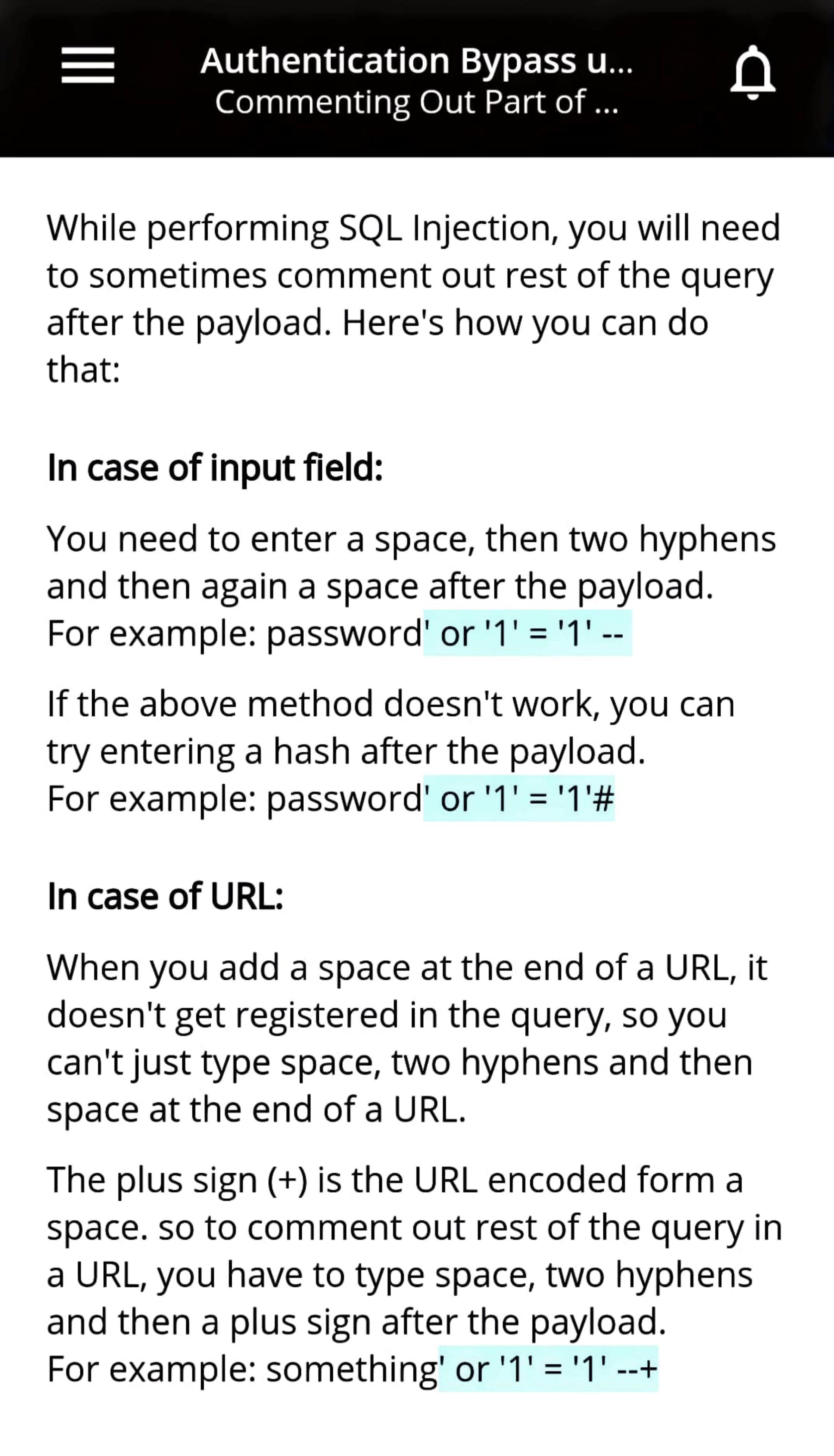
SQL injection

```
SELECT * FROM users WHERE username='x' AND password='y' OR 'a'='a'
```

Authentication Bypass

```
SELECT * FROM users WHERE username='x' AND password='y' OR'a'='a'
```



While performing SQL Injection, you will need to sometimes comment out rest of the query after the payload. Here's how you can do that:

In case of input field:

