Alright Alden! Diretso ko nang gawin lahat from 1 to 40 —  
 may section title sa taas, tapos bawat correct answer ay may asterisk (\*), at clean format gaya ng gusto mo. Eto na:

# I. Application Security Quiz Answers

1. Which of the following is a common web application security vulnerability?  
 a) Strong authentication  
 b) Secure communication  
 c) Proper encryption  
 d) SQL Injection \*

2. Why is application security important in the context of interconnected systems?  
 a) Applications are always isolated from other systems  
 b) Applications are immune to attacks  
 c) Applications never handle sensitive data  
 d) Applications are often connected across multiple networks and are vulnerable to threats \*

3. What technique helps protect code from being easily understood by attackers?  
 a) Code beautification  
 b) Code refactoring  
 c) Code commenting  
 d) Code obfuscation \*

4. What is one benefit of using a SIEM (Security Information and Event Management) system?  
 a) Centralize security alerts for better risk understanding \*  
 b) Decentralize security monitoring  
 c) Eliminate the need for firewalls  
 d) Improve system performance

5. Which of the following is an example of an insider threat?  
 a) Phishing attack  
 b) DDoS attack  
 c) Misuse of access by an employee \*  
 d) Malware infection

6. What is the purpose of a Web Application Firewall (WAF)?  
 a) Encrypt network traffic  
 b) Detect insider threats  
 c) Filter and monitor HTTP traffic between a web application and the Internet \*  
 d) Replace the need for a database firewall

7. What does multi-factor authentication (MFA) require?  
 a) Two or more types of credentials for authentication \*  
 b) Only a username and password  
 c) Only a biometric factor  
 d) Only an IP address check

8. What is the main goal of penetration testing?  
 a) Make applications slower  
 b) Increase system vulnerabilities  
 c) Identify and exploit vulnerabilities before attackers do \*  
 d) Train employees on phishing

9. Which of the following describes a Zero-Day vulnerability?  
 a) A vulnerability that has been patched  
 b) A vulnerability discovered by the vendor  
 c) A vulnerability that is exploited before a fix is available \*  
 d) A vulnerability known only to security teams

10. What is the main focus of the CIA triad in cybersecurity?  
 a) Confidentiality, Integrity, and Availability \*  
 b) Compliance, Innovation, and Audit  
 c) Complexity, Intelligence, and Automation  
 d) Control, Investigation, and Analysis

11. What is the process of verifying the identity of a user or system called?  
 a) Authorization  
 b) Authentication \*  
 c) Accounting  
 d) Auditing

12. Which of the following is a common method used in phishing attacks?  
 a) Sending fraudulent emails to trick users into revealing sensitive information \*  
 b) Exploiting software vulnerabilities  
 c) Direct brute-force attacks on servers  
 d) Denial of Service attacks

13. What does SQL Injection primarily target?  
 a) Application logic  
 b) Network configurations  
 c) Database queries \*  
 d) Operating system settings

14. In application security, what does "least privilege" principle mean?  
 a) Giving users full access by default  
 b) Providing the maximum permissions possible  
 c) Giving users only the access necessary to perform their job \*  
 d) Allowing users to set their own permissions

15. What is the main purpose of input validation?  
 a) To format user inputs nicely  
 b) To prevent malicious data from being processed by applications \*  
 c) To speed up user data entry  
 d) To authenticate users faster

16. Which term refers to malicious software designed to gain unauthorized access or cause damage?  
 a) Patch  
 b) Malware \*  
 c) Firewall  
 d) Protocol

17. Which security measure involves converting data into a coded format to prevent unauthorized access?  
 a) Authentication  
 b) Encryption \*  
 c) Authorization  
 d) Firewalling

18. What does HTTPS stand for?  
 a) HyperText Transmission Protocol Standard  
 b) Hyper Transfer Technology Secure  
 c) HyperText Transfer Protocol Secure \*  
 d) Highly Trusted Technology Protocol

