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

Software Security – *Sécurité Logicielle*

Quizz #1 – 18/10/2017

- 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 9 minutes (except 3rd of time : 12 minutes) / *Vous avez 9 minutes (sauf tiers temps: 12 minutes)*
- Write your name, firstname, and group on every sheet / *Ecrivez nom, prénom et groupe sur chaque feuille*
- Selecting all **correct answers** will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. *Entourer toutes les **réponses correctes** à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.*
- **Selecting an incorrect answer will reduce the grade by 1 point.** ***Entourer une réponse incorrecte réduit la note de 1 point.***

Question 1 (2 points)

A CSRF attack can be prevented by / *Une attaque CSRF peut être évitée par* :
(a) the use of cookies / *l'utilisation de cookies*
(b) connecting to a single site within the browser / *la connexion à un seul site dans le navigateur*
(c) secret token validation / *la validation d'un secret*
(d) prepared queries / *des requêtes préparées.*

Question 2 (2 points)

In a SQL injection, / *Lors d'une injection SQL,*
(a) one can exfiltrate data from a database / *on peut exfiltrer des données d'une base de données*
(b) one can inject data into a database / *on peut injecter des données dans une base de données*
(c) one cannot delete database tables / *on ne peut pas détruire des tables de la base*
(d) one can obtain a root shell. / *on peut obtenir un shell root.*

Question 3 (2 points)

Indicate malware-related terms in the following list / *Indiquez les termes en relation avec les logiciels malveillants dans la liste suivante* :
(a) ransomware / *rançongiciel*
(b) vulnerability / *vulnérabilité*
(c) Trojan horse / *cheval de Troie*
(d) virus / *virus.*

Question 4 (2 points)

A worm is / *Un ver est*
(a) a vulnerability / *une vulnérabilité*
(b) a spyware / *un espiogiciel*
(c) a botnet / *un botnet*
(d) a malware that self-propagates / *un malware qui se propage lui-même.*

Question 5 (2 points)

List possible SQL injections : / *Listez les injections SQL possibles :*
(a) blind injections / *injections à l'aveugle*
(b) deaf injections / *injections muettes*
(c) union-based injections / *injections basées sur l'union*
(d) error-based injections / *injections basées sur les erreurs.*

Name, Firstname / *Nom, Prénom* : ..... correction

Software Security – *Sécurité Logicielle*

Quizz #2 – 15/11/2017

- 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 9 minutes (except 3rd of time : 12 minutes) / *Vous avez 9 minutes (sauf tiers temps: 12 minutes)*
- Write your name, firstname, and group on every sheet / *Ecrivez nom, prénom et groupe sur chaque feuille*
- Selecting all **correct answers** will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. *Entourer toutes les **réponses correctes** à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.*
- **Selecting an incorrect answer will reduce the grade by 1 point.** ***Entourer une réponse incorrecte réduit la note de 1 point.***

Question 1 (2 points)

In a buffer-overflow attack / Dans u*ne attaque par buffer overflow*
(a) the attack can happen on the stack / *l'attaque peut se produire sur la pile*
(b) the attack can happen on the heap / *l'attaque peut se produire sur le tas*
(c) the attack can happen on the text segment / *l'attaque peut se produire sur le segment de texte*
(d) the attacker will always own a root shell / *l'attaquant sera toujours en possession d'un shell root*

Question 2 (2 points)

During a ROP attack, / *Lors d'une attaque ROP,*
(a) one can exfiltrate data from a database / *on peut exfiltrer des données d'une base de données*
(b) one can inject data into a database / *on peut injecter des données dans une base de données*
(c) the ASLR will be a hindrance / *l'ASLR sera une gêne*
(d) one can obtain a root shell / *on peut obtenir un shell root*

Question 3 (2 points)

A race condition may be related to: / *Une attaque par course peut être liée aux termes :*
(a) concurrency / *concurrence*
(b) memory corruption / *corruption mémoire*
(c) Trojan horse / *cheval de Troie*
(d) maze / *labyrinthe*

Question 4 (2 points)

A stack-based buffer overflow relies on: / *Un dépassement de tampon sur la pile s'appuie sur :*
(a) a jump at the code copied into the buffer / *un saut vers le code copié dans le tampon*
(b) a jump at the address copied into the buffer / un saut à l'adresse copiée dans le tampon
(c) a jump at the address pointed by the base pointer / *un saut à l'adresse pointée par le base pointer*
(d) a jump at the address pointed by the stack pointer / *un saut à l'adresse pointée par le stack pointer*

Question 5 (2 points)

A return-to-libc attack: / *Une attaque par retour dans la libc :*
(a) does not work with ASLR / *ne fonctionne pas avec l'ASLR*
(b) relies on code injected by the attacker / *s'appuie sur le code injecté par l'attaquant*
(c) does not work with W XOR X countermeasures / *ne fonctionne pas avec les contremesures W XOR X*
(d) makes use of return statements / *s'appuie sur des instructions de retour*

Name, Firstname / *Nom, Prénom* : ..... Corrected

Software Security – *Sécurité Logicielle*
Quizz #3 – 06/12/2017

- 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 9 minutes (except 3rd of time : 12 minutes) / *Vous avez 9 minutes (sauf tiers temps: 12 minutes)*
- Write your name, firstname, and group on every sheet / *Ecrivez nom, prénom et groupe sur chaque feuille*
- Selecting **all correct answers** will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. *Entourer toutes les **réponses correctes** à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.*
- **Selecting an incorrect answer will reduce the grade by 1 point. *Entourer une réponse incorrecte réduit la note de 1 point.***

Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / *Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?*

(a) Encryption / *le chiffrement*
(b) Privacy enforcement techniques / *les mécanismes de protection de la vie privée*
(c) Digital signature / *la signature numérique*
(d) Hash functions / *les fonctions de hachage*

Question 2 (2 points)

Digital signature : / *La signature numérique :*

(a) can ensure the non-repudiation of origin / *peut assurer la non-répudiation d'origine*
(b) can ensure the non-repudiation of destination / *peut assurer la non-répudiation de destination*
(c) relies on symmetric encryption / *s'appuie sur le chiffrement symétrique*
(d) may use hash functions / *peut utiliser des fonctions de hachage*

Question 3 (2 points)

Symmetric block ciphers may rely on: / *Les chiffres symétriques peuvent s'appuyer sur :*

(a) permutations / *des permutations*
(b) corruptions / *des corruptions*
(c) substitutions / *des substitutions*
(d) transpositions / *des transpositions*

Question 4 (2 points)

For block ciphers: / *Pour des chiffrements par blocs:*

(a) CBC mode offers a good protection / *le mode CBC offre une bonne protection*
(b) ECB mode offers a good protection / *le mode ECB offre une bonne protection*
(c) CTR mode offers a good protection / *le mode CTR offre une bonne protection*
(d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / *le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré*

Question 5 (2 points)

Security: / *La sécurité:*

(a) often improves usability / *améliore souvent l'utilisabilité*
(b) may introduce new vulnerabilities / *peut introduire de nouvelles vulnérabilités*
(c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
(d) aims at reducing risks to assets / *vise à réduire les risques sur le capital et ressources informatiques*