Exercice 1 :

Mot de passe : **Pr0t3g3z_V0s_Acc3s_1nd1r3ct**

Pour accéder à la page succès j'ai juste eu besoin de modifier l'url de l'exercice 1 en rajoutant a la fin de l'url succées.html

Cette faille est une faille du type accès indirect non autorisé pour régler ce problème il faut vérifier que l'utilisateur a bien les droits d'accès à la page concernée.

Exercice 2 :

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

Pour trouver le mot de passe utilisateur et l'identifiant j'ai juste eu a ouvrir la console de mon navigateur dans l'onglet réseau l'identifiant et le mot de passe sont écrit en dur dans le code javascript.

Pour pallier à cette faille j'aurais vérifier dans le serveur pour l'identifiant et le mot de passe et non coté client.

Exercice 3 :

Pour trouver la faille j'ai dû dans le champ de commentaires injecter une image qui lancait un script javascript

Pour pallier a cette faille je filtrerai les données d'un tiers avant de les stocker.

Exercice 4 :

Pour trouver l'identifiant et le mot de passe j'ai dû ouvrir la console de mon navigateur dans l'onglet réseau. J'ai écrit un identifiant et un mot de passe bidon j'ai pu lire le bon identifiant et mot de passe dans la méthode GET Identifiant : CalvinKim Mot de passe : Jc8b&RM52AL

Pour pallier à cette faille je n'utiliserai pas la méthode GET pour des actions importantes et échapper les données dynamiquement et ne pas les afficher.

Exercice 5 :

Pour trouver la faille j'ai du aller dans la console de mon navigateur dans l'onglet réseau puis j'ai appuyer sur le bouton ce connecter j'ai pue voir que le serveur attendais un user agent = « toto », j'ai juste eu a changer mon user agent en toto et j'ai pu me connecter.

Pour pallier a cette faille je ne montrerais pas l'user agent dans la méthode GET.

Exercice 6 :

Pour trouver cette faille j'ai écrit un identifiant et un mot de passe bison sur le serveur j'ai pue voir que la requête ce fessait avec des guillemets alors a la place d'un identifiant j'ai écrit 'OR 1=1 /* j'ouvre une simple cote j'écrit un vérification toujours vraie et j'ouvre un commentaire a la fin pour ne pas lancer la fin de la requête du serveur.

Pour pallier a cette faille j'utiliserais les requêtes préparées et j'échapperai les éléments dynamiquement.

Exercice 7 :

Pour trouver cette faille j'ai dû aller dans le code javascript j'ai trouver une fonction encoder je l'ai décoder a l'aide du site https://www.dcode.fr/desobfuscateur-javascript . Ce site ma retourné :

```
function anonymous( ) { a=prompt('Entrez le mot de
passe');if(a=='toto123lol'){alert('bravo');}else{alert('fail...');} }
```

Mot de passe : toto123lol

Pour pallier a cette faille je n'utiliserai pas la méthode GET ni le client pour vérifier le mot de passe mais avec le serveur.