Name, Firstname, Group / *Nom, Prénom, Groupe* : .....

Software Security – *Sécurité Logicielle*

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / *Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.*
- No exchange (eraser, pen, responses …) is allowed between students / *Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit*
- You must switch off your mobile phone and store it into your bag / *Vous devez éteindre votre téléphone portable et le ranger dans votre sac*
- You have 45 minutes (except 3rd of time : 60 minutes) / *Vous avez 45 minutes (sauf tiers temps: 60 minutes)*
- Write your name, firstname, and group on every sheet / *Ecrivez nom, prénom et groupe sur chaque feuille*
- Answer in English or in French / *Répondez en français ou en anglais*
- Be brief but precise. Show how you derive the answers to the questions (yes/no is not an answer) / *Soyez brefs mais précis. Montrez comment vous arrivez à la réponse (oui/non n'est pas une réponse).*
- The total number of points is : 32 / Le nombre total de points est de : 32

Question 1 (2 points)

What are the different types of cross-site scripting attacks? *Quels sont les différents types d'attaques cross-site scripting?*

Question 2 (3 points)

Explain how SQL injections work (illustrate with examples) and the basic measures to prevent them from happening? *Expliquez comment fonctionne une injection SQL (illustrez avec des exemples). Quelle est la mesure de base pour éviter une telle attaque ?*

Question 3 (3 points)

Which technique(s) can be used to exfiltrate secret data from a website? *Quelle(s) technique(s) peut/peuvent permettre d'exfiltrer des données secrètes d'un site web ?*

Question 4 (5 points)

Examine the following code, which has been crafted in order to defeat stack buffer overflow attacks. What do you think of the protection introduced (do not take into account the secret's size)? *Examinez le code suivant qui a été codé pour empêcher les attaques par stack buffer overflow. Que pensez-vous de la protection (sans prendre en compte la taille du secret) ?*

```
void func (char *str)
{
        int guard;
        int *secret = malloc (sizeof(int));
        *secret = generateRandomNumber();
        guard = *secret;
        char buffer[12];
        strcpy (buffer, str);
        if (guard != *secret) exit;
        return;
}
```

Question 5 (3 points)

What are cookies used for? Are they a solution or a problem with respect to security? *A quoi servent les cookies ? Sont-ils une solution ou un problème pour la sécurité ?*

Name, Firstname, Group / *Nom, Prénom, Groupe :* .....

Question 6 (5 points)

Select correct answers. Correct answers will be graded with 1 point, incorrect ones with -0.5 point. No answer adds or subtracts no point. There may be multiple answers to each question. *Répondez au QCM suivant (plusieurs réponses positives sont possibles pour chaque question). Une réponse correcte sera notée 1 point, une incorrecte -0,5 et pas de réponse : pas de point.*

- A worm is (a) a bug (b) a botnet (c) a malware that self-propagates (d) a countermeasure for protecting the heap. *Un ver est (a) un bug (b) un botnet (c) un malware qui se propage lui-même (d) une contremesure pour protéger la pile.*
- A CSRF originates from (a) stack manipulation (b) confusion between code and data (c) a Trojan horse (d) browsing a third party webpage. *Un CSRF provident (a) d'une manipulation de la pile (b) d'une confusion entre code et données (c) d'un cheval de Troie (d) de la navigation sur la page web d'une tierce partie*
- Exploiting a stack buffer overflow makes it possible to (a) modify the behavior of some software (b) modify the content of the heap (c) modify the content of the stack (d) modify the content of some protected memory region. *Exploiter un stack buffer overflow rend possible de (a) modifier le comportement d'un logiciel (b) modifier le contenu du tas (c) modifier le contenu de la pile (d) modifier le contenu d'une région mémoire protégée.*
- Stack canaris are meant to (a) protect the stack confidentiality (b) protect the stack integrity (c) modify the address of the process stack at startup (d) prevent the execution of code injected onto the stack. *Un canari de pile est destiné à (a) protéger la confidentialité de la pile (b) protéger l'intégrité de la pile (c) modifer l'adresse de la pile d'un processus à chaque démarrage (d) empêcher l'exécution de code injecté sur la pile*
- A race condition that may be exploited may arise from (a) processes running exclusively in sequence (b) accesses to shared variables (c) modifying the ESP register (d) non-atomic operations. *Une situation de concurrence exploitable peut survenir (a) lorsque des processus s'exécutent de manière exclusive en séquence (b) lors d'accès à des variables partagées (c) en cas de modification du registre ESP (d) pour des opérations non-atomiques.*

Question 7 (3 points)

A number of countermeasures relies on filtering user input in order to remove some dangerous characters. Provide a few examples of such mechanisms. Explain whether such a countermeasure is enough and why. *Nombre de contre-mesures s'appuient sur le filtrage des inputs utilisateur pour enlever des caractères dangereux. Donnez quelques exemples et expliquez si une telle contremesure est suffisante et pourquoi.*

Question 8 (8 points)

Define what these terms or acronyms mean and explain in one line what they refer to. *Définissez ce que ces termes ou acronymes signifient et expliquez en une ligne de quoi il s'agit.*

1. CSRF: .....
2. TOCTOU: .....
3. XSS: .....
4. SQLI: .....
5. Malware:.....
6. ROP: .....
7. ASLR:.....
8. Hash function:.....