Protocole d’expérimentation FDI-LEEX

Période d’expérimentation :
Date de début : 22/02/2023
Date de fin : jj/mm/aaaa

Membre du groupe :

- lecler_a
- bouyer_l
- fremon_g
- guiffa_g
- plouy-_e

Contexte :
Un nouveau développeur à été recruté en alternance. Lors de sa première mission, il est amené à développer une fonctionnalité nécessitant une connexion à une base de données.

Sa fonctionnalité consiste à s’authentifier afin d’accéder à une page monitorant des VMs client, contenant donc des informations assez sensibles.

Son projet a été validé par l’équipe de développement ainsi que le chef de projet et une mise en production sur le serveur client a été effectuée.

Mais il s’avère que quelques mois plus tard, le client contacte l’entreprise pour lui annoncer une mauvaise nouvelle : le client s’est fait piraté et ses informations sont exposées. Le dossier a été remis à notre équipe pour découvrir comment cela a pu se produire et espérer retrouver ces attaquants.

Nous voulons donc comparer les différentes failles connues à l’aide du site de l’OWASP afin de déterminer plus précisément la faille exploitée par les attaquants et suggérer au développeur les améliorations possibles.

Objet du protocole :
Le protocole consiste donc à se mettre dans les mêmes conditions de l’attaquant et tester différentes failles afin de déterminer la cause. Une fois la cause trouvée, nous allons expérimenter différentes solutions afin de déterminer si une solution est meilleure qu’une autre, si nous avons besoin de l’entièreté des solutions trouvées et comment celles-ci impactent le développement.

Objectif détaillé :

- L'objectif dans un premier temps :

Dans un premier temps, l'objectif de ce protocole est de déterminer la faille exploitée par les attaquants et ainsi effectuer les correctifs nécessaires. Pour cela, nous allons devoir tester les différentes possibilités d'accès aux informations et parvenir à celles-ci. Nous allons également tester les différents correctifs afin de comprendre comment développer différemment pour satisfaire un certain degré de sécurité et qu'impactent les changements.

- L'objectif dans un second temps :

Dans un second temps, l'objectif est de sensibiliser l'alternant mais également l'équipe de développement aux bonnes pratiques afin qu'ils réduisent considérablement les failles pouvant être utilisées pour récupérer les données par des personnes tiers et leur faire adopter les solutions adéquatement.

Environnement de test :

Création du contexte :

- Créer une BDD pour reproduire la situations décrite
- Créer des scénario d'attaques et des scripts les simulants

Pour les technologies, la base de données sera mySQL et pour ce qui est du code, nous le développerons en php8.
Nous aurons accès à la même base de données via Docker.

Nous utiliserons également burp pour voir ce qu'il se passe quand on envoie une requête. Nous pourrons faire un comparatif avec wireshark afin de déterminer si un outil est plus efficace que l'autre pour cette expérimentation.

Solutions :
Nous aborderons les requêtes préparées en sql, la complexité des mots de passe, les systèmes de timer d'authentification ainsi qu'une bonne gestion des droits utilisateurs avec des comptes adéquats.

Protocole d'expérimentation :

Test de nos solutions :

- Mise en place de protocole de détections
- Mise en place de protocole de sécurité
- Jeu des scripts d'attaque
- Comparaison des résultats de défense

Documentation :

SIte de l'OWASP : https://owasp.org/
Exemple d'injections SQL : https://book.hacktricks.xyz/pentesting-web/sql-injection
Injections et bonnes pratiques : https://www.vaadata.com/blog/fr/injections-sql-principes-impacts-exploitations-bonnes-pratiques-securite/

Extension possible :

Si notre projet devait aller plus loin, nous pourrions :

- Tester d'autres types d'attaques (ne pas se limiter à des injections SQL)
- Créer différentes failles dans notre application afin de les exploitées
- Enrichir le site/la db de manière générale

Note de synthèse / observations :

TODO