Bao mat web_ Nhom 01

Dashboard / My courses / WESE331479_23_2_01 / Topic 6 / Kiểm tra giữa kỳ

Started on	Tuesday, 26 March 2024, 8:01 AM
State	Finished
Completed on	Tuesday, 26 March 2024, 8:28 AM
Time taken	27 mins 8 secs
Grade	**9.75** out of 10.00 (**98**%)

Question 1

Complete

Mark 0.25 out of 0.25

What block cipher encryptions are safe to use?

○ a. Twofish, Blowfish, Triple DES (3DES)

● b. Rijndael, Advanced Encryption Standard (AES), Twofish

○ c. AES, Blowfish, Triple DES (3DES)

○ d. Advanced Encryption Standard (AES), Twofish, Blowfish

Question 2

Complete

Mark 0.25 out of 0.25

What are the weaknesses included in Software and Data Integrity Failures?

● a. Deserialization of Untrusted Data, Download of Code Without Integrity Check

○ b. Download of Code Without Integrity Check, Insufficient Entropy

○ c. Download of Code Without Integrity Check, Broken or Risky Crypto Algorithm

○ d. Insufficient Entropy, Deserialization of Untrusted Data

Question 3

Complete

Mark 0.25 out of 0.25

Who is the winner of the 2015 Password Hashing Competition?

- ● a. Argon2
- ○ b. BLAKE2
- ○ c. scrypt
- ○ d. SHA-3

Question 4

Complete

Mark 0.25 out of 0.25

What type of OWASP is the use of default values?

- ● a. Security Misconfiguration
- ○ b. Broken Access Control
- ○ c. XSS
- ○ d. Using components with known vulnerabilities

Question 5

Complete

Mark 0.25 out of 0.25

Your application is created using a language that does not support a clear distinction between code and data. Which vulnerability is most likely to occur in your application?

- ● a. Injection
- ○ b. Insufficient transport layer protection
- ○ c. Failure to restrict URL access
- ○ d. Insecure direct object references

Question 6

Complete

Mark 0.25 out of 0.25

Which of the following consequences is most likely to occur due to an injection attack?

- ○ a. Insecure direct object references
- ● b. Denial of service
- ○ c. Cross-site request forgery
- ○ d. Spoofing

Question 7

Complete

Mark 0.25 out of 0.25

Which of the following attacks occurs when a malicious user convinces a victim to send a request to a server with malicious input and the server echoes the input back to client?

● a. Reflected XSS
○ b. Failure to restrict URL access
○ c. Persistent XSS
○ d. Insecure direct object references

Question 8

Complete

Mark 0.25 out of 0.25

Which mitigation technique helps you tell the parser that a specific character is a literal and not a control character?

○ a. Allow list
○ b. Block list
○ c. Table indirection
● d. Escaping

Question 9

Complete

Mark 0.25 out of 0.25

Arccording to OWASP Top 10 , which of the following is not the type of XSS?

● a. Virtual XSS
○ b. Stored XSS
○ c. DOM XSS
○ d. Reflected XSS

Question 10

Complete

Mark 0.25 out of 0.25

What linter is used to find packages with known vulnerabilities?

○ a. prospector
○ b. dodgy
● c. safety
○ d. pylint
○ e. bandit,

Question 11

Complete

Mark 0.25 out of 0.25

Let X be a person working in TESTBOOK and he is an admin. X has username as admin and password as admin123. Name the vulnerability from the top 10 OWASP that TESTBOOK website faces.

○ a. XML External Entities
● b. Broken Authentication
○ c. Sensitive Data Exposure
○ d. Injection

Question 12

Complete

Mark 0.00 out of 0.25

What package you should use to parse xml?

● a. xml
○ b. defusedxml

Question 13

Complete

Mark 0.25 out of 0.25

It is safe to use pickle for the serialization.

○ a. True
● b. False

Question 14

Complete

Mark 0.25 out of 0.25

For which OWASP type we can use the principle of Least Privilege prevention techniques?

○ a. XML external entities
○ b. Injection
● c. Broken Access control
○ d. Broken Authentication

Question 15

Complete

Mark 0.25 out of 0.25

_________ attack is a type of attack against an application that parses XML input.

● a. XXE
○ b. Injection
○ c. HTML
○ d. XSS

Question 16

Complete

Mark 0.25 out of 0.25

Which mitigation technique can help you strictly define valid input?

○ a. Memory size checks
○ b. Table indirection
● c. Allow list
○ d. Escaping

Question 17

Complete

Mark 0.25 out of 0.25

LDAP stands for

● a. Lightweight Directory Access Protocol
○ b. Lightweight Directory Access Port
○ c. Lightweight Dictionary Access Protocol
○ d. Lightweight Dictionary Access Port

Question 18

Complete

Mark 0.25 out of 0.25

Which of the following is most common intercepting tool?

○ a. SQL Map
○ b. BeEF
○ c. Commix
● d. Burp Suite

Question 19

Complete

Mark 0.25 out of 0.25

Which terms are correct for the peppering?

○ a. The pepper should be shared between stored passwords. and The pepper should be unique like a salt.

● b. The pepper should be stored in the secrets vault. and The pepper should be shared between stored passwords.

○ c. The pepper should be stored in the database and The pepper should be stored in the secrets vault.

○ d. The pepper should be unique like a salt. and The pepper should be stored in the database.

Question 20

Complete

Mark 0.25 out of 0.25

Which category of OWASP Top 10 broadly cover SolarWinds malicious update-related issue?

