulnerability and determine what DBMS is used by this web application.

<http://testphp.vulnweb.com/artists.php?artist=1>

Input is being parsed as part of the query.

1. Using the “ORDER BY” command to find the number of columns that is included in that web form of <http://testphp.vulnweb.com/artists.php?artist=1>

A screenshot of a computer

Description automatically generated 3

1. Using the “Union” function to find the number of columns that is included in the above form. A screenshot of a computer

   Description automatically generated 3 columns
2. Identify the column that can be used to present the result of injected code.

A screenshot of a computer

Description automatically generated 2 and 3

1. Find the version of the DBM and the database name that is currently connected.

A screenshot of a computer

Description automatically generated

1. Find names of all tables that reside in the acuart database.

A screenshot of a computer

Description automatically generated

1. Find all the column names in the table “users”.

A screenshot of a computer

Description automatically generated

1. Find all usernames and passwords that in the table “users”.

A screenshot of a computer

Description automatically generated

1. Find the number of columns that returned by the original SQL statement of the following URL <http://testphp.vulnweb.com/product.php?pic=2>

A screenshot of a computer

Description automatically generated11

1. Find names of all the databases/schemas of this web application.

A screenshot of a computer

Description automatically generated

1. Try to obtain 5 extra information from the acuart database. (e.g. All the information stored in the product table, all the information in the artists table, columns used in guestbook table.) column 2,3,7,9 are vulnerable