Q1/4

You are performing a hacking practice on a given website. The first step you performed was to check if a URL parameter is vulnerable to SQLi by applying a single quote to the end of a parameter value like this:
news?id=5666'
Why would you do so?

A	If 5666 is going into an SQL statement, it will cause an error. This corresponds to a vulnerability and can be exploited.	✓

Well done. Correct Answer.

Explanation:
If we apply a single quote and the website's responds with some error there is a chance that its due to the ' causing an error in the SQL statement. Whereas, if we put the single quote and nothing happens, i.e. response is completely the same, then there is a high chance that that specific parameter isn't vulnerable to SQL injection. Hence, putting ' as the first step can tell us a lot of things.

B	' is used to make any application vulnerable to SQL injection.

Q2/4

Consider the injection scenario: select * from test where id='HERE' What ever you write in the parameter replaces HERE. Which of the following cannot be used to run an OR condition?

A	Bla' or 'a'='a
B	' or 88=88--+
C	' or 'x'='x'--+
D	' or 5=5-- ✓

Well done. Correct Answer.

Explanation:
Double hyphens are always sent using a space at the end of the query. Generally, we cannot send space in the URL's, and for this reason these are sent as --+.

Q3/4

Which of the following statements are true while using UNION?

A For union to work, both select statements should have the same number of columns.

B Union can be used for exploiting sql injection vulnerabilities.

C The syntax for union command is: SELECT a1,a2,a3...aN FROM x UNION SELECT b1,b2,b3....bN FROM Y

D All of the above ✓

Well done. Correct Answer.

Explanation:
UNION based SQL injections are used to exploit vulnerabilities and it requires same number of columns to be present in both the Select statements.

Q4/4

There are several problems while using UNION based SQL injections. Which of the following corresponds to these problems?

A Finding number of columns in a website, which is not showing SQL error

B Finding names of the columns and table to UNION

C Both (a) and (b) ✓

Well done. Correct Answer.

Explanation:
There are several issues faced while using UNION based SQL injections. If, we do not know the names of table and columns, then UNION can't be used. If, a website is not showing an SQL error, it becomes very difficult to find number of columns and without finding number of columns, UNION can't be used.

D None of the above

Now that we have come to the end of this topic, you should be able to:

1. Understand SQL queries via GET parameters
2. Perform basic union based SQL Injections
3. Understand basic challenges faced during union based SQL injections

If you have doubts regarding any of the above-mentioned points, please go through the videos again.