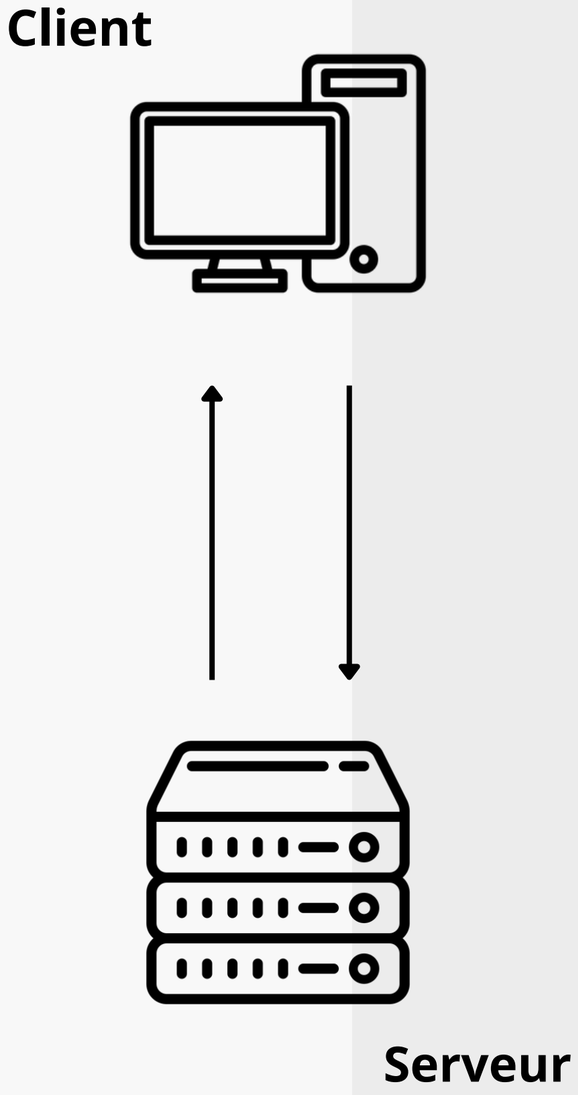
/01

Injections SQL

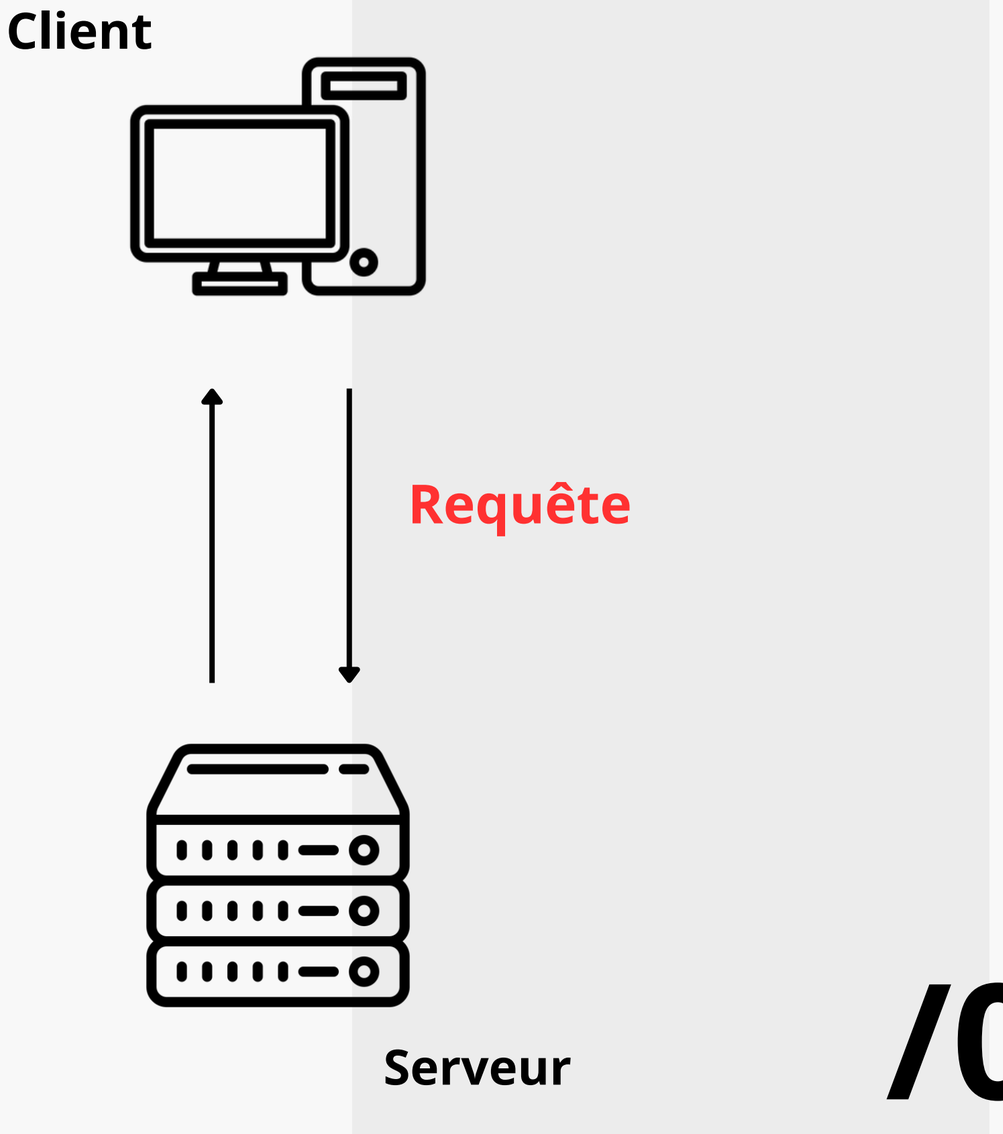
Rappels

Comment fonctionne un site web ?



