Sécurité du développement

Commencé le	Monday 14 April 2025, 11:30
État	Terminé
Terminé le	Monday 14 April 2025, 11:48
Temps mis	18 min 26 s

Question **1**
Terminé
Noté sur 2,00
Marquer la question

never use **printf(3)** with a format string provided by an attacker.

Ne jamais utiliser **printf(3)** avec une chaine de format fournie par un assaillant.

- [x] a. That format string can even be used to write to memory, using the correct format specifier.

  Cette chaine de format permet même d'écrire en mémoire, en utilisant le bon spécificateur de format.
- [x] b. That format string can be used to display "extra" parameters, which will often be sensitive information on the stack, including memory addresses (leading to address leaks that can be the missing ingredient to exploiting a buffer overflow, for instance)

  Cette chaine de format pourra être utilisée pour afficher des paramètres en plus, qui peuvent être des informations confidentielles sur la piste, en particulier des adresses mémoire (la fuite d'adresse étant souvent un prérequis à l'utilisation d'un débordement de tampon par exemple).

Question **2**
Terminé
Noté sur 2,00
Marquer la question

CVE:

- [ ] a. A specialized CI (continuous integration) system based on cvs (an ancestor of git) oriented towards bug fixes: every known security issue corresponds to a number test in that system.

  Un système d'intégration continu basé sur cvs (un vieil équivalent de git) spécialisé dans les tests de correction de bug: chaque problème de sécurité connu fait l'objet d'un test numéroté dans ce système.
- [ ] b. A database of known attacks for penetration testers.

  Une base de données d'attaques pour les consultants qui font des tests de pénétration.
- [x] c. A centralized database of security issues, independently of the operating system, that associates a unique identifier to each problem.

  Une base de donnée centralisée de problèmes de sécurité, indépendante de l'OS, qui associe un identifiant unique à chaque problème.

Question **3**
Terminé
Noté sur 2,00
Marquer la question

On modern systems, buffer overflows on the stack are made harder to exploit by the following techniques.Sur les systèmes modernes, les buffer overflows sur la pile sont rendus plus difficiles à exploiter par les techniques suivantes:

- a. Address randomizationAdressage aléatoire
- b. Guard pagesAddresse randomizationPages de gardeAdressage aléatoire
- c. Address randomizationNon executable stacksCanarisAdressage aléatoirePile non executableCanaris

Question **4**
Terminé
Noté sur 2,00
Marquer la question

What is a canari ?Qu'est-ce qu'un canari ?

- a. A known sequence of bits used to detect various overflowsUne valeur donnée utilisée pour détecter des débordements divers
- b. A series of zeroes used to properly terminate buffers to avoid overflowsUne série de zéros placée en fin de tampon pour éviter les débordements
- c. A known sequence of bits written by the compiler over an attacker's buffer overflow to restore normal behaviorUne valeur donnée que le compilateur écrit par dessus un débordement de tampon pour recréer un comportement normal

Question **5**
Terminé
Noté sur 2,00
Marquer la question

qu'appelle-t-on un "zero day" ?
What's the meaning of "zero day" ?

- [ ] a. un jour blanc, où aucun nouveau code n'est écrit, car tout le monde se consacre à la recherche de bugs
  a day where no developer writes any new code, rather everyone is hunting for bugs.
- [ ] b. la date de sortie d'une version majeure de logiciel, où tous les dev attendent les rapports de bug
  major software release date, with all developers anxiously awaiting bug reports
- [x] c. un bug qu'on découvre car des exploits circulent dans la nature, avant l'existence de correctifs
  A bug discovered after exploits are already spotted in the wild, thus before any fix exists.

Question **6**
Terminé
Noté sur 2,00
Marquer la question

When you are root (uid = 0)/
Lorsqu'on est root (uid = 0)

- [x] a. The system will still check permission rights before granting you access to a file
  Le système va quand même vérifier les droits d'un fichier avant de vous permettre d'y accéder.
- [ ] b. The system will almost never check permission right, except for NFS mounts and immutable files
  Le système vous laissera accéder à presque tous les fichiers sans vérifier les permissions, à l'exception des montages NFS et des fichiers immutables.
- [ ] c. The system will never check permission rights before granting you access to a file
  Le système ne va jamais regarder les permissions et vous donner accès à tous les fichiers

Question **7**
Terminé
Noté sur 2,00
Marquer la question

The following snippet could be an excerpt from a service program starting as root.
L'extrait suivant pourrait provenir d'un programme de service tournant en tant que root.

```
1 ...
2 /* this starts as root */
3 /* open and read the config file */
4 int fd = open_config_file();
5 if (fd != -1)
6         err(1, "Couldn't open config");
7 if (!parse_config_file(fd))
8         err(1, "Couldn't read config");
9 close(fd);
10
11 /* find the service login creds */
12 struct passwd *creds = getpwnam(config->name);
13 if (!creds)
14         err(1, "Daemon %s doesn't exist", config->name);
15 /* change identity */
16 setuid(creds->pw_uid);
17 setgid(creds->pw_gid);
18 ...
~
~
~
~
~
```

One the lines is very wrong !
Une des lignes est très très fausse.

Réponse : 16

Question **8**
Terminé
Noté sur 2,00
Marquer la question

Vrai ou faux: si un attaquant a accès au code binaire d'un programme, c'est généralement suffisant, il existe des outils qui permettent de décompiler un programme, ou de l'exécuter en pas en pas. Le fait de disposer du code source n'est qu'un bonus pour la plupart des attaquants chevronnés.

True or false: if an attacker has the binary code they want to attack, it's generally quite enough. There are tools that allow decompiling most such programs, along with debugger-like tools that allow running through it step-by-step. Having the source code on the side is just a bonus for most seasoned attackers.

Veuillez choisir une réponse.

- (•) Vrai
- ( ) Faux

Question **9**
Terminé
Noté sur 2,00
Marquer la question

Randomizing memory addresses makes the task of attackers more difficult, as they have to craft a payload tailored to a given process, but they also make debugging more difficult, since crashes can't be reproduced with certainty. Hence the need to actually debug every crash using core dumps and a trusty debugger.

La randomisation des adresses mémoire rend la vie dure aux attaquants, qui doivent fignoler leur attaque pour s'adapter à la cartographie mémoire d'un processus donnée, mais elle rend aussi le debug plus difficile, car les crashs ne sont pas toujours reproductibles. D'où la nécessité d'apprendre à debugguer à partir d'un core dump et d'un bon debugger.

Veuillez choisir une réponse.

- (•) Vrai
- ( ) Faux

Question **10**
Terminé
Noté sur 2,00
Marquer la question

L'API SQL **select** ne devrait jamais être utilisée: comme elle permet d'utiliser des paramètres, elle peut conduire aux mêmes problèmes de chaine de format que **printf**, et donc à des fuites d'adresse mémoire.

The SQL **select** API should never be used: as it allows passing parameters to an sql squery, it leads to the same kind of problems that make **printf** so dangerous, including memory address leaks.

Veuillez choisir une réponse.

- ( ) Vrai
- (•) Faux

Terminer la relecture