|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| a | **Établissement de formation**  **de Saint Berthevin** | | Nom, Prénom :  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**

OK !!

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

**Broken Access Control** - Possibilité d’accéder à la page d’informations sans devoir être connecté, on peut modifier l’id pour accéder à toutes les pages d’informations.

**Injection SQL** - Possibilité de modifier la structure de la DB et de la supprimer: <http://localhost/learning-security/authentication/informations.php?id=1;drop%20database%20authentication>

**Injection XSS** – Créer un compte avec ce username la : <script>alert('test')</script>

**Mot de passe en claire dans la BDD**

**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**