République algérienne démocratique et populaire

Ministère De L'enseignement Supérieur Et De La Recherche Scientifique

Université « Yahia Farès » De Médéa



Rapport Du TP :

Réaliser une attaque SQL injection

Enseigner par : Mr.Rahim messouad

Réaliser par : Haddad Islem

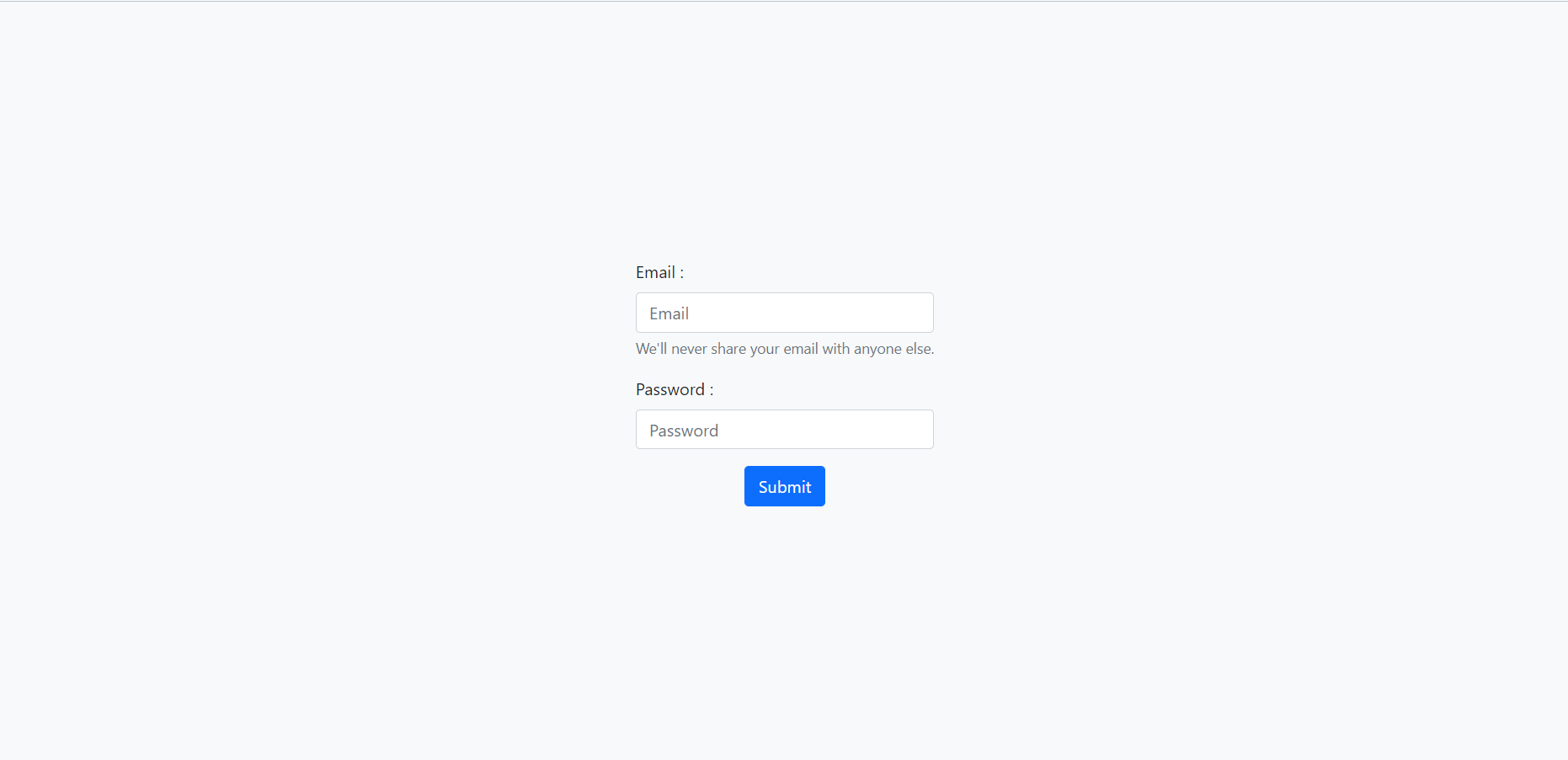
