ITÉRATION 2

Dépendances

Modalités

- Travail individuel en autonomie
- 1,5 jour en présentiel

Objectifs

Dans les applications, les dépendances à d'autres modules sont partout. Nous aborderons le sujet de la mise à jour des dépendances et des outils qui peuvent aider.

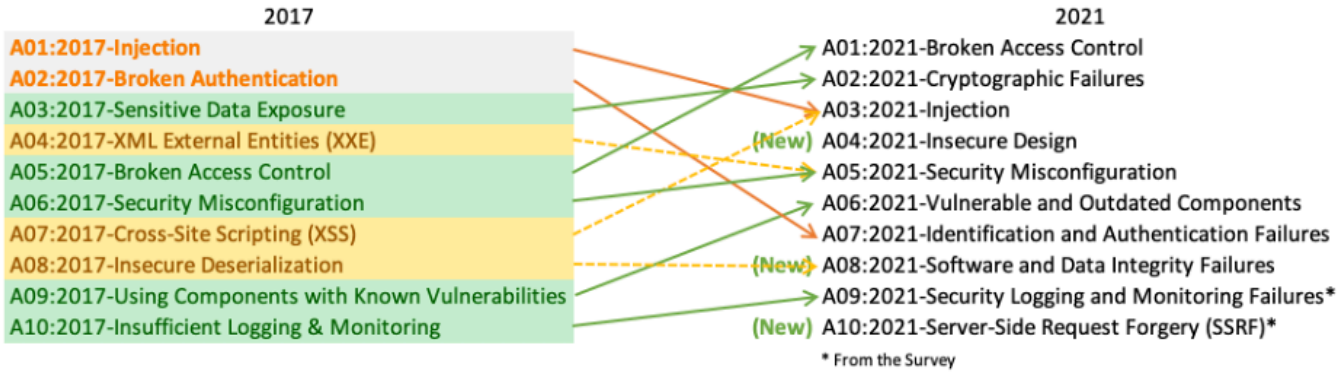
Compétences

- Diagnostiquer un dysfonctionnement et le corriger
- Mettre à jour le projet avec ses dépendances

1.1 — Le rôle des dépendances (et l'exemple de log4j)

1h — Présentiel

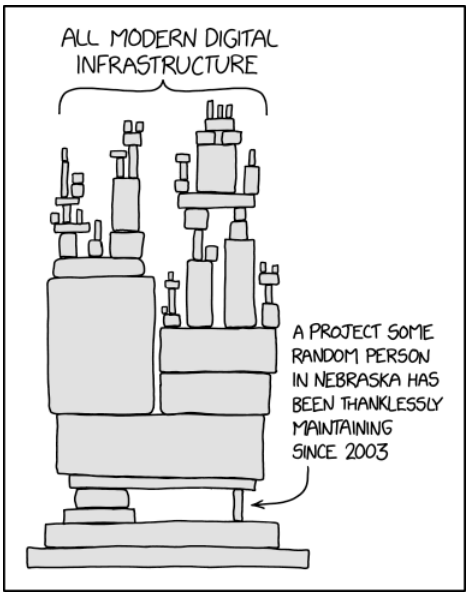
Dans ce module, nous allons parler de l'élément 6 de la liste OWASP (https://owasp.org/www-project-top-ten/): composants vulnérables ou non mis à jour.



Pouvez-vous dire pourquoi ?

Généralement, une application dépend de dizaines, voire de centaines ou de milliers de bibliothèques et d'outils. Si l'un d'entre eux a un problème de sécurité, votre application a également un problème.

Assez souvent nous connaissons des dépendances directes, mais pas toujours des dépendances de dépendances. Un épisode de XKCD (https://xkcd.com/2347/) sur le sujet :



Fin 2021, il y avait un problème de sécurité important dans une bibliothèque de journalisation appelée log4j. Le problème permettait l'exécution de code à distance et des applications utilisant une version vulnérable sont encore trouvées de temps en temps.

Il existe plusieurs articles sur la question dans “ressources”. Je recommande de lire au moins [2] ou [3]. Connaissez-vous une application utilisant log4j ?