19. What is Cross-Site Scripting (XSS)?  
 a) An attack that manipulates network routing  
 b) An attack where malicious scripts are injected into trusted websites \*  
 c) An attack on system firmware  
 d) A type of phishing attack

20. What kind of attack involves overwhelming a system with traffic to make it unavailable?  
 a) SQL Injection  
 b) Denial of Service (DoS) attack \*  
 c) Phishing attack  
 d) Malware infection

21. Which of the following best describes a botnet?  
 a) A network of infected computers controlled remotely by an attacker \*  
 b) A type of firewall  
 c) A security patching system  
 d) A software debugging tool

22. What is an API (Application Programming Interface) vulnerability?  
 a) Strengthening API authentication  
 b) A system where APIs are automatically patched  
 c) A weakness in an API that can be exploited by attackers \*  
 d) Automatic updating of API versions

23. What is the purpose of patch management?  
 a) Ignoring updates to maintain stability  
 b) Regularly updating software to fix vulnerabilities \*  
 c) Rewriting applications from scratch  
 d) Backing up applications weekly

24. What is a honeypot in cybersecurity?  
 a) A password cracking tool  
 b) An encryption method  
 c) A decoy system designed to lure attackers \*  
 d) A malware removal software

25. What does "social engineering" typically involve?  
 a) Breaking into data centers  
 b) Exploiting hardware vulnerabilities  
 c) Manipulating people into divulging confidential information \*  
 d) Engineering network hardware

26. What is the main goal of network segmentation?  
 a) Merging different networks  
 b) Limiting the spread of security breaches \*  
 c) Increasing network speed  
 d) Simplifying user authentication

27. What is ransomware?  
 a) A type of firewall  
 b) A phishing tool  
 c) Malware that encrypts files and demands payment for their release \*  
 d) A password management software

28. What kind of security testing evaluates software without executing it?  
 a) Dynamic analysis  
 b) Penetration testing  
 c) Static analysis \*  
 d) Fuzz testing

29. Which practice helps protect against password attacks?  
 a) Using the same password for all accounts  
 b) Writing passwords on sticky notes  
 c) Implementing strong password policies and MFA \*  
 d) Disabling account lockout policies

30. What does the term "threat modeling" refer to?  
 a) Building a firewall  
 b) Encrypting all databases  
 c) Identifying and evaluating potential threats to a system \*  
 d) Creating malware for testing

31. What is Cross-Site Request Forgery (CSRF)?  
 a) Exploiting DNS vulnerabilities  
 b) An attack that tricks a user into executing unwanted actions on a web application \*  
 c) Intercepting SSL traffic  
 d) Logging keystrokes remotely

32. What is an SSL/TLS certificate used for?  
 a) Encrypting communications between a web server and a browser \*  
 b) Generating dynamic website content  
 c) Blocking malware  
 d) Detecting phishing sites

33. What is the purpose of vulnerability scanning?  
 a) Creating software updates  
 b) Identifying known security weaknesses in systems \*  
 c) Penetrating systems for data  
 d) Encrypting communications

34. What security risk is associated with using default passwords?  
 a) Improved user convenience  
 b) Easier exploitation by attackers \*  
 c) Faster network speeds  
 d) Better system stability

35. What is session hijacking?  
 a) Installing a virus remotely  
 b) Deleting user sessions permanently  
 c) Taking over a valid user session to gain unauthorized access \*  
 d) Encrypting user sessions for protection

36. What is the purpose of the OWASP Top Ten?  
 a) A list of best programming languages  
 b) A catalog of hardware vulnerabilities  
 c) A list of the most critical web application security risks \*  
 d) A ranking of antivirus software

37. What does a firewall primarily do?  
 a) Monitors and controls incoming and outgoing network traffic based on security rules \*  
 b) Encrypts all data  
 c) Deletes malware automatically  
 d) Strengthens WiFi signal

38. What is a brute force attack?  
 a) A polite request for password reset  
 b) Sending malware via email  
 c) Trying many combinations of passwords to gain unauthorized access \*  
 d) Encrypting user data for protection

