

## Rapport Devoir Sécurité :

### Exercice 1 :

**Comment trouver la faille :**

On fait un accès indirect a la page depuis l'ULR et on trouve le mot de passe :

**Pr0t3g3z\_V0s\_Acc3s\_1nd1r3ct**

**Solution de correction :**

Pour éviter ce genre de problème on doit faire en sorte de ne pas partir du principe que si un utilisateur ce trouve sur une page c'est qu'il a le droit.

### Exercice 2 :

**Comment trouver la faille :**

On recherches les informations de connexion dans le front en inspectant la page et on trouve le mdp :

**N3\_p@s\_St0ck3r\_L3s\_M0ts\_D3\_P@ss3\_D@ns\_L3\_Fr0nt**

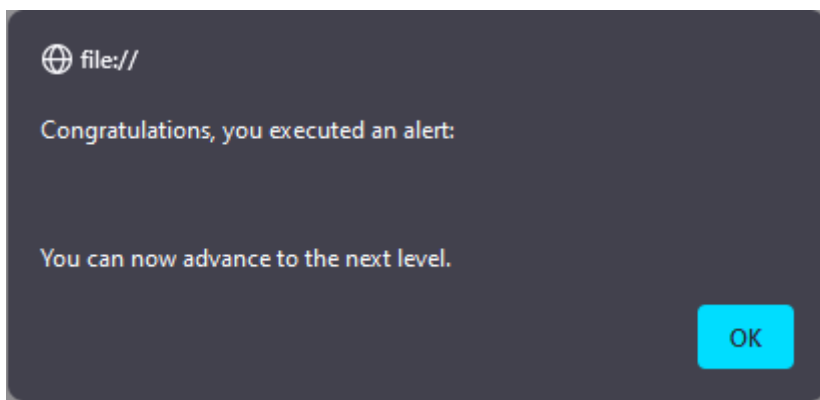
**Solution de correction :**

Pour éviter ce genre de faille il suffit de ne pas renseigner les identifiants dans le front de la page. Ou mettre en place un hachage.

### Exercice 3 :

**Comment trouver la faille :**

On insere une image qui contiendra un onerror dans laquelle se trouvera une alert()



**Solution de correction :**

Pour éviter ce genre de faille il suffit d'échapper les caractères

## Exercice 4

**Comment trouver la faille :**

On recherche dans les entêtes de la console et on trouve que la console nous renvoie les identifiants attendus par le serveur :

```
X-Psw: Jc8b&RM52AL  
X-User: CalvinKim
```

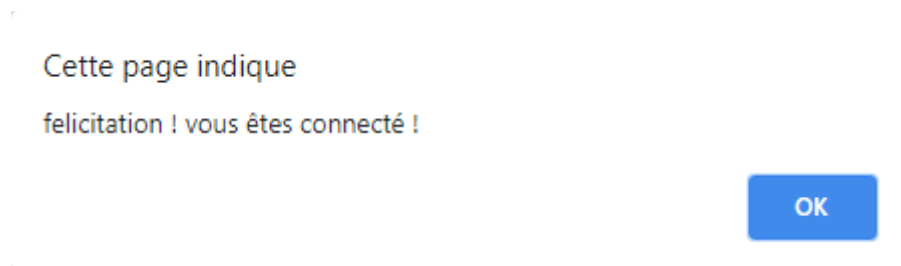
On trouve le mot de passe : Jc8b&RM52AL

**Solution de correction :**

## Exercice 5

**Comment trouver la faille :**

Pour trouver la faille on a trouvé un user-agent.



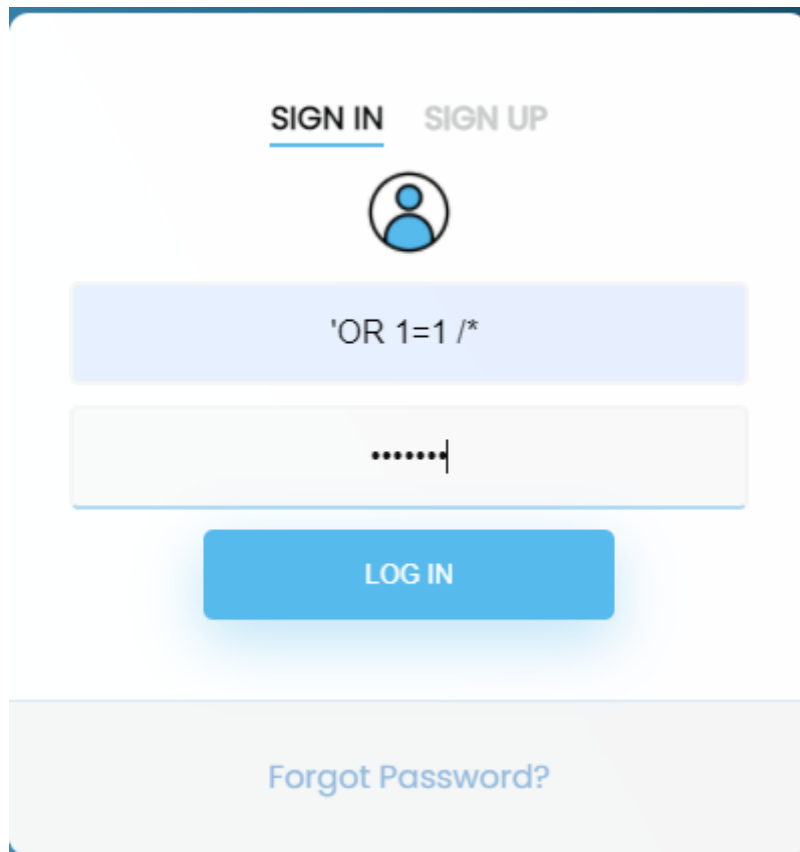
**Solution de correction :**

Ne pas renseigner l'utilisateur agent dans le débogueur.

## Exercice 6 :

Comment trouver la faille :

On effectue une injection SQL « 'OR 1=1 /\* » et on met ce que l'on veut dans le mot de passe



The screenshot shows a login interface with two tabs at the top: 'SIGN IN' (active) and 'SIGN UP'. Below the tabs is a user icon. The username field contains the SQL injection payload 'OR 1=1 /\*'. The password field is masked with dots. A blue 'LOG IN' button is positioned below the password field. At the bottom of the form is a link that says 'Forgot Password?'.

Solution de correction :

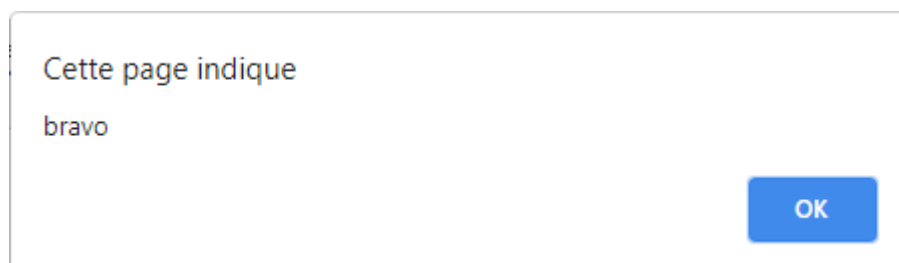
On utilise des requêtes préparées

## Exercice 7 :

Dans la page index on observe une obfuscation que l'on traduit par :

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

on entre donc le mdp toto123lol et on observe :



The screenshot shows a dialog box with the text 'Cette page indique' followed by 'bravo' on the next line. In the bottom right corner, there is a blue button labeled 'OK'.