Step by Step Guide of SQL Injection Attack

sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 –dbs

1. sqlmap - It is a popular open-source penetration testing tool that automates the process of detecting and exploiting SQL injection vulnerabilities in web applications.
2. -u - It specifies the target URL of the website that is vulnerable to SQL injection.
3. <http://testphp.vulnweb.com/artists.php?artist=1> - This is the target URL that contains the vulnerable parameter 'artist'.
4. --dbs - This option instructs sqlmap to enumerate the databases that exist on the target server.

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart –columns

1. sqlmap - It is a popular open-source penetration testing tool that automates the process of detecting and exploiting SQL injection vulnerabilities in web applications.
2. -u - It specifies the target URL of the website that is vulnerable to SQL injection.
3. <http://testphp.vulnweb.com/listproducts.php?cat=1> - This is the target URL that contains the vulnerable parameter 'cat'.
4. -D - This option instructs sqlmap to use the specified database for the attack.
5. acuart - This is the name of the database to be used for the attack.
6. --columns - This option instructs sqlmap to enumerate the columns in the tables of the specified database.

In summary, the command is using sqlmap to scan the target URL for SQL injection vulnerabilities and, once it finds one, it is using the specified database to enumerate the columns in the tables of the database.

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C email –dump

1. sqlmap - It is a popular open-source penetration testing tool that automates the process of detecting and exploiting SQL injection vulnerabilities in web applications.
2. -u - It specifies the target URL of the website that is vulnerable to SQL injection.
3. <http://testphp.vulnweb.com/listproducts.php?cat=1> - This is the target URL that contains the vulnerable parameter 'cat'.
4. -D - This option instructs sqlmap to use the specified database for the attack.
5. acuart - This is the name of the database to be used for the attack.
6. -T - This option specifies the table to be targeted by sqlmap.
7. users - This is the name of the table to be targeted by sqlmap.
8. -C - This option specifies the column to be targeted by sqlmap.
9. email - This is the name of the column to be targeted by sqlmap.
10. --dump - This option instructs sqlmap to dump the contents of the specified column.

In summary, the command is using sqlmap to scan the target URL for SQL injection vulnerabilities and, once it finds one, it is using the specified database and table to dump the contents of the specified column. In this case, it is dumping the contents of the 'email' column in the 'users' table of the 'acuart' database.