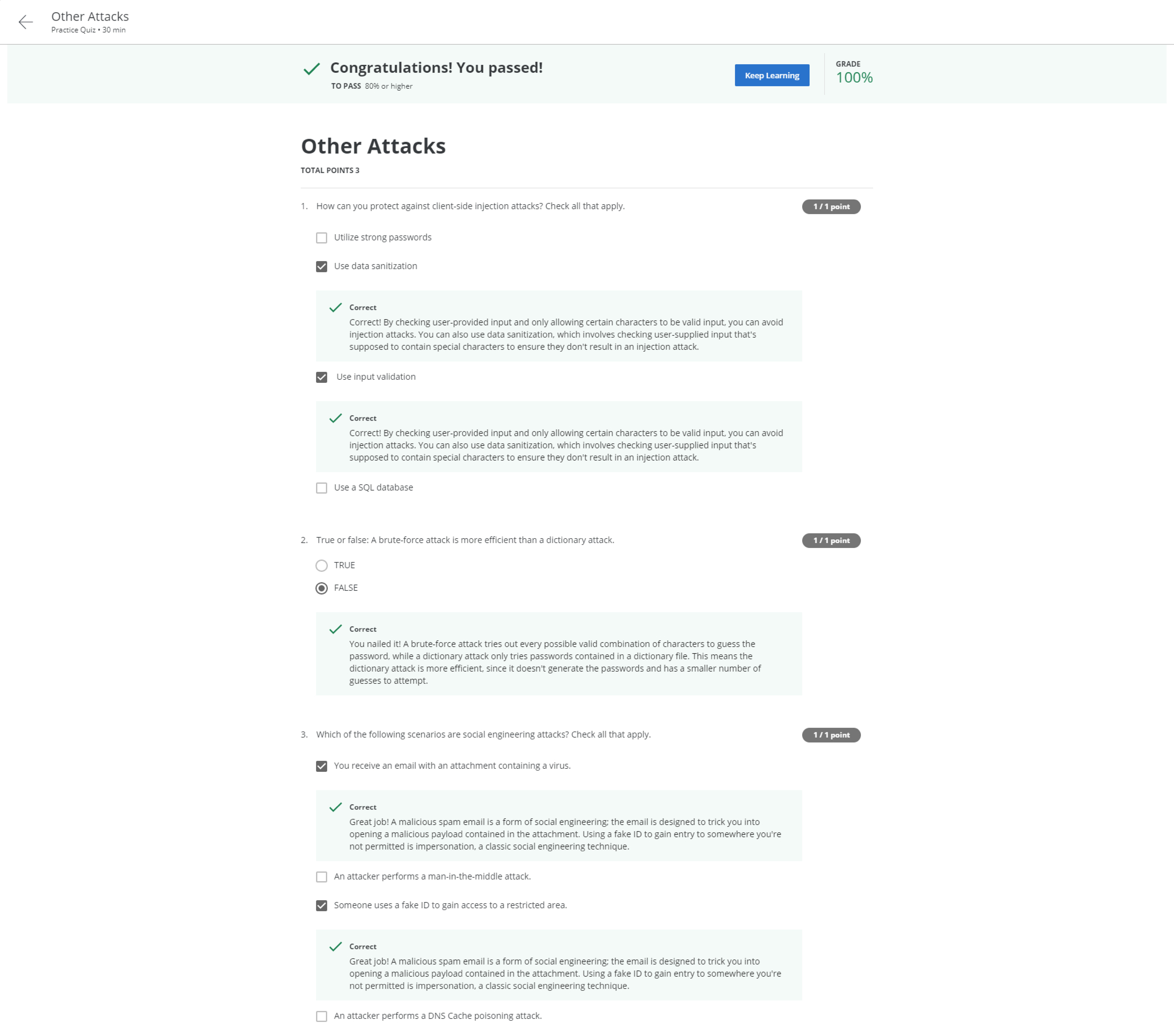

✓ Congratulations! You passed!

TO PASS 80% or higher

GRADE
100%

Other Attacks

TOTAL POINTS 3

1. How can you protect against client-side injection attacks? Check all that apply.

1 / 1 point

□ Utilize strong passwords

☑ Use data sanitization

✓ Correct

Correct! By checking user-provided input and only allowing certain characters to be valid input, you can avoid injection attacks. You can also use data sanitization, which involves checking user-supplied input that's supposed to contain special characters to ensure they don't result in an injection attack.

☑ Use input validation

✓ Correct

Correct! By checking user-provided input and only allowing certain characters to be valid input, you can avoid injection attacks. You can also use data sanitization, which involves checking user-supplied input that's supposed to contain special characters to ensure they don't result in an injection attack.

□ Use a SQL database

2. True or false: A brute-force attack is more efficient than a dictionary attack.

1 / 1 point

○ TRUE

● FALSE

✓ Correct

You nailed it! A brute-force attack tries out every possible valid combination of characters to guess the password, while a dictionary attack only tries passwords contained in a dictionary file. This means the dictionary attack is more efficient, since it doesn't generate the passwords and has a smaller number of guesses to attempt.

3. Which of the following scenarios are social engineering attacks? Check all that apply.

1 / 1 point

☑ You receive an email with an attachment containing a virus.

✓ Correct

Great job! A malicious spam email is a form of social engineering; the email is designed to trick you into opening a malicious payload contained in the attachment. Using a fake ID to gain entry to somewhere you're not permitted is impersonation, a classic social engineering technique.

□ An attacker performs a man-in-the-middle attack.

☑ Someone uses a fake ID to gain access to a restricted area.

✓ Correct

Great job! A malicious spam email is a form of social engineering; the email is designed to trick you into opening a malicious payload contained in the attachment. Using a fake ID to gain entry to somewhere you're not permitted is impersonation, a classic social engineering technique.

□ An attacker performs a DNS Cache poisoning attack.