39. What is "pharming" in cybersecurity?  
 a) Planting viruses on farms  
 b) Scanning servers for vulnerabilities  
 c) Redirecting users to fake websites without their knowledge \*  
 d) Encrypting web server traffic

40. What is two-factor authentication (2FA)?  
 a) Authentication using one password  
 b) Authentication using biometrics only  
 c) Authentication by verifying IP address  
 d) Authentication requiring two different forms of verificatiion \*

—--------------

Which team is primarily responsible for analyzing and mitigating security incidents?  
 a) Legal Team  
 b) Development Team  
 c) Sales Team  
 d) Security Operations Center \*

An attack that exploits a previously unknown vulnerability is called:  
 a) Replay attack  
 b) Brute force attack  
 c) Zero-day attack \*  
 d) Dictionary attack

What does an Intrusion Detection System (IDS) do?  
 a) Prevents unauthorized access  
 b) Encrypts sensitive data  
 c) Repairs damaged systems  
 d) Detects unauthorized access \*

What is the purpose of a risk register?  
 a) To document identified risks and their management \*  
 b) To record all incidents that occur  
 c) To schedule employee tasks  
 d) To design network diagrams

Which of the following best defines social engineering?  
 a) Using firewalls to block attacks  
 b) Manipulating people to gain confidential information \*  
 c) Encrypting sensitive data  
 d) Using automated tools to exploit vulnerabilities

What is phishing?  
 a) Testing network vulnerabilities  
 b) Unauthorized access to systems  
 c) Fraudulent attempts to obtain sensitive information \*  
 d) Encryption of confidential data

Which of the following is a physical security control?  
 a) Firewall  
 b) Antivirus software  
 c) Security badge access system \*  
 d) VPN

What does two-factor authentication (2FA) provide?  
 a) A second password for the same account  
 b) An extra layer of security by requiring two forms of verification \*  
 c) A backup method for data recovery  
 d) Faster access to systems

Which of the following is an example of malware?  
 a) Phishing  
 b) Ransomware \*  
 c) Encryption  
 d) Authentication

A firewall primarily serves to:  
 a) Encrypt traffic  
 b) Control incoming and outgoing network traffic \*  
 c) Detect intrusions  
 d) Backup data

What is the purpose of encryption?  
 a) Speed up network connections  
 b) Protect data by converting it into unreadable form \*  
 c) Identify vulnerabilities  
 d) Increase system memory

What does a vulnerability scanner do?  
 a) Prevents malware infections  
 b) Identifies potential security weaknesses \*  
 c) Creates system backups  
 d) Encrypts network traffic

What is a botnet?  
 a) A type of firewall  
 b) A network of infected computers controlled by an attacker \*  
 c) A legitimate set of cloud servers  
 d) An anti-virus software

What is the main goal of penetration testing?  
 a) To recover lost data  
 b) To identify vulnerabilities by simulating attacks \*  
 c) To encrypt sensitive data  
 d) To speed up the network

Which of the following best describes a brute-force attack?  
 a) An attack that tricks users into providing information  
 b) An attack that tests multiple passwords until the correct one is found \*  
 c) An attack that blocks users from accessing a system  
 d) An attack that floods a system with traffic

A denial-of-service (DoS) attack attempts to:  
 a) Encrypt files on a server  
 b) Steal user credentials  
 c) Overwhelm systems to make them unavailable \*  
 d) Monitor network traffic

The process of verifying the identity of a user is called:  
 a) Authorization  
 b) Validation  
 c) Authentication \*  
 d) Accounting

Which of the following refers to an insider threat?  
 a) Malware introduced from the internet  
 b) Threats from employees within the organization \*  
 c) Threats from competitors  
 d) Threats from hackers abroad

What is multi-factor authentication (MFA)?  
 a) Authentication using a single password  
 b) Authentication using backup codes only  
 c) Authentication requiring multiple verification methods \*  
 d) Authentication through email only

