Exercice 1 :

Mot de passe : **Pr0t3g3z_V0s_Acc3s_1nd1r3ct**

- Comment reproduire la faille : Ne pas contrôler si l'utilisateur a l'autorisation d'accéder à une page
- Comment trouver la faille : Le bouton dans le code source mène à la page perdu.html, pour accéder à une page différente il suffit de taper le nom du fichier dans l'URL.
- Comment corriger la faille : Vérifier que la personne dispose des accès pour accéder à la page

Exercice 2 :

Mot de passe : **N3_p@s_St0ck3r_L3s_M0ts_D3_P@ss3_D@ns_L3_Fr0nt**

- Comment reproduire la faille : En stockant le mot de passe dans le front
- Comment trouver la faille : Ouverture du fichier exo2.js, le mot de passe et le nom d'utilisateur est stocké en dur dans le fichier
- Comment corriger la faille : Ne pas stocker les mots de passe en dur dans son code

Exercice 3 :

Dans le input :

- Comment reproduire la faille : Interpréter les balises html dans les input
- Comment trouver la faille : Interpréter des balises HTML en y ajoutant du javascript
- Comment corriger la faille : Filtrer les données et échapper les données dynamiques

Exercice 4 :

Mot de passe : Jc8b&RM52AL

- Comment reproduire la faille :
- Comment trouver la faille : Aller dans inspecter l'élément → réseau
  Lancer une requête de connexion → ouvrir la requête généré → on obtient un champ X-Psw et X-User

Exercice 5 :

Dans inspecter l'élément : conditions du reseau → agent utilisateur decocher et rentrer toto dans champs en dessous

- Comment trouver la faille : Allez dans inspecter l'élément, partie réseau lancer une requête en cliquant sur "se connecter", des fichiers user-agent sont généré, en ouvrir un et on trouve le nom de l'agent qui est "toto"
- Comment corriger la faille : Changer le user-agent

Exercice 6 :

Mot de passe : 1=1' ;--

- Comment reproduire la faille : En injectant du SQL dans les champs de saisie ou dans l'URL, en n'utilisant pas de requête préparée et en ne vérifiant pas les données
- Comment trouver la faille : Entrer 1=1 suivie d'une apostrophe pour simuler une fin de requête, un ";" pour simuler la fin d'une ligne suivie de "—" pour mettre le reste du code en commentaire
- Comment corriger la faille : Utiliser des requêtes préparées, échapper les éléments dynamiques

Exercice 7 :

- Comment trouver la faille : Copier-coller le script, supprimer les 2 dernières parenthèse et les remplacer par .toString
- Comment corriger la faille : Ne pas stocket le mot de passe même si il est obfusquer.

Mot de passe : toto123lol