○ a. Security Logging and Monitoring Failures

○ b. Identification and Authentication Failures

● c. Software and Data Integrity Failures

○ d. Server-Side Request Forgery

Question 21

Complete

Mark 0.25 out of 0.25

Which hash function you should use if you need to hash large amounts of data?

○ a. Argon2

○ b. SHA-2

○ c. bcrypt

● d. BLAKE2

Question 22

Complete

Mark 0.25 out of 0.25

If a website does not validate authorization of a user for direct references to restricted files, then to which threat such a website is vulnerable?

○ a. Injection

● b. Insecure Direct Object References

○ c. XML External Entity

○ d. XSS

Question 23

Complete

Mark 0.25 out of 0.25

"|/bin/ls -al" is a payload for which injection attack?

○ a. HTML Injection
○ b. SQL Injection
○ c. All of the above
● d. OS Command Injection

Question 24

Complete

Mark 0.25 out of 0.25

Which of the following scenarios is most likely to cause an injection attack?

○ a. A Web action performs an operation on behalf of the user without checking a shared secret.
○ b. Unvalidated input can be distinguished from valid instructions.
● c. Unvalidated input is embedded in an instruction stream.
○ d. A Web application does not validate a client’s access to a resource.

Question 25

Complete

Mark 0.25 out of 0.25

Which of the following is not OWASP Top 10 vulnerabilities?

○ a. Broken Authentication
● b. Privacy Breach
○ c. XSS
○ d. Insecure Deserialization

Question 26

Complete

Mark 0.25 out of 0.25

Which of the following automated tools are used for SQLi attack?

○ a. Wireshark
○ b. commix
● c. sqlmap
○ d. BeEF

Question 27

Complete

Mark 0.25 out of 0.25

Which of the following input sources can be directly controlled by a malicious user?

- ● a. Window.location and GET/POST parameters
- ○ b. GET/POST parameters and Ports and network resources
- ○ c. Server configuration files and GET/POST parameters
- ○ d. Window.location and Server configuration files

Question 28

Complete

Mark 0.25 out of 0.25

You should use a blacklist wherever possible; use whitelists only as a secondary defense.

- ○ a. True
- ● b. False
- ○ c. 1 and 3

Question 29

Complete

Mark 0.25 out of 0.25

Which of the following is most vulnerable to injection attacks?

- ● a. Regular expressions
- ○ b. Session IDs
- ○ c. Registry keys
- ○ d. Server configuration files

Question 30

Complete

Mark 0.25 out of 0.25

Which of the following languages are the primary targets of cross-site scripting?

- ○ a. XSLT
- ○ b. SQL
- ● c. HTML
- ○ d. XPath

Question 31

Complete

Mark 0.25 out of 0.25

Which package you shouldn’t use for a key generation?

● a. random
○ b. os
○ c. secrets

Question 32

Complete

Mark 0.25 out of 0.25

WHICH OF THE CATEGORY ADDED NEWLY IN OWASP TOP 10 2021?

○ a. Insecure Design, Software and Data Integrity Failure, Software and Data Integrity Failure
○ b. Software and Data Integrity Failure, SSRF, Broken Access Control
○ c. Broken Access Control, Insecure Design, Software and Data Integrity Failure
● d. Insecure Design, Software and Data Integrity Failure, SSRF

Question 33

Complete

Mark 0.25 out of 0.25

What are the cryptographic hash function properties?

● a. One-way function change and Fixed-length hash values
○ b. Reversible function change and Deterministic behavior
○ c. Unfixed hash values and One-way function change
○ d. Unfixed hash values and Fixed-length hash values

Question 34

Complete

Mark 0.25 out of 0.25

What does 'nonrepudiation' mean?

○ a. What can you do?
● b. Who did what?
○ c. Has the data changed?
○ d. Who created this data?

Question 35

Complete

Mark 0.25 out of 0.25

Which of the following is safe from SQLi (JAVA)?

○ a. String custname = request.getParameter("customerName");String query = "SELECT balance FROM data WHERE uname = "+ custname;

● b. String custname = request.getParameter("customerName");String query = "SELECT balance FROM user WHERE uname = ? ";PreparedStatement pstmt = connection.prepareStatement(query);pstmt.setString(1, custname);

Question 36

Complete

Mark 0.25 out of 0.25

How to prevent Injection vulnerability in a web application?

● a. Input validation, Use of safe API

○ b. Use Security Headers, Use of safe API

○ c. Use of safe API, Use HTTPS/TLS protocol

○ d. Use HTTPS/TLS protocol, Input validation

Question 37

Complete

Mark 0.25 out of 0.25

A user is able to pass malicious input that invokes control codes in your Web application. Which vulnerability is most likely to occur in your Web application?

○ a. Insufficient transport layer protection

● b. Injection

○ c. Failure to restrict URL access

○ d. Insecure direct object references

Question 38

Complete

Mark 0.25 out of 0.25

What hash functions are safe from the 'hashlib' package?

○ a. SHA-1, SHA-2, SHA-3

○ b. MD5, SHA-2, SHA-3

○ c. MD5, SHA-1

● d. SHA-2, SHA-3, BLAKE2

Question 39

Complete

Mark 0.25 out of 0.25

Which of the following is/are OWASP Top 10 2021 vulnerabilities?

● a. Broken Access Control, Injection

○ b. Broken Access Control, XSS

○ c. XSS, SSRF

○ d. Injection, XSS

Question 40

Complete

Mark 0.25 out of 0.25

It is safe to use `==` to compare 2 hash values.

● a. False

○ b. True

◄ BT WebGoat A5 - A10

Jump to...