|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Établissement de formation**  **de Saint Berthevin** | | Nom, Prénom : ZWICK Erwan  Section : | |
| Matière : **Dévloppement de modules sécurisés** | | | Nom du formateur : | |
| Thème étudié :  Objectif pédagogique : | | | | Cours |
| Exercices |
| Evaluation |
| Note obtenue : |
| Corrigé |
| Date : | | Appréciations : | | |

**https://github.com/mflasquin/learning-security**

**1 – Faites fonctionner le TP login sur votre machine**

**2 – Listez les failles potentielles dans l’application (servez vous du top 10 de l’OWASP)**

A1 :2017 :Injection SQL au niveau de l’URL de la page informations.php on peut insérer une requête telle que :

« informations.php?id= (select count(\*) from users where password like "%password%") » pour pouvoir deviner le mot de passe de façon aveugle.

A2:2017-Broken Authentication l’enregistrement des mots de passe se fait en clair dans la base de données

A5:2017-Broken Access Control l’accès aux pages fonctions et informations ne contrôle pas la présence d’un utilisateur connecté. Une personne avec le lien vers ces pages peut donc les afficher.

A7:2017-Cross-Site Scripting (XSS) au niveau du formulaire d’enregistrement register.php, on peut insérer du code JS, tel que « <script>alert(‘coucou’) </script> », dans le champs « champs d’utilisateur », script qui sera ensuite exécuté lorsqu’un utilisateur affichera la page d’information de l’utilisateur.

https://github.com/Erwanwan1/learning-security

**3 – Proposez un moyen de corriger ces failles**

**4 – Sur la page d’inscription ‘register.php’ améliorez le champ de mot de passe en proposant à l’utilisateur de saisir un mot de passe fort (avec zxcvbn par exemple)**

**5 – Stocker le mot de passe de manière sécurisée**

**6 – Mettre en place un système de captcha sur l’inscription / login**

**7 – Mettre en place un système de connexion avec OAuth2**