# Site à attaquer

## BTS SIO / FRC

| DATE | PRESTATIONS REALISEES PAR : | PRESTATIONS REALISEES POUR : |
|---|---|---|
| 25/09/2023 | | FRC |

Cet énoncé des Travaux (EDT) est émis dans le but de créer un site Web contenant des vulnérabilités, qui sera ensuite intégré dans une présentation globale sur les risques cyber lors du FRC de novembre 2023.

## Période d'exécution

Les services commenceront le 25/09/2023, et se poursuivront jusqu'au 05/10/2023

## Ressources de participation

## Étendue des travaux

Les étudiants doivent fournir les services et les produits livrables comme suit :

*Le projet implique la création d'un site web pour une organisation dont le contexte sera précisé au début du projet. Ce site web devra délibérément contenir des vulnérabilités permettant des injections SQL.*

## Matériaux livrables

*Une machine virtuelle contenant le site internet*

## Critères de réalisation

Les étudiants doivent remplir les conditions de réalisation suivantes :

- Création du site Web en utilisant les langages HTML/CSS/PHP/SQL.
- Le site doit être accessible à partir d'un navigateur sur la machine hôte.
- Il est également nécessaire de fournir un tutoriel d'utilisation du site ainsi que des instructions pour effectuer des attaques sur le site.

Contenu du site  (vous pouvez vous inspirer du site https://www.fitnesspark.fr):

- Une page d'accueil
- Une page de présentation des activités
- Une page connexion membre

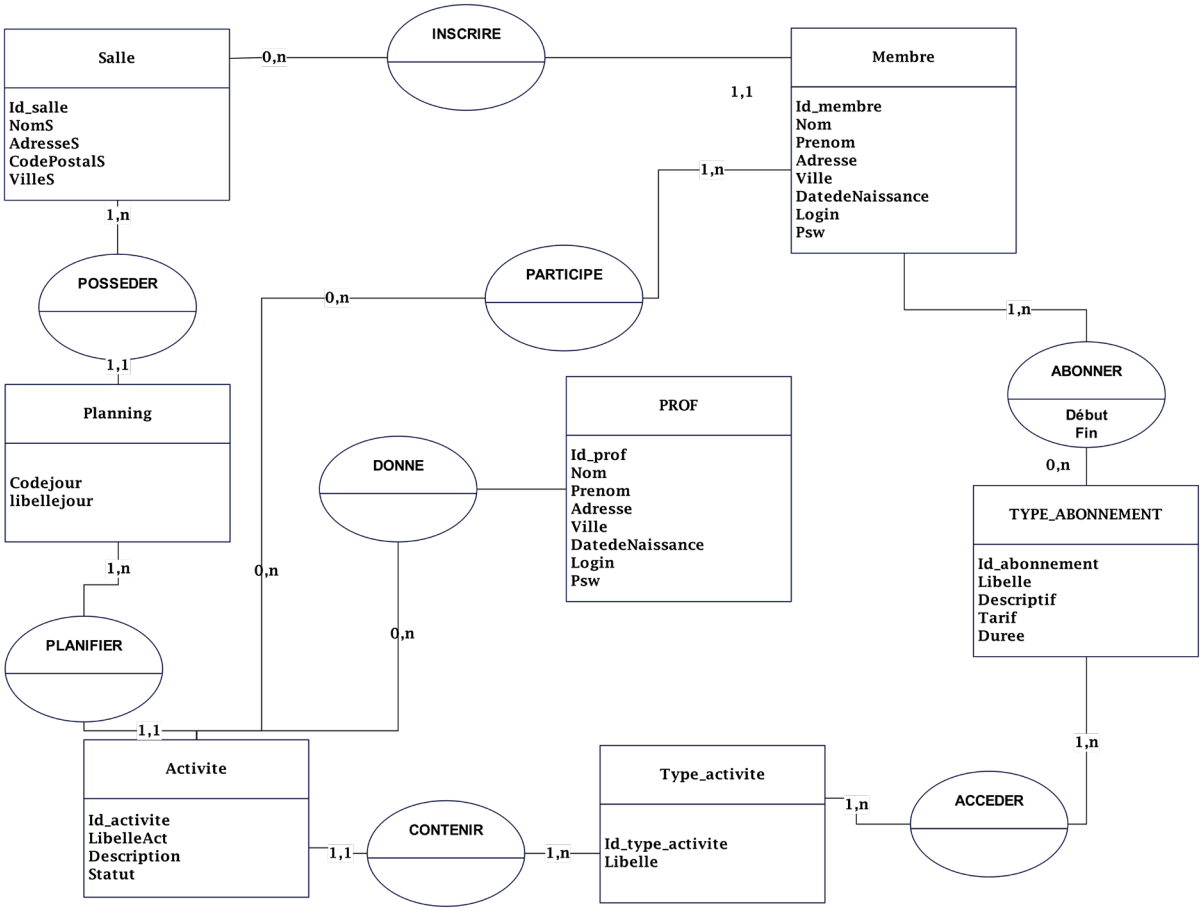
## Information complémentaire

Pour comprendre les injections SQL, vous devez lire le document suivant

https://www.cloudflare.com/fr-fr/learning/security/threats/sql-injection/

VOT
RE

Vous devez créer une base de données selon le schéma suivant (vous devrez l'alimenter et ne pas mettre en place de procédure de sécurité) :



Vous devez créer un fichier de connexion à la base de donnée appelé cnx.php qui se situera dans un répertoire config

Pour la connexion à la base de donnée vous utiliserez la méthode mysqli comme le montre l'exemple ci-dessous

```
<?php

    $host = "localhost";

    $user_mysql = "root";              // nom d'utilisateur de l'utilisateur de MySQL

    $password_mysql = "";     // mot de passe de l'utilisateur de MySQL

    $database = "matable";

    $db = mysqli_connect($host, $user_mysql, $password_mysql, $database);

    mysqli_set_charset($db, "utf8");

if(mysqli_errno($db))

{

echo "Can't Connect to mySQL:".mysqli_connect_error();

}

?>
```

VOT
RE

Les requêtes à mettre dans le site seront du type suivant

```
<?php
    $host = "localhost";
    $user_mysql = "root";              // nom d'utilisateur de l'utilisateur de MySQL
    $password_mysql = "";     // mot de passe de l'utilisateur de MySQL
    $database = "matable";
    $db = mysqli_connect($host, $user_mysql, $password_mysql, $database);
    mysqli_set_charset($db, "utf8");
if(mysqli_errno($db))
{
echo "Can't Connect to mySQL:".mysqli_connect_error();
}
?>
```

VOT
RE

```php
<?php

   // code source de articles.php

<?php

        include("cnx/cnx.php")  ;

        $query_dest = "SELECT id_destination,Destination FROM destination";

   $rs_dest = mysqli_query($db, $query_dest);

        if(mysqli_num_rows($rs_dest) > 0)

            {

                echo "<form name='form_update' method='get' action='recherche.php'>";

                echo "<select name= 'destination'>";

                echo '<option value="">'.'--- Choisir une destination ---'.'</option>';

               while($r = mysqli_fetch_assoc($rs_dest))

               {

                  echo "<option value='".
$r['id_destination'] ."'>" .$r['Destination'] .'</option>';

                      }

                echo '</select>';

            }

?>
```

VOT
RE