



Full Name: Kenneth Choi

Email: kennethichoi@gmail.com

Test Name: **MBA: Security**

Taken On: 2 Aug 2019 11:02:18 PDT

Time Taken: 9 min 56 sec/ 10 min

Work Experience: 1 years

Invited by: Jeff

Invited on: 2 Aug 2019 10:57:44 PDT

Tags Score:

| | |
|-----------|----------|
| Essential | 42.62/50 |
| SQL | 5/5 |
| Security | 42.62/50 |
| XSS | 5/5 |

85.2%

42/50

scored in **MBA: Security** in 9 min 56 sec on 2 Aug 2019 11:02:18 PDT

Recruiter/Team Comments:

No Comments.

| Question Description | Time Taken | Score | Status |
|---|--------------|---------|--------|
| Q1 Which of the following can leave a website vulnerable to Cross-Site Scripting (X > Multiple Choice | 34 sec | 5/ 5 | ✓ |
| Q2 In order to keep application secrets (api keys, hash secrets, etc) safe, develop > Multiple Choice | 40 sec | 0/ 5 | ✗ |
| Q3 A server is vulnerable to SQL injection when _____. > Multiple Choice | 3 min 53 sec | 5/ 5 | ✓ |
| Q4 Which of the following make it more difficult to execute a Man in the Middle att > Multiple Choice | 34 sec | 5/ 5 | ✓ |
| Q5 Storing passwords in plain text in a database _____. > Multiple Choice | 24 sec | 5/ 5 | ✓ |
| Q6 In the event that a database is compromised, storing a salted hash of a password > Multiple Choice | 20 sec | 5/ 5 | ✓ |
| Q7 In order to help protect user's data, which of the following make a user's accou > Multiple Choice | 19 sec | 3.33/ 5 | ⚠ |
| Q8 Which of the following are ways in which a hacker could steal user information? > Multiple Choice | 34 sec | 4.29/ 5 | ⚠ |
| Q9 Which kind of attack floods a server with requests with the intent of blocking t > Multiple Choice | 3 min 15 sec | 5/ 5 | ✓ |



QUESTION 1



Correct Answer

Score 5

Multiple Choice

Security

XSS

Essential

QUESTION DESCRIPTION

Which of the following can leave a website vulnerable to Cross-Site Scripting (XSS) attacks?

CANDIDATE ANSWER

Options: (Expected answer indicated with a tick)

- ☒ ☐ embedding un-escaped user-created text inside a script tag
- ☒ ☐ allowing users to create their own html which is stored and later rendered.
- ☒ ☐ loading un-escaped user-created text into an href value
- ☒ ☐ loading un-escaped user-created text into a DOM element

No Comments

QUESTION 2



Wrong Answer

Score 0

Multiple Choice

Security

Essential

QUESTION DESCRIPTION


In order to keep application secrets (api keys, hash secrets, etc) safe, developers should _____.


CANDIDATE ANSWER


Options: (Expected answer indicated with a tick)


- ☐ store application secrets only in private repositories on GitHub or Bitbucket
- ☒ ☐ never commit application secrets into the source code management
- ☒ ☐ create specific environment variables for each application secret in the production environments
- ☐ store the secrets in an encrypted form and write an encryption/decryption library that runs when the application is first launched.


No Comments


| | |
|---|---|
| QUESTION 3  Correct Answer | Multiple Choice Security SQL Essential |
| Score 5 | QUESTION DESCRIPTION A server is vulnerable to SQL injection when _____. |
| | CANDIDATE ANSWER Options: (Expected answer indicated with a tick) <div><input type="radio"/> only when the site is not secured using SSL/TLS.</div> <div><input type="radio"/> when post data is transmitted unencrypted to the server.</div> <div><input checked="" type="radio"/> when user input is used directly in SQL queries.</div> <div><input type="radio"/> any time SQL is used to query a database.</div> |
| | No Comments |


| | |
|--|--|
| QUESTION 4  Correct Answer | Multiple Choice Security Essential |
| Score 5 | QUESTION DESCRIPTION Which of the following make it more difficult to execute a Man in the Middle attack? |
| | CANDIDATE ANSWER Options: (Expected answer indicated with a tick) <div><input type="radio"/> Requiring users to log in before using any part of the site.</div> <div><input type="radio"/> Using a two-factor authentication system that requires a user to enter a code from a text message along with their username and password.</div> <div><input type="radio"/> Using a CDN to deliver all assets and media (images, JavaScript, CSS, etc.) when a user browses the website.</div> <div><input checked="" type="radio"/> Forcing the use of SSL/TLS for all connections on a site.</div> |
| | No Comments |