**Année universitaire : 2020/2021**

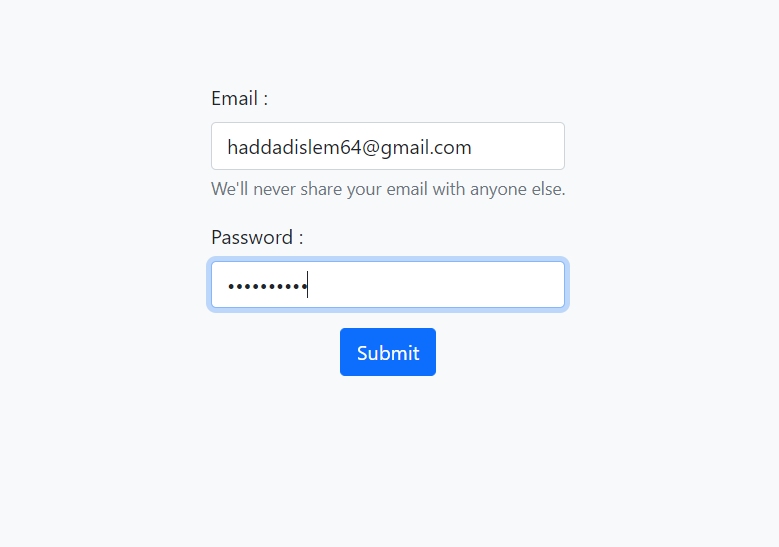
**Introduction :**

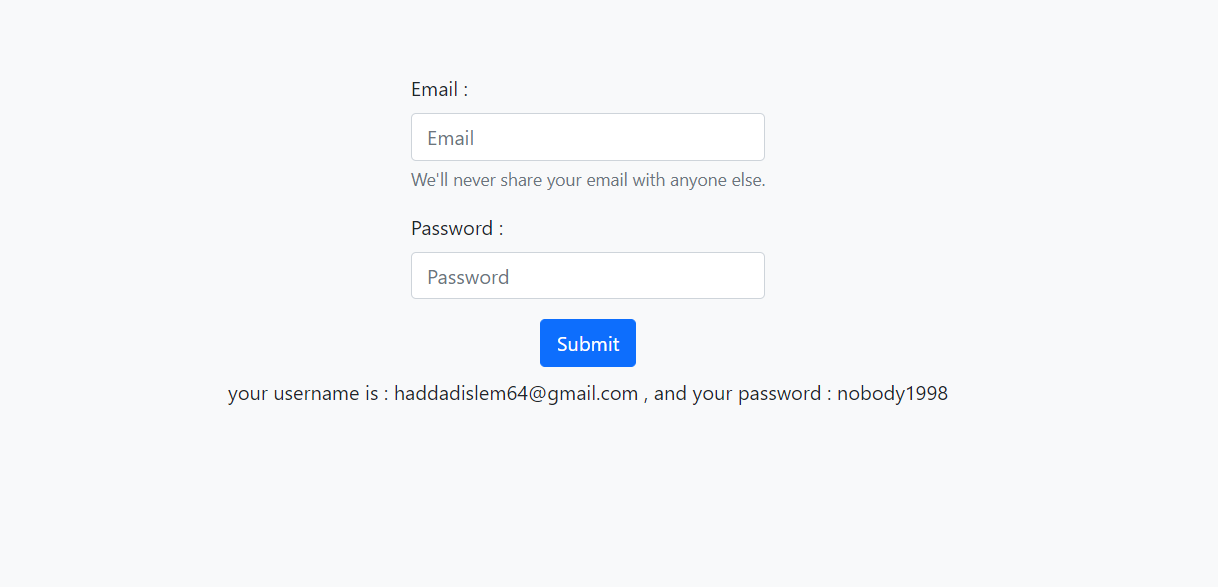
Parmi l’un des vulnérabilités des application web est les attaque SQL injection, ce type attaque est un groupe de méthodes d’exploitation de faille qui interagissant directement avec la base de données.