What is the purpose of a digital certificate?  
 a) Encrypt database passwords  
 b) Provide proof of identity electronically \*  
 c) Store large amounts of data  
 d) Manage physical security

Which of the following is considered a strong password?  
 a) password123  
 b) admin  
 c) JohnDoe2020  
 d) 9#vT8$pZ3w! \*

What does a VPN primarily do?  
 a) Detects intrusions  
 b) Encrypts internet traffic and masks IP addresses \*  
 c) Speeds up internet connections  
 d) Monitors employee activity

What type of attack is a SQL injection?  
 a) Network attack  
 b) Social engineering attack  
 c) Database attack \*  
 d) Physical attack

What is the first step in incident response?  
 a) Eradication  
 b) Containment  
 c) Identification \*  
 d) Recovery

What is the term for weaknesses that can be exploited by threats?  
 a) Opportunities  
 b) Controls  
 c) Vulnerabilities \*  
 d) Certifications

What does CIA stand for in cybersecurity?  
 a) Confidentiality, Integrity, Availability \*  
 b) Control, Inspection, Authentication  
 c) Compliance, Investigation, Authorization  
 d) Cybersecurity, Information, Access

Which of the following is an example of two-factor authentication?  
 a) Password only  
 b) Password and PIN  
 c) Password and fingerprint scan \*  
 d) Password and username

What kind of malware locks the user out and demands payment?  
 a) Spyware  
 b) Adware  
 c) Worm  
 d) Ransomware \*

What is the purpose of patch management?  
 a) Create backup copies  
 b) Encrypt sensitive files  
 c) Update software to fix vulnerabilities \*  
 d) Speed up systems

What is spear phishing?  
 a) Random mass email phishing  
 b) Phishing targeting a specific individual \*  
 c) Phishing using websites  
 d) Phishing via SMS

What is the purpose of a honeypot?  
 a) To store backup data  
 b) To deceive attackers by simulating vulnerable systems \*  
 c) To encrypt traffic  
 d) To monitor employee emails

What does DLP (Data Loss Prevention) aim to do?  
 a) Prevent unauthorized data transmission \*  
 b) Speed up the internet  
 c) Backup data files  
 d) Encrypt web traffic

Which one is an example of logical security control?  
 a) Security guard  
 b) Fire extinguisher  
 c) Firewall \*  
 d) Door lock

What is whitelisting in cybersecurity?  
 a) Blocking unauthorized users  
 b) Allowing only approved programs or users \*  
 c) Encrypting user data  
 d) Deleting inactive accounts

Which of the following is NOT a common form of malware?  
 a) Virus  
 b) Worm  
 c) Firewall \*  
 d) Trojan

What is the primary goal of social engineering attacks?  
 a) Infect systems with malware  
 b) Physically damage hardware  
 c) Manipulate individuals to divulge confidential information \*  
 d) Steal backup tapes

What does an antivirus program do?  
 a) Blocks all incoming network traffic  
 b) Detects and removes malicious software \*  
 c) Encrypts all communications  
 d) Tests system vulnerabilities

What is the best description of ransomware?  
 a) Malware that steals passwords  
 b) Malware that encrypts data and demands payment \*  
 c) Malware that deletes files randomly  
 d) Malware that monitors user activity

What is the purpose of network segmentation?  
 a) To combine all servers into one network  
 b) To separate networks to improve security \*  
 c) To enable faster file sharing  
 d) To reduce power consumption

What is two-factor authentication (2FA)?  
 a) Authentication using one password  
 b) Authentication using biometrics only  
 c) Authentication by verifying IP address  
 d) Authentication requiring two different forms of verification \*

—----------------------

1. What is the first step when a vulnerability is found in a system?  
 a) Ignore it  
 b) Report it to the software vendor or CERT \*  
 c) Fix it quietly  
 d) Sell the information to interested parties

2. What is the main purpose of cybersecurity compliance?  
 a) To increase IT costs  
 b) To create more rules for employees  
 c) To protect individuals and organizations in the digital environment \*  
 d) To make systems complicated