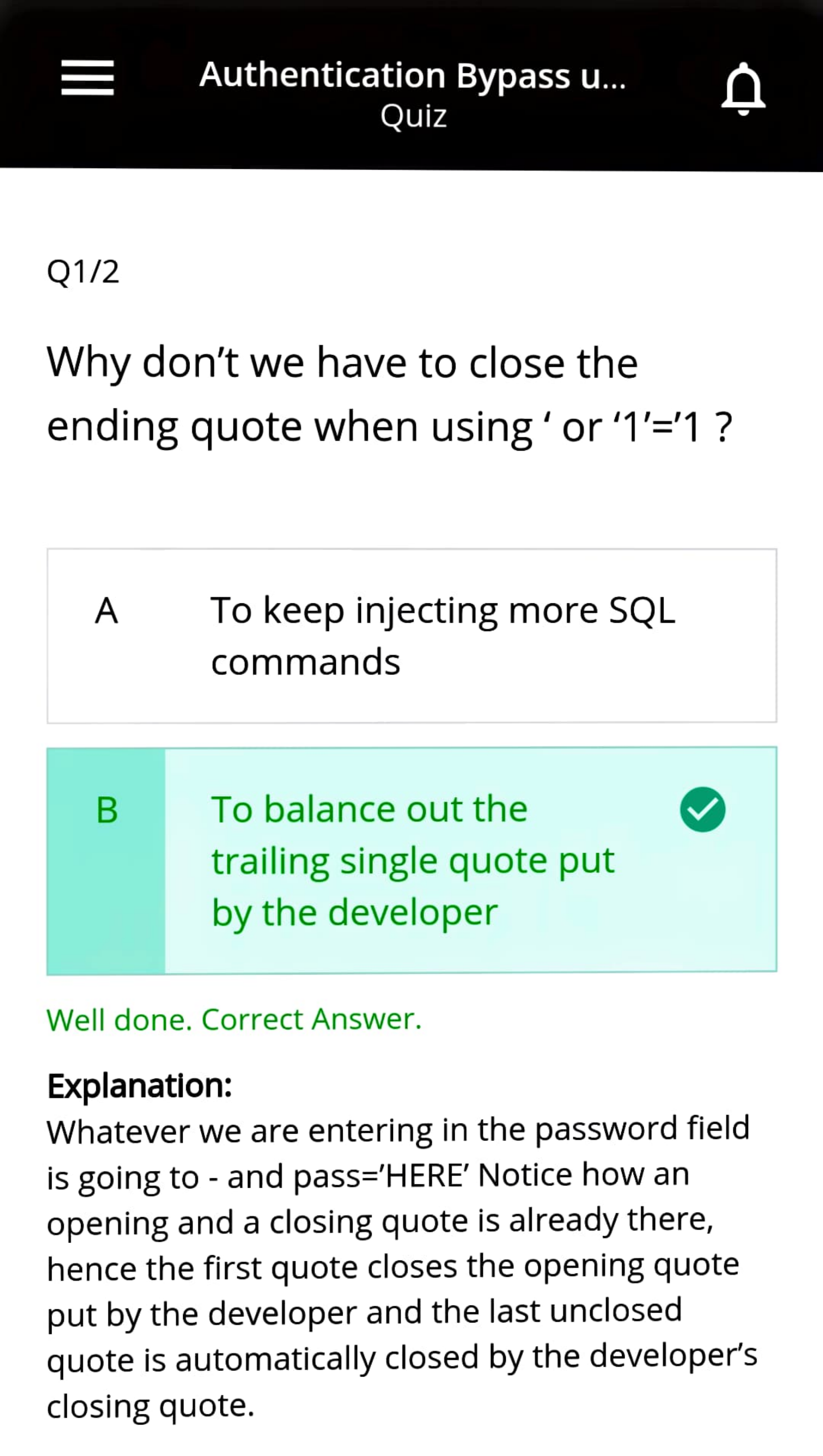
You need to enter a space, then two hyphens and then again a space after the payload.
For example: password' or '1' = '1' --

If the above method doesn't work, you can try entering a hash after the payload.
For example: password' or '1' = '1'#

In case of URL:

When you add a space at the end of a URL, it doesn't get registered in the query, so you can't just type space, two hyphens and then space at the end of a URL.

