Quiz 4

Deadline	Tuesday, 09 June 2020 at 6:00PM
Latest Submission	*no submission yet*
Maximum Mark	5

Question 1 (1 mark)

Among the issues of using HTTP Basic for authentication in REST API security

(a) ○	The password is sent over the network in base64 encoding which can be converted back to plain text
(b) ○	The password is sent repeatedly, for each request (i.e. larger attack window)
(c) ○	All of the above mentioned

Question 2 (1 mark)

Which statement is NOT true in regard to using Json Web Token (JWT)

(a) ○	the token is self contained
(b) ○	the token is meant to be short live (i.e. expire)
(c) ○	Using JWT invalidate the Statelessness of our REST API

Question 3 (1 mark)

In Oauth, the scope of resources/operations the third party is permitted to access is NOT customizable in the development phase of the API.

(a) ○	true
(b) ○	false

Question 4 (1 mark)

As best practice in securing your REST API, you should restrict HTTP methods by

(a) ○	Whitelisting permitted methods
(b) ○	Black-listing not permitted methods
(c) ○	use API keys for authentication

Question 5 (1 mark)

When transferring sensitive data in your REST API GET request (e.g., API key), the sensitive data should be transferred in

(a) ○	the Header
(b) ○	the URL
(c) ○	a parameter in the URL