3. What is phishing?  
 a) Hacking into systems  
 b) A method of encryption  
 c) Fraudulent attempts to obtain sensitive information via email or websites \*  
 d) A type of firewall

4. Which law focuses on financial privacy in the US?  
 a) HIPAA  
 b) GDPR  
 c) Gramm-Leach-Bliley Act \*  
 d) PCI DSS

5. What does whistleblowing refer to?  
 a) Reporting minor workplace issues  
 b) Reporting good practices  
 c) Disclosing unethical behavior or wrongdoing within an organization \*  
 d) Ignoring problems

6. What is an example of an unethical practice?  
 a) Encrypting data  
 b) Reporting a breach  
 c) Misuse of privileged information \*  
 d) Following company policies

7. What are possible consequences of non-compliance?  
 a) Legal fines and reputational damage \*  
 b) Increased profits  
 c) Enhanced security  
 d) Promotion opportunities

8. What security principle is associated with protecting data?  
 a) Principle of encryption \*  
 b) Principle of openness  
 c) Principle of disclosure  
 d) Principle of expansion

9. What is the role of cybersecurity ethics?  
 a) Making systems faster  
 b) Reducing regulations  
 c) Safeguarding the integrity and confidentiality of information \*  
 d) Simplifying software

10. What is a key factor in promoting cybersecurity ethics?  
 a) Faster internet  
 b) Ethical leadership \*  
 c) More complex systems  
 d) Increased sales

11. What does HIPAA stand for?  
 a) Health Information Protection and Access Act  
 b) Health Insurance Portability and Accountability Act \*  
 c) Health Information Privacy and Accountability Act  
 d) High-security Internet Privacy Access Agreement

12. What term refers to a legal requirement to protect individuals' personal data?  
 a) Compliance regulation \*  
 b) Encryption policy  
 c) Fair use doctrine  
 d) Data breach notification law

13. What is the role of a Data Protection Officer (DPO)?  
 a) To provide technical support  
 b) To oversee data protection strategy and ensure compliance with regulations \*  
 c) To track employee attendance  
 d) To manage marketing campaigns

14. What ethical principle involves the responsibility to report security vulnerabilities?  
 a) Accountability \*  
 b) Responsibility  
 c) Confidentiality  
 d) Integrity

15. What must a penetration tester obtain before performing an assessment?  
 a) User credentials  
 b) Customer reviews  
 c) Explicit written authorization \*  
 d) Third-party audit certification

16. What is the principle of least privilege in cybersecurity?  
 a) Limiting user access rights to the minimum necessary \*  
 b) Granting users full access to systems  
 c) Allowing unrestricted data access  
 d) Encouraging open sharing of information

17. Which of the following is a key compliance principle in cybersecurity?  
 a) Voluntary data sharing  
 b) Adherence to legal and regulatory requirements \*  
 c) Flexibility  
 d) Unrestricted access to information

18. Which principle best describes ethical conduct in security operations?  
 a) Adhering strictly to legal requirements  
 b) Following a set of moral principles that govern decisions and actions \*  
 c) Prioritizing organizational profits over individual rights  
 d) Implementing the most advanced security technologies

19. Which law governs electronic contracts in many countries?  
 a) The Data Protection Act  
 b) The Privacy Act  
 c) The Electronic Communications and Transactions Act (ECTA) \*  
 d) The Cybersecurity Act

20. Which of the following is NOT a key component of cyber law?  
 a) E-commerce Regulation  
 b) Personal Privacy  
 c) Cybercrime regulations  
 d) Intellectual property rights \*

21. What is the role of the Computer Emergency Response Team (CERT)?  
 a) To develop software  
 b) To provide support during cybersecurity incidents \*  
 c) To regulate internet service providers  
 d) To enforce cyber laws

22. Your company collects user data and shares it with advertisers without informing users. What compliance principle is violated?  
 a) Informed consent \*  
 b) Least privilege  
 c) Backup policies  
 d) Integrity

