### 1.

Question 1

Why is communicating over HTTPS more secure than HTTP?

1 / 1 point

There is client-side encryption and server-side decryption

There is only server-side encryption and client-side encryption

Encryption and decryption are performed both on the client- and server-side.

Both client- and server-side are encrypted but decryption is not performed.

Correct

Correct! HTTPS is secure which means that there is encryption for data exchanged both at client- and server-side which can also be decrypted.

### 2.

Question 2

Which of the following HTTPS methods is used to partially update data?

1 / 1 point

PUT

POST

GET

PATCH

Correct

Correct! PATCH is used to partially updating a resource.

### 3.

Question 3

Which of the following HTTP status codes inside the response header indicate server-side errors?

1 / 1 point

300-399

400-499

100-199

500-599

Correct

Correct! The status codes mentioned are used to indicate server-side errors to the client inside the response headers.

### 4.

Question 4

RESTful APIs are considered to be stateless. What this means is the state is saved \_\_\_\_\_\_\_\_.

1 / 1 point

Both on client and server

On neither the client- nor server-side

Only on the server

Only with the client

Correct

Correct! The server does not contain any state of the API client making the request and cannot identify who is making the request.

### 5.

Question 5

Which of the following can be a layer in the RESTful API communication system that data encounters while being passed between the client and server? Select all that apply.

1 / 1 point

Firewall

Correct

Correct! Firewalls are security systems over the network that help control and monitor the network traffic between the client and server based on security rules.

Headers

Load balancer

Correct

Correct! Load balancers help in the efficient distribution of network traffic before the requests from client reach the server.