3iLINGENIEURS </les sciences informatiques>		Année : 2022/2023
NOM : **Prénom :** **Groupe :**	***Web – J. Grasset***	**15/03/2023**

Partie écrite

1. Injection SQL : expliquez **brièvement** le principe et indiquez comment les éviter.

Injection SQL : faire exécuter du code SQL via les données envoyées au serveur, par exemple via un formulaire

Pour éviter : nettoyerles chaines de caractères, rendre inopérants les caractères qui permettent l'injection

Avec PDO ou mysqli:

requêtes préparées, nettoyage automatique
Avec PDO ou mysqli, vous pouvez utiliser des requêtes préparées, qui nettoient automatiquement les entrées utilisateur, rendant ainsi l'injection SQL beaucoup plus difficile. Les requêtes préparées remplacent les valeurs des paramètres avec des espaces réservés, ce qui empêche le code SQL malveillant d'être interprété comme une commande SQL valide. Cela offre une protection efficace contre les attaques par injection SQL.

2. Quelle URL permet d'accéder à un fichier appelé zou.php, situé à la racine web du serveur guili-guili.eu, en lui transmettant en get :
   - Hello, dans le paramètre appelé message
   - 66, dans le paramètre appelé nombre

http://guiliguili-guili.eu/zou.php?message=Hello&nombre=66

3. Que fait l'instruction var_dump ?

`var_dump` affiche des informations sur une variable, y compris son type et sa valeur.
C'est un outil de débogage en PHP.

4. Lorsqu'on crée un formulaire en HTML on peut indiquer le type de certaines données, voire ajouter des contraintes. Par exemple <input type="number" min= »15 » max= »30 »>
   a. Quel est l'effet de ces précisions pour l'utilisateur ?
   b. Quel est l'effet de ces précisions sur la sécurité des données reçues côté serveur ?

a. Ces précisions dans un formulaire HTML facilitent à l'utilisateur la saisie de données en fournissant des indications sur le type attendu et les plages de valeurs autorisées.

b. Du côté serveur, ces précisions peuvent renforcer la sécurité en simplifiant la validation des données et en réduisant les risques liés à la manipulation de données inappropriées ou malveillantes.

5. Indiquez ce qu'affiche chacune des lignes suivantes (valeur affichée ou erreur). Inutile de justifier votre réponse.

```
echo 156+"10" ;
echo 156.10 ;
echo "156"."10" ;
echo "10"+"156" ;
echo ("10"."01")+"20" ;
```

166

156.1

15610

166

1021