23. Your organization receives a “right to be forgotten” request under GDPR. What should be your legal response?  
 a) Notify the government  
 b) Ignore the request  
 c) Delete all the user’s personal data unless required for legal reasons \*  
 d) Archive the data for future use

24. What best illustrates the importance of compliance with cybersecurity frameworks?  
 a) It allows employees to browse freely  
 b) It encourages non-standard security practices  
 c) It promotes unlimited internet use  
 d) It ensures legal protection and reduces liability \*

25. Which international standard provides best practices for an information security management system (ISMS)?  
 a) ISO 45001  
 b) ISO/IEC 27001 \*  
 c) ISO 9001  
 d) ISO 14001

26. What does "integrity" refer to in cybersecurity ethics?  
 a) Consistency in actions and decisions \*  
 b) Securing personal interests  
 c) Protecting against financial loss  
 d) Honesty and truthfulness

27. Which of the following is NOT considered a cybercrime?  
 a) Online Chatting \*  
 b) Phishing  
 c) Identity theft  
 d) Hacking

28. What is the primary function of a compliance audit in IT security?  
 a) To ensure adherence to policies and regulations \*  
 b) To monitor bandwidth  
 c) To manage social media accounts  
 d) To detect malware

29. A company implements strong security policies but doesn’t train employees on recognizing phishing attacks. Which principle is being neglected?  
 a) Role-based encryption  
 b) Technical safeguards  
 c) Physical access control  
 d) Administrative safeguards \*

30. What best describes the relationship between cybersecurity and compliance?  
 a) Compliance ensures marketing success  
 b) Cybersecurity protects against internal policies, while compliance addresses external regulations \*  
 c) They are unrelated areas of concern  
 d) Compliance is optional, while cybersecurity is mandatory

31. Which of the following is a legal requirement under GDPR?  
 a) Obtaining consent for data processing \*  
 b) Selling data to third parties  
 c) Keeping data indefinitely  
 d) Collecting as much data as possible

32. An employee at a hospital accesses a patient’s medical records out of curiosity. Which law has likely been violated?  
 a) Sarbanes-Oxley Act  
 b) Family Educational Rights and Privacy Act  
 c) Health Insurance Portability and Accountability Act \*  
 d) General Data Protection Regulation

33. A cloud service provider loses customer data due to a failed backup system. What compliance issue does this scenario illustrate?  
 a) Inadequate disaster recovery planning \*  
 b) Failure to maintain data accuracy  
 c) Breach of data minimization  
 d) Violation of intellectual property

34. What does the term "data breach" refer to?  
 a) Unauthorized access to confidential data \*  
 b) A software update  
 c) A system upgrade  
 d) A network outage

35. What is the main purpose of encryption in cybersecurity?  
 a) To protect data by making it unreadable to unauthorized users \*  
 b) To enhance internet speed  
 c) To create backups  
 d) To slow down data transfer

36. What is the responsibility of cybersecurity professionals in terms of continuous learning and professional development?  
 a) Optional for career advancement  
 b) Not relevant to ethical considerations  
 c) Only required for certification purposes  
 d) Necessary to stay updated with evolving threats and technologies \*

37. What is the significance of the "golden rule" in cybersecurity ethics?  
 a) Prioritizing personal interests over others  
 b) Ignoring the impact of actions on others  
 c) Treating others as one would like to be treated \*  
 d) Engaging in unethical practices

38. What is the GDPR?  
 a) A cybersecurity certification  
 b) The General Data Protection Regulation, a data protection law in the EU \*  
 c) A type of malware  
 d) A form of encryption

39. What ethical principle involves treating all individuals fairly and without discrimination?  
 a) Trustworthiness  
 b) Responsibility  
 c) Fairness \*  
 d) Accountability

40. Which U.S. law mandates safeguards for financial data held by institutions?  
 a) SOX  
 b) FERPA  
 c) HIPAA  
 d) GLBA \*