SLH - 2024

Midterm

SLH 2024

Maxime Augier

21 novembre 2024

Nom :

Prénom :

Indications :

- Tout matériel pédagogique est autorisé.
- L'accès a Internet est autorisé.
- L'utilisation de LLM est autorisée.
- Toute communication avec d'autres personnes est interdite.
- Le rendu se fait en ligne sur Cyberlearn, en déposant un fichier `.md` pour les réponses textuelles, et les sources complétées

Total: 40 points

Questions Générales (13 pts)

1) Est-il possible d'utiliser un token anti-CSRF contenant toujours la même valeur que le cookie, ou celà annule-t-il complètement l'effet de protection contre les CSRF ? **(2 pts)**

2) Le lab 1 portait sur deux attaques; les CSRF et une autre attaque. Quel outil de sécurité est typiquement utilisé pour automatiser l'exploitation de cette autre attaque ? **(1 pt)**

3) Vous êtes un chercheur en sécurité et vous avez découvert la vulnérabilité logicielle suivante: si on envoie à l'utilisateur ciblé un email, dans lequel on lui demande d'ouvrir un shell et d'exécuter la commande `rm -rf /*`, le shell déclenche une cascade d'actions dont le résultat final est de détruire le système de fichiers de la machine ciblée.

Sous quelle CWE peut-on classer cette vulnérabilité ? Calculez son score CVSS. **(2 pts)**

4) Quelle **vulnérabilité** ayant un impact sur l'**intégrité** est présente dans le fragment de code suivant ? **(2 pts)**

```
public void write_data(String filePath) throws IOException {
    try {
        File file = new File("", filePath);
        if (file.exists()) {
          throw new IOException("file exists");
        }
        FileOutputStream fs = new FileOutputStream(file);
        fs.write(get_my_arbitrary_data().getBytes());
        fs.close();

    } catch (IOException e) {
        System.out.println("Exception: " + e.getMessage());
    }
}
```

5) Voyez-vous d'autres problèmes avec ce code ? **(2 pts)**

6) Donnez une expression régulière avec laquelle on peut filtrer du HTML fourni par un utilisateur, pour éliminer le risque d'une attaque XSS **(2 pts)**

7) Qu'est-ce qui est le plus pratique à utiliser, `execve()` ou `system()` ? **(2 pts)**

Revue de code (12 pts)

Considérez le code fourni dans `market.c`, qui implémente un service illégal de vente de drogue sur le darknet.

Trouvez et corrigez:

8) un problème de gestion mémoire. **(2 pts)**

9) un problème de débordement. **(2 pts)**

10) un problème d'utilisation d'une API intrinsèquement dangereuse **(2 pts)**

11) un problème de validation d'entrée. **(2 pts)**

12) un problème de traitement d'erreur incorrect. **(2 pts)**

13) un problème de logique métier. **(2 pts)**

Rust (15 pts)

Nous sommes en 2050 au Sécuristan, une brutale dictature totalitaire qui utilise une intelligence artificielle pour surveiller les agissements des citoyens. Une pandémie de corpwnavirus se répand a grande vitesse dans la population; votre mission est de traiter le flux d'information sorti de l'IA pour effectuer un traçage de contacts et identifier le patient zéro.

Le fichier `events.txt` contient une liste d'évenements de surveillance. Certains de ces évènements ne sont pas pertinents pour le traçage de contacts; d'autres indiquent qu'une contamination à pu se produire, soit bidirectionnelle (chaque personne aurait pu infecter l'autre), soit unidirectionnelle (la contamination ne peut aller que dans un seul sens).

Le fichier contient également des évènements de tests, indiquant qu'une personne a testé positivement ou négativement à la présence du virus.

14) Implémentez la fonction `persons`, qui reconnaît et extrait le nom des personnes mentionnées dans une ligne de log **(7 pts)**

15) Implémentez la fonction `parse_event`, qui parse une ligne de log, et produit une description structurée de l'évènement, telle que définie dans le template de code. **(8 pts)**

Bonus (+5 pts)

Implémentez un algorithme qui identifie les personnes pouvant potentiellement être le patient zéro, sachant que:

- Au moment ou débute le log, une seule personne (le patient zéro) est infectée
- Le taux de transmission est de 100% pour les évènements présents dans le log
- Aucune transmission ne peut avoir lieu sans la présence d'un évènement dans le log
- Les tests, positifs ou négatifs, sont fiables à 100%
- Le virus peut infecter la même personne plusieurs fois (pas d'immunité)
- Il n'existe pas deux personnes différentes ayant le même nom et prénom.

Pour identifier le patient zéro, vous pouvez utiliser l'algorithme suivant:

- Pour chaque personne P, on note C_P l'ensemble des contaminants de P à l'instant présent, c'est à dire les personnes Q pour lesquelles il existe une chaîne de transmission, non interrompue par un test négatif, allant de Q à P; et on note S l'ensemble des personnes suspectées d'être le patient zéro.
- A l'instant zéro (début du log) toutes les personnes sont suspectes, et chaque personne est elle-même son seul contaminant:

$$\forall P : (C_P := \{P\})$$

$$S = \{\forall P : P\}$$

- À l'instant où une personne A contamine une personne B, l'ensemble des contaminants de A vient s'ajouter à celui de B:

$$C_B := C_B \cup C_A$$

- À l'instant où une personne P obtient un test négatif, il n'a plus de contaminants possibles:

$$C_P := \emptyset$$

- À l'instant où une personne P obtient un test positif, le patient zéro fait partie de C_P, et on peut exclure tous les autres suspects:

$$S := S \cap C_P$$

FIN

PAGE VIDE