1. SQL
   1. Explain the string you used for the SQL injection and explain why it works.

The string I used for username and password was 1’ OR ‘1’ = ‘1. With 1’ OR ‘1’ = ‘1, the SQL statement at the server becomes

*SELECT \* FROM accounts WHERE username= ‘1’ or ‘1’=’1’ AND password=’1’ or ‘1’=’1’*

As ‘1’=’1’ is always true, the above statement will just return all the values.

* 1. What is the table name used to display user details?

The table name used to display user details was *accounts*.

* 1. What are the fields in this table?

The fields in the *accounts* table include *Username*, *Password* and *Signature*.

1. XSS
   1. Explain which content you inserted in the second order attack, and how it works
   2. Explain the flask script you wrote to create the POST request for the first-order attack
2. Injection
   1. Explain which command you used to obtain the content of “/etc/passwd”, and why it works
   2. Explain which command you used to obtain the reverse shell, and why it works