**L’attaque SQL injection Union :**

Il existe plusieurs méthodes d’attaque par l’injection SQL, l’un de ce dernier est l’attaque injection SQL par Union, c’est une attaque très dangereuse qui base sur l’utilisation du UNION pour observer le contenu de base de données, dans Ce TP en va voire comment en peut réaliser une attaque SQLi avec la méthode Union, Note quand as déjà pupulé notre base de données pour tester notre attaque

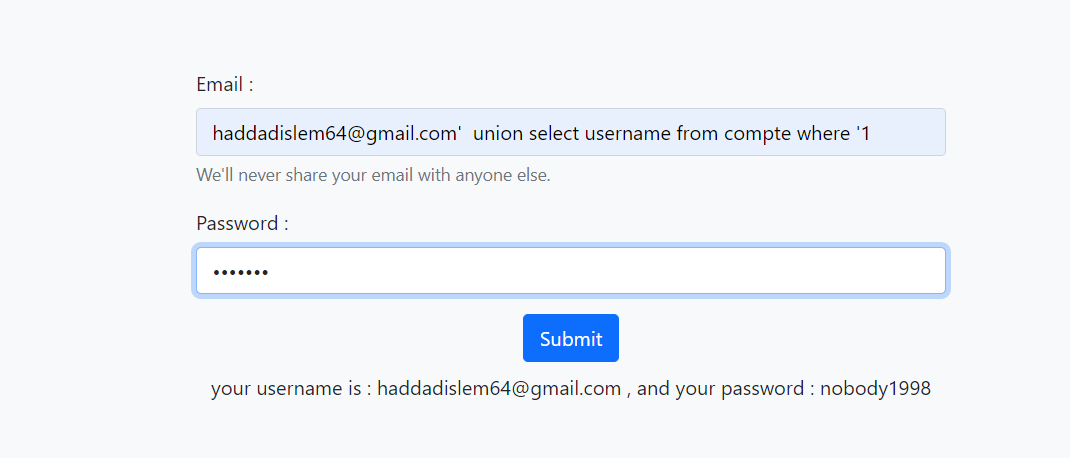
On a une page Web par example qui affiche les données d’un  
  
Pour utilisateur normal , qui va entrai sont email et son mot de passe il sera affiché dans cette page comme celle lui ci :