The plus sign (+) is the URL encoded form a space. so to comment out rest of the query in a URL, you have to type space, two hyphens and then a plus sign after the payload.
For example: something' or '1' = '1' --+



Authentication Bypass u...
Quiz

Q1/2

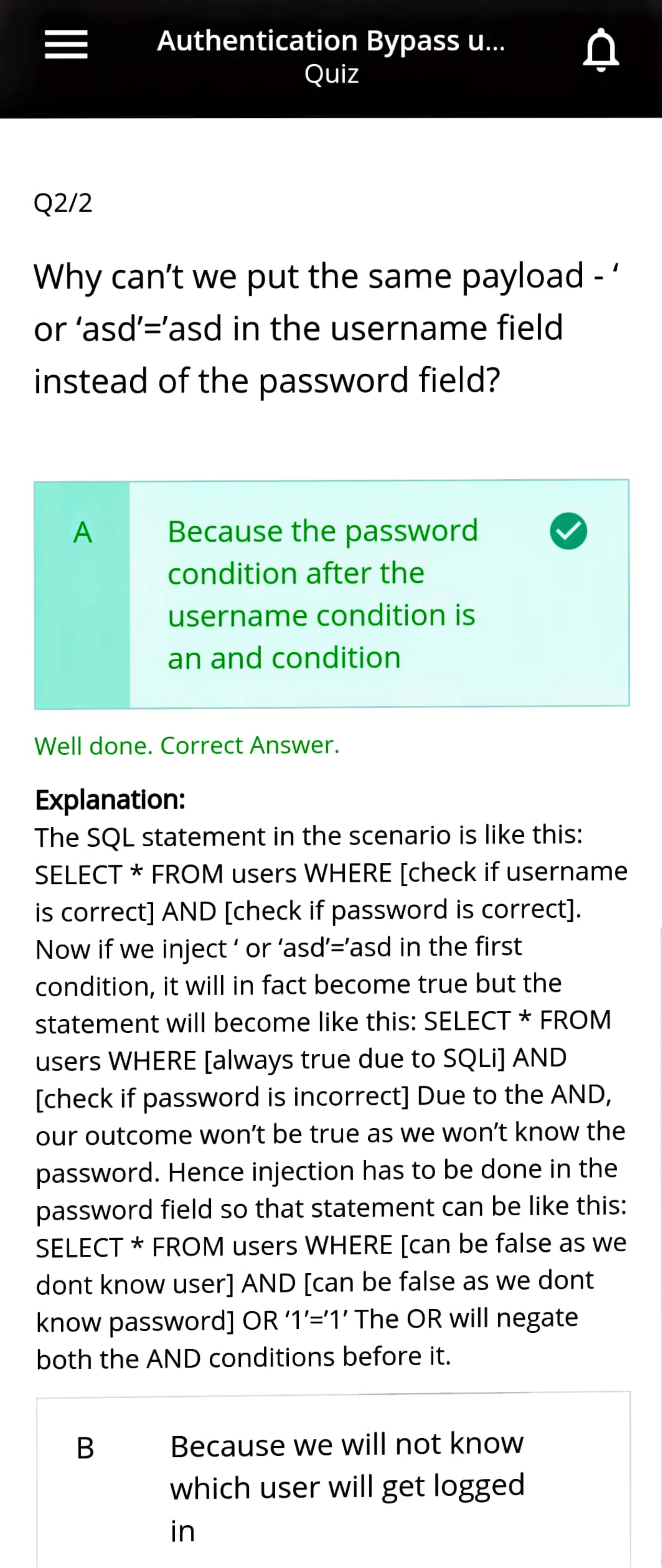
Why don’t we have to close the ending quote when using ‘ or ‘1’=’1 ?

A To keep injecting more SQL commands

B To balance out the trailing single quote put by the developer ✓

Well done. Correct Answer.

Explanation:
Whatever we are entering in the password field is going to - and pass=’HERE’ Notice how an opening and a closing quote is already there, hence the first quote closes the opening quote put by the developer and the last unclosed quote is automatically closed by the developer’s closing quote.



