


注意：考試開始鈴響前，不得翻閱試題，
並不得書寫、畫記、作答。

國立清華大學 108 學年度碩士班考試入學試題

系所班組別：資訊安全研究所

考試科目(代碼)：資訊安全(2501)

— 作答注意事項 —

1. 請核對答案卷(卡)上之准考證號、科目名稱是否正確。
2. 作答中如有發現試題印刷不清，得舉手請監試人員處理，但不得要求解釋題意。
3. 考生限在答案卷上標記「由此開始作答」區內作答，且不可書寫姓名、准考證號或與作答無關之其他文字或符號。
4. 答案卷用盡不得要求加頁。
5. 答案卷可用任何書寫工具作答，惟為方便閱卷辨識，請儘量使用藍色或黑色書寫；答案卡限用 2B 鉛筆畫記；如畫記不清(含未依範例畫記)致光學閱讀機無法辨識答案者，其後果一律由考生自行負責。
6. 其他應考規則、違規處理及扣分方式，請自行詳閱准考證明上「國立清華大學試場規則及違規處理辦法」，無法因本試題封面作答注意事項中未列明而稱未知悉。

國立清華大學 108 學年度碩士班考試入學試題

系所班組別：資訊安全研究所碩士班

考試科目（代碼）：資訊安全 (2501)

共_6_頁，第_1_頁 *請在【答案卷、卡】作答

Part I (75%) Please select one correct answer according to the question (3 points/each).

1. Which of the following correctly defines SQL injection?
 - (a) Modifying a database query statement through false input to a function
 - (b) The process by which application programs manipulate strings to a base form
 - (c) Inputs to web applications that are processed by different parsers
 - (d) Character code sets that all Multilanguage capability

2. Which of the following correctly describes cross-site scripting (XSS)?
 - (a) Overflowing the allocated storage area to corrupt a running program
 - (b) Attempting to break a cryptographic system
 - (c) Exploiting the trust a site has in the user's browser
 - (d) Exploiting the trust a site has for the site

3. Which of the following correctly describes cross-site request forgery (XSRF)?
 - (a) Attacking a system by sending malicious input and relying upon the parsers and execution elements to perform the requested actions
 - (b) An enhanced data cryptographic encapsulation method
 - (c) Attacking a system by sending script commands and relying upon the parsers and execution elements to perform the requested actions
 - (d) Attempting to break a cryptographic system

4. When examining a packet capture from your network, you notice a large number of packets with the URG, PUSH, and FIN flags set. What type of traffic are you seeing in that packet capture?
 - (a) Botnet control channel
 - (b) Smurf attack
 - (c) Xmas attack
 - (d) Replay attack

5. The Smurf attack is an example of what kind of attack?
 - (a) DDoS
 - (b) Ransomware
 - (c) SQL injection
 - (d) Clickjacking

國立清華大學 108 學年度碩士班考試入學試題

系所班組別：資訊安全研究所碩士班

考試科目（代碼）：資訊安全 (2501)

共 6 頁，第 2 頁 *請在【答案卷、卡】作答

6. Your antivirus solution has detected malware on one of your computers. The AV program tells you the malware is located in a certain directory, but when you go to remove the malware you discover that the directory does not exist. This is most likely an example of:
 - (a) A Trojan horse
 - (b) An armored virus
 - (c) A transient virus
 - (d) A mobile malware infection

7. Which of the following is not a best practice for secure router configuration?
 - (a) Disabling each, CHARGEN, and other simple services
 - (b) Disabling IP source route
 - (c) Enabling Telnet access
 - (d) Enabling logging

8. When enabling port security on a switch interface, traffic is usually restricted based on:
 - (a) IP address
 - (b) Source port
 - (c) Protocol
 - (d) MAC address

9. You've been asked to help configure a router that is used to connect a remote branch office to your corporate headquarters. The router will need to be managed remotely from the corporate headquarters. Which of the following protocols would you recommend be used to manage the remote router?
 - (a) HTTP
 - (b) Telnet
 - (c) SSH
 - (d) SNMP

10. What does LEAP do?
 - (a) Modernizes Wi-Fi with a new encryption cipher
 - (b) Provides TLS support for Wi-Fi authentication under Windows
 - (c) Provides a lightweight mutual authentication protocol for clients and uses dynamic WEP keys
 - (d) Forces Cisco devices to use WPA2

國立清華大學 108 學年度碩士班考試入學試題

系所班組別：資訊安全研究所碩士班

考試科目（代碼）：資訊安全 (2501)

共 6 頁，第 3 頁

*請在【答案卷、卡】作答

11. Why is the buffer overflow such a popular attack?
 - (a) It is easy to accomplish over the internet.
 - (b) Attackers can use it to break any encryption.
 - (c) The same code will work on any system.
 - (d) It can provide arbitrary code execution.

