Q1/6

Following is the sql query which is vulnerable to sql injection:
SELECT * FROM students where id=1
You want to test AND 1=1, what will be the payload?

A ' AND 1=1

B " AND 1=1

C AND 1=1

Well done. Correct Answer.

Explanation:
As we see that in the sql query there is no single quote used (id is an integer). If there is no single quote we don't need to close any single quote or we don't need to close any double quote, to do an injection we simply use AND1=1 hence option 3.

D None of the above

Q2/6

An injection where we ask yes/no questions to the SQL using AND/OR is called _____.

A Time based blind injection

B Error based SQL injection

C Boolean based blind injection ✓

Well done. Correct Answer.

Explanation:
When testing for Boolean Based SQL injection we first ask the website to evaluate a true condition (and 1=1) and then a false condition (and 1=0). If the website responds differently to true and false with respect to the response length being 10000 when we ask a true question and 259 when we ask a false question, we can then use that information to ask things we don't know about, like if the length of the database name is 6 (and length(database())=6). If the response length is 10000, we would know that the length is indeed 6 else we can try a different length.

72% students get this answer correct at their first attempt

D None of the above

Q3/6

Time based blind injections are useful when we can do SQL injection easily and we can extract data on the website as text in HTTP response.

A True

B False ✓

Well done. Correct Answer.

Explanation:
Time based injections are the last resort. They are used when none of the other injections are working. In Time based injections, we ask the website yes/no questions but unlike boolean based injections where website gives bigger response in case of true statement and smaller response or error in case of false statement, time based injections always give the same response but in different time. Attacker tells the website to respond after x second,s if the asked question is true and y seconds if it is false. Upon looking at the response time, the attacker then knows whether the question he asked was true or false.

Q4/6

If a website is only exploitable using Time based injection, what is the response for the following queries:
A : id=1 AND (if 1=1 then sleep for 10 seconds)--+
B : id=1 AND (if 1=0 then sleep for 10 seconds)--+
Note: If we only submit id=1 i.e no sqli payload, the response is the text: "Hello"

A — A and B both return hello ✓

Well done. Correct Answer.

Explanation:
We need to perform time based injections when we know the website doesn't respond differently for either TRUE or FALSE condition. In the case of A where 1=1 the response time will be delayed by 10 seconds and response will be Hello. In the case of B where 1=0 the response will also be Hello but the response time will not be delayed by 10 seconds because as mentioned above the website is exploitable using Time based injection in which the website doesn't respond differently for TRUE or FALSE condition. If there is a change in the response time we would have tried boolean based injection instead of time based.

30% students get this answer correct at their first attempt

B — A returns hello

C — B returns hello

D — None of the above

Q5/6

When we insert a single quote on a website and we get an error saying "You have an SQL syntax error near the character" (Standard MySql error). What kind of injections are possible

A Error based injection

B Time based injection

C Boolean Based injection

D All of the above

Well done. Correct Answer.

Explanation:
As the website is showing complete MySQL error, Error based injection is the easiest to do but that does not mean that other injections are not possible as time and boolean based injections even work when SQL error is not shown at all but injection still exists.

Q6/6

Consider we are doing error based injection and we put the following payload
convert(int,(select 255*2)).
What will be the response?

A Cannot convert string value select 255*2 into int

B select 255*2

C No error

Well done. Correct Answer.

Explanation:
The convert function tries to convert the second parameter into the data type of first parameter. Here the second parameter is (select 255*2) and the output data type is int. But here we will not put (select 255*2) into single quotes, this means this will be executed. Now once this is executed the output is 255*2 which is 510. Now the sql injection will try to convert into an integer, and that is the reason the output is 'No error'.

D (select 255*2)

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

1. Understand the basic reasoning behind Error based SQL Injections, Boolean based SQL Injections and Time based SQL Injections.

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