

## Secure coding course - Student Background

This questionnaire is to collect data about the background of the participants. The answers to this questionnaire are NOT used by any means to evaluate/grade them.

**First name:** \_ \_ \_ \_ \_

**Last name:** \_ \_ \_ \_ \_

### 1. What is your occupation?

You are currently:

- ☐ only studying, full time
- ☐ also working as an employee
- ☐ also working as a self employed (e.g. consultant)
- ☐ also running your own company
- ☐ other: \_\_\_\_\_

### 2. For how many years have you studied Computer Science at a University level?

\_\_\_\_\_

### 3. What is your Major?

\_\_\_\_\_

### 4. Please select from the list below the courses you have already fully attended

- ☐ Operating Systems
- ☐ Security Engineering
- ☐ Programming
- ☐ Databases
- ☐ Network / Network security

Other relevant courses:

### 5. Do you have any working experience?

Please specify the length of your working experience in years

### 6. What are or have been your roles at work?

Answer this question only if at Question 5 you have specified any working experience

\_\_\_\_\_

### 7. Have you ever been involved in any security-specific activity (e.g. IT risk assessment)?

Please choose only one of the following options ☐ Yes ☐ No

To answer the questions 10-14 please use the following scale:

**0-No knowledge:** I have no knowledge or experience with this topic.

**1-Novice:** I have a minimal or 'textbook' knowledge of area without connecting it to practice.

**2-Beginner:** I have a working knowledge of key aspects of area.

**3-Competent:** I have good working and background knowledge of area.

**4-Proficient:** I have a deep understanding of area.

**5-Expert:** I have an authoritative knowledge of area.

---

8. **How would you describe your level of expertise in system security (e.g. memory structure, ACL/RBAC, ..)?**

Please choose only one of the following options:

*novice* ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 *expert*

9. **How would you describe your level of expertise in network security (e.g. MitM attacks, channel security, ..)?**

Please choose only one of the following options:

*novice* ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 *expert*

10. **How would you describe your level of expertise in cryptography?**

Please choose only one of the following options:

*novice* ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 *expert*

11. **How would you describe your level of expertise in developing software attacks?**

Please choose only one of the following options:

*novice* ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 *expert*

12. **How would you describe your level of expertise in software development (any language)?**

Please choose only one of the following options:

*novice* ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 *expert*

13. **What programming languages are you the most experienced with? Please order them by preference in descending order (most preferred one to least preferred one).**

---

14. **How would you describe your level of expertise in software architecture (e.g. design patterns, Class diagrams, ..)?**

Please choose only one of the following options:

*novice* ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 *expert*

**15. What is SQL injection? Choose the most appropriate answer. Choose only one answer.**

- ☐ An attack against the database that allows the attacker to drop a table in a database.
- ☐ An attack that, by using specific strings that are not correctly interpreted by the application, allows the attacker to perform some pre-determined operation on the database.
- ☐ An attack that uses a malformed string that, when interpreted by the backend, results in a valid query that is executed by the DB.
- ☐ An attack that affects the availability of a database by injecting rogue code in a web application.
- ☐ Don't know

**16. What is XSS attack? Choose the most appropriate answer. Choose only one answer.**

- ☐ An attack that exploits lack of input validation to affect the integrity of the webpage the user visits, and potentially the confidentiality of user's data.
- ☐ An attack that by redirecting the user to different domains allows the attacker to exfiltrate cookies or other session information.
- ☐ An attack that duplicates a webpage to trick the user in inserting private information that are then sent to the attacker.
- ☐ An attack that can only allow the attacker to hijack a network session.
- ☐ Don't know

**17. How do you build a stack buffer overflow exploit that allows you to execute arbitrary code on the system? Choose the most appropriate answer. Choose only one answer.**

- ☐ You forge an input string that modifies the values stored in memory in such a way that the system executes arbitrary functions
  - ☐ You forge an input string that, by overwriting specific addresses in memory (e.g. the RET address), alters the execution flow to one controlled by the attacker.
  - ☐ You forge an input string that, when loaded in memory, modifies the CPU registers EAX and EIP.
  - ☐ Don't know
  - ☐ None of the above seems appropriate. Please provide your own definition below:
- 

**18. What is the main design difference between asymmetric and symmetric cryptography? Choose the most appropriate answer. Choose only one answer.**

- ☐ Asymmetric cryptography requires a key to be negotiated before the encrypted message is sent. Symmetric cryptography is based on a known key that the parties store locally and use for every communication.
- ☐ Symmetric cryptography is based on one key for both encryption and decryption. The robustness of the protocol depends entirely on its secrecy. Asymmetric encryption uses two keys, only one of which needs to remain secret.
- ☐ The robustness of symmetric cryptography depends on the length of the key. The robustness of asymmetric cryptography depends on the seed of the random number generator used to generate the public and private keys.
- ☐ Because integer factorisation is a hard problem to solve, generating the public and private keys necessary for asymmetric cryptography is, computationally, a very expensive operation. This is not the case for symmetric cryptography.
- ☐ Don't know

**19. What is a race condition? Choose the most appropriate answer. Choose only one answer.**

- ☐ A bug in a program that causes availability issues when triggered on multi-threaded systems that use shared memory.
- ☐ The behaviour of a program for which its output is dependent on the order in which actions are executed by the operating system scheduler, which is uncontrollable by the program.
- ☐ The hazardous behaviour of a multi-threaded program that does not contain any synchronization instructions, semaphores or mutual exclusion (mutex).
- ☐ A security vulnerability which can lead two threads in the same process to access the same shared memory resource concurrently and cause a memory integrity violation.
- ☐ Don't know

**20. What is a garbage collector? Choose the most appropriate answer. Choose only one answer.**

- ☐ A mechanism employed by a programming language in order to free-up unused memory on the stack and heap.
- ☐ A program that monitors the memory of another program and deallocates memory which is no longer referenced by the latter program.
- ☐ A technique through which the Java Virtual Machine is able to free memory references to the stack memory of a running Java program.
- ☐ A form of automatic memory management, which delegates the task of freeing unused memory from the programmer to the runtime environment.
- ☐ Don't know