12. What makes a website vulnerable to SQL Injection?
 - (a) Poorly filtered input fields
 - (b) A website that has a Microsoft SQL database powering it.
 - (c) Overly long text input boxes
 - (d) Low password strength requirements

13. Why is cross-site scripting successful?
 - (a) It uses a different memory register every time.
 - (b) Its code runs in an encrypted state.
 - (c) It uses zero-day vulnerabilities.
 - (d) It folds malicious code in with verified content from a compromised site.

14. Why is free Wi-Fi, such as in coffee shops, a popular target for session hijacking?
 - (a) The unsecured Wi-Fi allows an attacker to place malicious files on the user's machine.
 - (b) The site uses a captive portal.
 - (c) Unsecured Wi-Fi allows the attacker to sniff the wireless session for a user's session cookie.
 - (d) The user does not engage VPN over wireless.

15. Which of the following tools or methods is most likely to show you which servers in your server farm allow anonymous access to shares, have TCP port 80 open, and are running an old version of PHP?
 - (a) Protocol analyzer
 - (b) Port scanner
 - (c) Vulnerability scanner
 - (d) Baseline review

國立清華大學 108 學年度碩士班考試入學試題

系所班組別：資訊安全研究所碩士班

考試科目（代碼）：資訊安全 (2501)

共 6 頁，第 4 頁

*請在【答案卷、卡】作答

16. Why is DES no longer considered effective?
- (a) It only works with public keys.
 - (b) Its key-space is too small.
 - (c) It was replaced by the one-time pad method.
 - (d) It was replaced by RSA.
17. What does SSL depend on for authentication?
- (a) The SHA-256 hash
 - (b) The client's digital signature
 - (c) Hierarchy of trust established by the root CA
 - (d) The private key password
18. What is unique characteristics of one-time pads?
- (a) Unbreakable
 - (b) 4096-bit symmetric keys
 - (c) Provides Integrity
 - (d) Vulnerable to weak keys
19. Which cipher depends on the difficulty in factoring problem?
- (a) RSA
 - (b) ECC
 - (c) AES
 - (d) SHA-256
20. What factor is not the security goal ?
- (a) Non-repudiation
 - (b) Availability
 - (c) Confidentiality
 - (d) Integrity

國立清華大學 108 學年度碩士班考試入學試題

系所班組別：資訊安全研究所碩士班

考試科目（代碼）：資訊安全 (2501)

共 6 頁，第 5 頁 *請在【答案卷、卡】作答

21. How does a block cipher handle plaintext input?
- (a) It divides the input into predefined lengths, and pads the remainder to maintain a set length.
 - (b) It generates a key of the same length as the input and encrypts the text.
 - (c) It uses a hash algorithm to reduce the input to match the current key.
 - (d) It encrypts it only to the private key.
22. When you get an SSL certificate from a web page, what kind of cipher is used?
- (a) One-time pad
 - (b) Symmetric
 - (c) Asymmetric
 - (d) All of the above
23. When would non-repudiation be important to your application?
- (a) An attacker breaks the encryption algorithm.
 - (b) A collaborative user makes changes to a document that need to be securely tracked.
 - (c) One user adds a new user to the system.
 - (d) A user wants to provide his files from snooping during transmission.
24. Diffie-Hellman is representative of what branch of cryptography?
- (a) Symmetric
 - (b) Asymmetric
 - (c) Steam Cipher
 - (d) Hash function
25. Which port does Telnet use?
- (a) UDP port 22
 - (b) TCP port 22
 - (c) UDP port 23
 - (d) TCP port 23

國立清華大學 108 學年度碩士班考試入學試題

系所班組別：資訊安全研究所碩士班

考試科目（代碼）：資訊安全 (2501)

共_6_頁，第_6_頁

*請在【答案卷、卡】作答

Part II (25%) Please answer the following questions.

26. (5%) What is Steganography?
27. (5%) In $GF(2^8)$, find the inverse of (x^5) modulo $(x^8+x^4+x^3+x+1)$
28. (5%) List the parameters (block size, key size, and the number of rounds) for the three AES versions.
29. (5%) How to use SQL injection to successfully bypass the following login SQL command? Why?

*SELECT * FROM users WHERE (name='userName') and (pw='password');*

30. (5%) What is the vulnerability of the following C code? Why? What is commonly called for the vulnerability?

```
int main()
{
    char buf[0x20];
    setvbuf(stdout, 0, 2, 0);
    printf("Input...:");
    read(0, buf, 100);
    return 0;
}
```