Q2/2

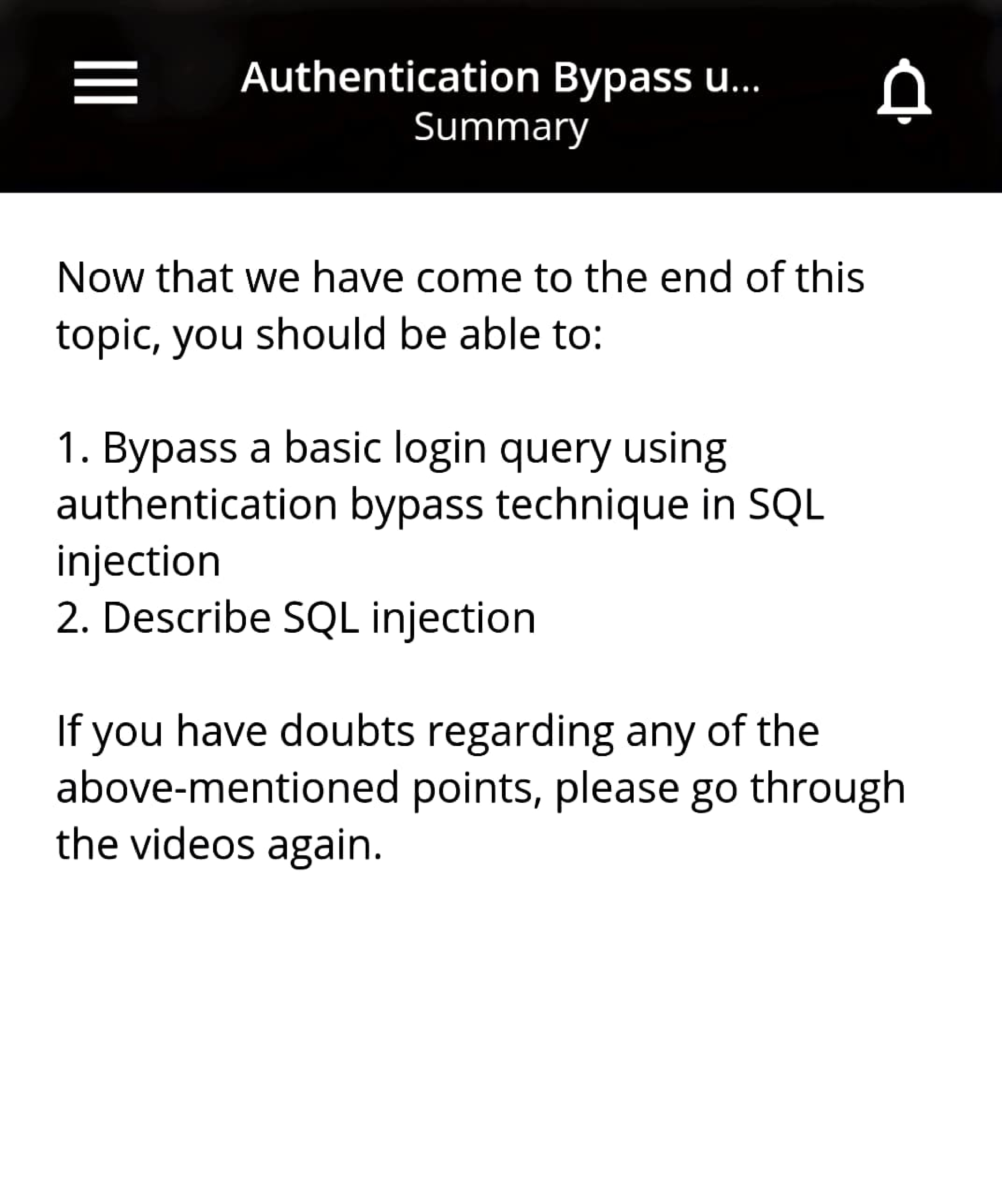
Why can’t we put the same payload - ‘ or ‘asd’=’asd in the username field instead of the password field?

A Because the password condition after the username condition is an and condition ✓

Well done. Correct Answer.

Explanation:
The SQL statement in the scenario is like this: SELECT * FROM users WHERE [check if username is correct] AND [check if password is correct]. Now if we inject ‘ or ‘asd’=’asd in the first condition, it will in fact become true but the statement will become like this: SELECT * FROM users WHERE [always true due to SQLi] AND [check if password is incorrect] Due to the AND, our outcome won’t be true as we won’t know the password. Hence injection has to be done in the password field so that statement can be like this: SELECT * FROM users WHERE [can be false as we dont know user] AND [can be false as we dont know password] OR ‘1’=’1’ The OR will negate both the AND conditions before it.

B Because we will not know which user will get logged in



Authentication Bypass u...

Summary

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

1. Bypass a basic login query using authentication bypass technique in SQL injection
2. Describe SQL injection

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