Exercice 1 :

Mot de passe : **Pr0t3g3z_V0s_Acc3s_1nd1r3ct**

Il suffit de mettre dans l'url « success.html » au lieu de « index.html » pour accéder à la page.

Pour protéger ce site, il faudrait vérifier les droits de la personne avant d'arriver sur la page.

Exercice 2 :

Identifiant : Admin

Mot de passe : GKyMxMNdNYrMFtvXae14

Il suffit d'inspecter le code, regarder le contenu du fichier javascript afin de déterminer les identifiants valides.

Il faut faire une vérification coté serveur afin que l'hackeur ne puisse pas déterminer les identifiants de cette façon.

Exercice 3 :

Il suffit d'écrire dans la zone de texte :

Pour éviter cette faille, je filtre les données reçues d'un tiers avant de les stocker

Exercice 4 :

Il faut se rendre dans le navigateur, essayer de se connecter avec des identifiants au hasard et allez inspecter le code dans la section réseau, la méthode GET que l'on perçoit nous permet de déterminer ensuite les identifiants valide qui sont :

Identifiant : CalvinKim

Mot de passe : Jc8b&RM52AL

Pour éviter cette faille, il faut éviter d'utiliser la méthode GET pour des informations importantes.

Exercice 5 :

Pour cet exercice, j'ai utilisé le navigateur Chrome, j'ai inspecté le code de la page et suis allez dans l'onglet Console > More Tools > Network Conditions > Décocher la sélection automatique de l'user agent et y insérer l'user agent valide « toto » que l'on retrouve de la même façon que le précédent exercice, on essaie de se connecter et on vérifie les requêtes dans l'onglet réseau, ainsi on peut déterminer l'user-agent valide.

Pour éviter cette faille, il faut éviter d'utiliser la méthode GET pour des informations importantes.

Exercice 6 :

Pour cet exercice, il faut entrer « 'OR 1 = 1 /* » afin de modifier la requête SQL et d'autoriser la connexion de manière très simple (1 = 1).

Pour éviter ce genre d'injection SQL, il faut utiliser des requêtes préparées.

Exercice 7 :

Ici, il faut utiliser un Désobfuscateur afin de traduire le JS natif en UTF 8, ainsi on peut déterminer le mot de passe qui est toto123lol.

Pour éviter ce genre de faille, il faut éviter d'utiliser la méthode GET et passer par le serveur plutôt que par le client pour les vérifications de données.