The following are step-by-step instructions for carrying out an SQL injection attack using sqlmap, a widely used open-source penetration testing tool for detecting and exploiting SQL injection vulnerabilities in web applications:

First, use the sqlmap command followed by the target URL of the website that is vulnerable to SQL injection, with the "--dbs" option to enumerate the databases that exist on the target server.

Then, use the sqlmap command with the target URL containing the vulnerable parameter, followed by the "-D" option to specify the database to be used for the attack, and the "--columns" option to enumerate the columns in the tables of the specified database.

Finally, use the sqlmap command with the target URL, "-D" option, "-T" option to specify the table to be targeted, "-C" option to specify the column to be targeted, and "--dump" option to dump the contents of the specified column.

In summary, these steps involve using sqlmap to scan the target URL for SQL injection vulnerabilities and, once one is found, using the specified database, table, and column to dump its contents. For example, one could dump the email addresses of users in the 'users' table of the 'acuart' database by specifying the relevant options in the sqlmap command.