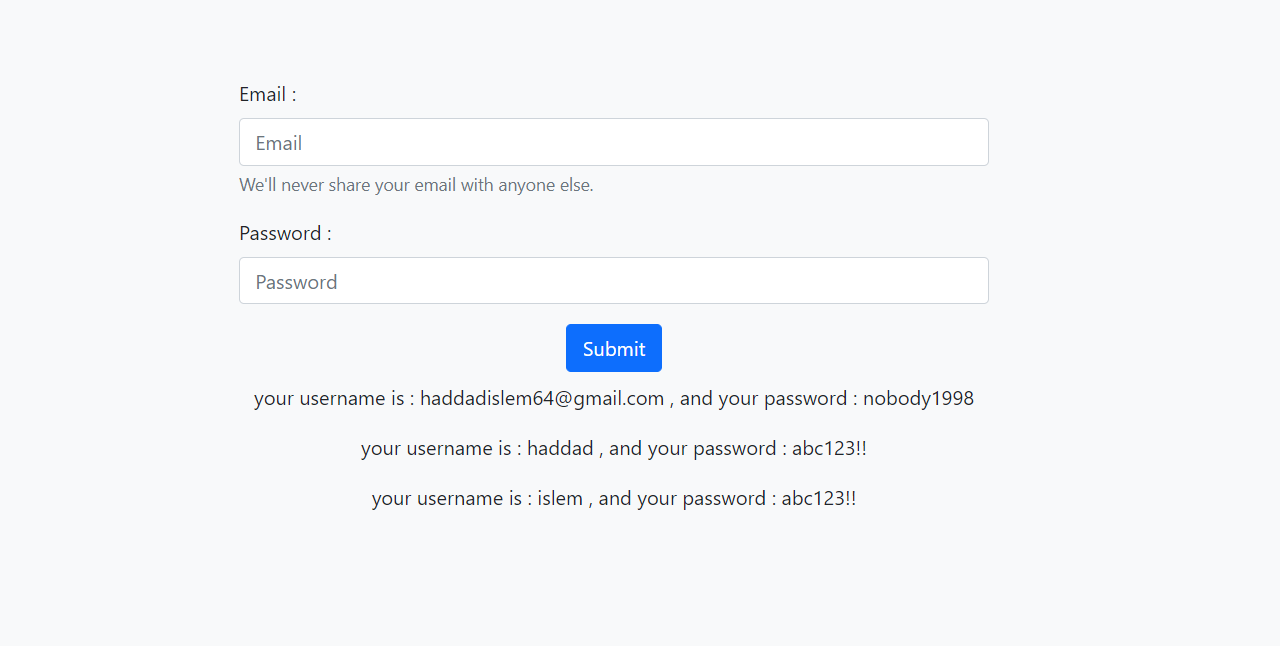
Et on obtenu cette résultats   
  
  
**Attaque SQL injection en méthode union :**

Maintenant supposons qu’un utilisateur a la place de validé ces données a partir ce cette forme il écrit dans l’input Email cette commande :

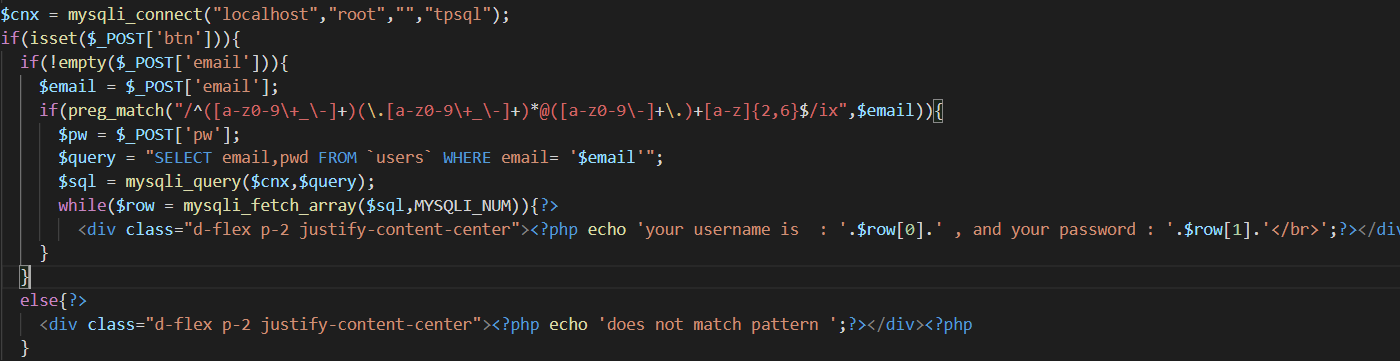
Nomemail' union select username,password from compte where '1  
un example reel :

haddadislem64@gmail.com' union select username,password from compte where '1  
  


lorsque on clique submit, cette requête submit au serveur notre forme qui concat dans notre query :   
  
**SELECT email,pwd FROM `users` WHERE email= 'haddadislem64@gmail.com' union select username,password from compte where '1' ;**

qui affiche cette page :  


donc on a fait une SQL injection et on a affiché des données d’autre utilisateur que on n’ont pas leur information ,  
  
Pour ce protégé de ce type d’attaque il faut quand fait n’empêche les attaque SQL injection , 1.on peut Controller les input de ne pas avoir certain méta caractère , expression régulière  
 en utilisant le fonction preg\_match() avec l’expression régulière pour Controller l’input email : /^([a-z0-9\+\_\-]+)(\.[a-z0-9\+\_\-]+)[\*@([a-z0-9\-]+\.)+[a-z]{2,6}$/ix](mailto:*@([a-z0-9\-%5d+\.)+%5ba-z%5d%7b2,6%7d$/ix)  
  
voici comment le code php doit etre :



Quand une mauvaise valeur fabriquer par example sql injection , ce message sera affiché