RESSOURCES

- La liste “top 10” de OWASP https://owasp.org/www-project-top-ten/
- [2] Comment fonctionne la vulnérabilité log4j, avec des liens vers des vidéos https://www.upguard.com/blog/apache-log4j-vulnerability
- [3] Log4j explained - https://www.swarmnetics.com/blog/apache-log4j-vulnerability-explained/
- https://nvd.nist.gov/vuln/detail/CVE-2021-44228
- Bulletin d'alerte du CERT-FR sur log4j https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-022/
- “Un an après la découverte de Log4j, l'extrême vulnérabilité, des organisations n'ayant pas appliqué les correctifs” - ah oui… https://www.zdnet.fr/actualites/un-an-apres-la-decouverte-de-log4j-l-extreme-vulnerabilite-des-organisations-n-ayant-pas-applique-les-correctifs-39950002.htm

COMPÉTENCES ASSOCIÉES

- Diagnostiquer un dysfonctionnement et le corriger

1.2 — Conduit… le retour

1h — Présentiel

Nous avons déjà travaillé avec l'application "conduit". Réinstallons l'application en local ou dans une VM, nous allons travailler sur ses dépendances.

Remarque : selon la version du système que vous utilisez, il peut être nécessaire de finir les tâches 1.4 et/ou 1.5 pour installer l'application (en cas d’un erreur pendant ‘`composer install`’).

RESSOURCES

- https://github.com/LivingStoneHgS/conduit-backend-tests

COMPÉTENCES ASSOCIÉES

- Diagnostiquer un dysfonctionnement et le corriger

1.3 — Dependencies de “conduit”

2h — Présentiel

Quelles sont les dépendances de "conduit" ?
Que devez-vous installer pour l'exécuter ? Dans quelle version ?
Y a-t-il des indices dans le code source ?
Existe-t-il des fichiers contenant de telles informations ?

Rédigez une note avec une liste des dépendances et leurs versions actuelles.

Choisissez 3 dépendances qui, selon vous, pourraient avoir une implication sur la sécurité et recherchez leurs dernières versions. Quelle est la différence avec celui que vous avez ? Y a-t-il des problèmes de sécurité ? (vous pouvez consulter les *release notes* ou utiliser le script que vous avez développé dans le dernier module).

Ajoutez votre analyse à la note.

RESSOURCES

- https://github.com/LivingStoneHgS/conduit-backend-tests
- https://ubuntu.com/security/notices

COMPÉTENCES ASSOCIÉES

- Diagnostiquer un dysfonctionnement et le corriger

1.4 — Mises à jour applicatifs

2h — Présentiel

L'application a une version de ses dépendances définies (regardez dans les fichiers .json).

Comment pouvez-vous le mettre à jour avec tous les correctifs récents ?

RESSOURCES

https://www.freecodecamp.org/news/how-to-update-npm-dependencies/
https://www.lecoindunet.com/difference-apt-update-upgrade-full-upgrade

COMPÉTENCES ASSOCIÉES

- Mettre à jour le projet avec ses dépendances

1.5 Mises à jour du système

2h — Présentiel

Un certain nombre de bibliothèques utilisées par l'application proviennent du système. Mettez-le à jour. Pour un peu plus de difficulté, vous pouvez envisager de mettre à jour la version de la distribution, par exemple dans Debian, en passant de *stable* à *testing*.

Assurez-vous que l'application fonctionne après la mise à jour. Comment pourriez-vous tester la mise à jour automatiquement ?

RESSOURCES

- https://www.lecoindunet.com/difference-apt-update-upgrade-full-upgrade

COMPÉTENCES ASSOCIÉES

- Mettre à jour le projet avec ses dépendances

1.6 Automation avec dependabot

2h — Présentiel

Il est possible d'automatiser les mises à jour de vos dépendances. Bien sûr, la plupart du temps lorsque la mise à jour fonctionne parfaitement, tous les problèmes doivent être résolus manuellement. Dependabot est un outil sur GitHub permettant exactement cela. Pouvez-vous configurer dependabot avec conduit ?

RESSOURCES

- Documentation officielle: https://docs.github.com/en/code-security/dependabot
- Dependabot en 1 minute: https://www.youtube.com/watch?v=yvXKlDgiGHo

COMPÉTENCES ASSOCIÉES

- Mettre à jour le projet avec ses dépendances

Livrables

Dans ce projet, nous devrions avoir :

- ➔ Une note avec la liste de dépendances de conduit et quelques exemples plus détaillés
- ➔ Fichiers de dépendance de conduit après la mise à jour