| | |
|---|--|
| QUESTION 5  Correct Answer | Multiple Choice Security Essential |
| Score 5 | QUESTION DESCRIPTION Storing passwords in plain text in a database _____. |
| | CANDIDATE ANSWER Options: (Expected answer indicated with a tick) <div><input checked="" type="radio"/> makes users' passwords vulnerable to theft through unintended access to the database (SQL injection, stolen backups, etc.) <input type="radio"/> is fine as long as the database is properly set up to be accessed only by the root account on the server. <input type="radio"/> is safe for websites with fewer than 1000 users. <input type="radio"/> is fine in non-relational database.</div> No Comments |

| | |
|--|---|
| QUESTION 6  Correct Answer | Multiple Choice Security Essential |
| Score 5 | QUESTION DESCRIPTION In the event that a database is compromised, storing a salted hash of a password instead of the password itself will protect against: |
| | CANDIDATE ANSWER Options: (Expected answer indicated with a tick) <div><input checked="" type="radio"/> Rainbow Table attacks <input type="radio"/> SQL injection <input type="radio"/> Man in the Middle attacks <input type="radio"/> DoS/DDoS attacks</div> No Comments |

| | |
|---|---|
| QUESTION 7  Correct Answer | Multiple Choice Security Essential |
| Score 3.33 | QUESTION DESCRIPTION In order to help protect user's data, which of the following make a user's account more secure? |
| | CANDIDATE ANSWER Options: (Expected answer indicated with a tick) <div><input checked="" type="checkbox"/> <input type="radio"/> Forcing users to update their passwords on a regular basis (without allowing repeated passwords).</div> <div><input checked="" type="checkbox"/> <input type="radio"/> Forcing users to create passwords that are longer.</div> <div><input checked="" type="checkbox"/> <input type="radio"/> Forcing users to authenticate via SSL/TLS before entering their account information.</div> <div><input type="radio"/> Sending users' username and password through a GET request instead of a POST request.</div> |
| | No Comments |

| | |
|--|---|
| QUESTION 8  Correct Answer | Multiple Choice Security Essential |
| Score 4.29 | QUESTION DESCRIPTION Which of the following are ways in which a hacker could steal user information? |
| | CANDIDATE ANSWER Options: (Expected answer indicated with a tick) <div><input checked="" type="checkbox"/> <input type="radio"/> Session hijacking</div> <div><input checked="" type="checkbox"/> <input type="radio"/> Man in the Middle attack</div> <div><input checked="" type="checkbox"/> <input type="radio"/> SQL injection</div> <div><input checked="" type="checkbox"/> <input type="radio"/> Cross Site Scripting</div> <div><input checked="" type="checkbox"/> <input type="radio"/> Cross-Site Request Forgery</div> <div><input checked="" type="checkbox"/> <input type="radio"/> Phishing</div> <div><input checked="" type="checkbox"/> <input type="radio"/> Social Engineering</div> |
| | No Comments |

| | |
|---|---|
| QUESTION 9  Correct Answer | Multiple Choice Security Essential |
| Score 5 | QUESTION DESCRIPTION Which kind of attack floods a server with requests with the intent of blocking traffic from reaching that server? |
| | CANDIDATE ANSWER Options: (Expected answer indicated with a tick) <input checked="" type="radio"/> <input type="radio"/> DDoS <input type="radio"/> Man in the Middle <input type="radio"/> Rainbow Table <input type="radio"/> Dictionary |
| | No Comments |

| | |
|---|---|
| QUESTION 10  Correct Answer | Common Security Risks > Multiple Choice Security Essential |
| Score 5 | QUESTION DESCRIPTION Select the term that best matches the following definition: <i>A way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.</i> |
| | CANDIDATE ANSWER Options: (Expected answer indicated with a tick) <input type="radio"/> DoS <input checked="" type="radio"/> <input type="radio"/> Phishing <input type="radio"/> SQL Injection <input type="radio"/> Malware |
| | No Comments |