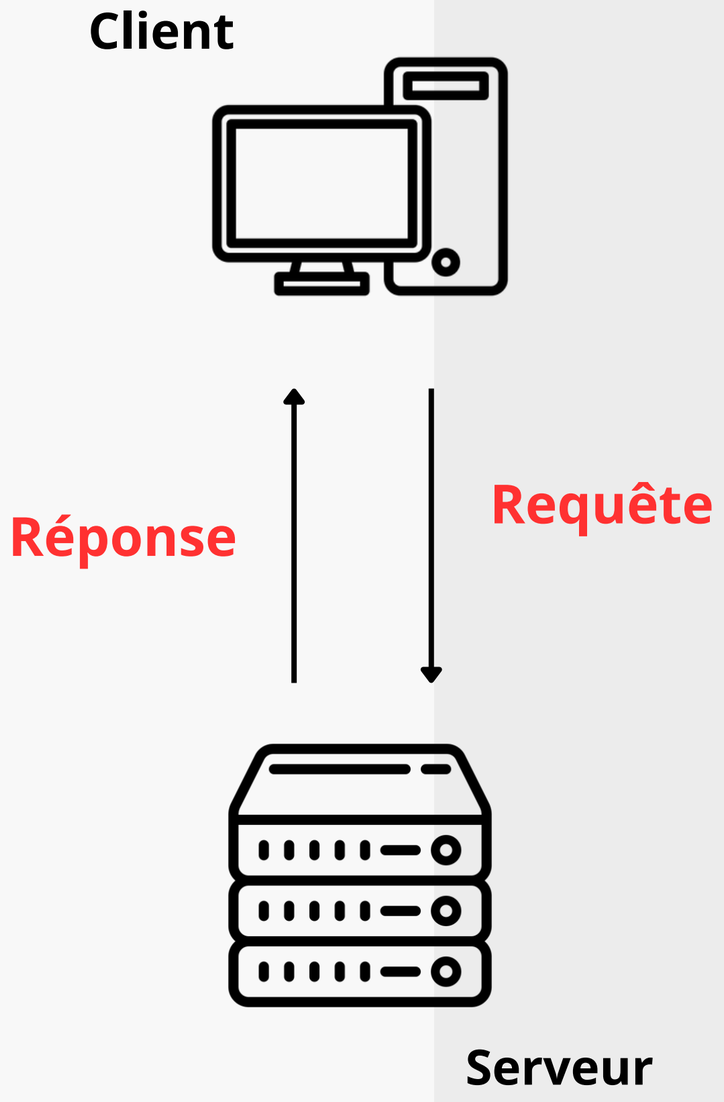
Rappels

Comment fonctionne un site web ?



Rappels

Comment fonctionne un site web ?

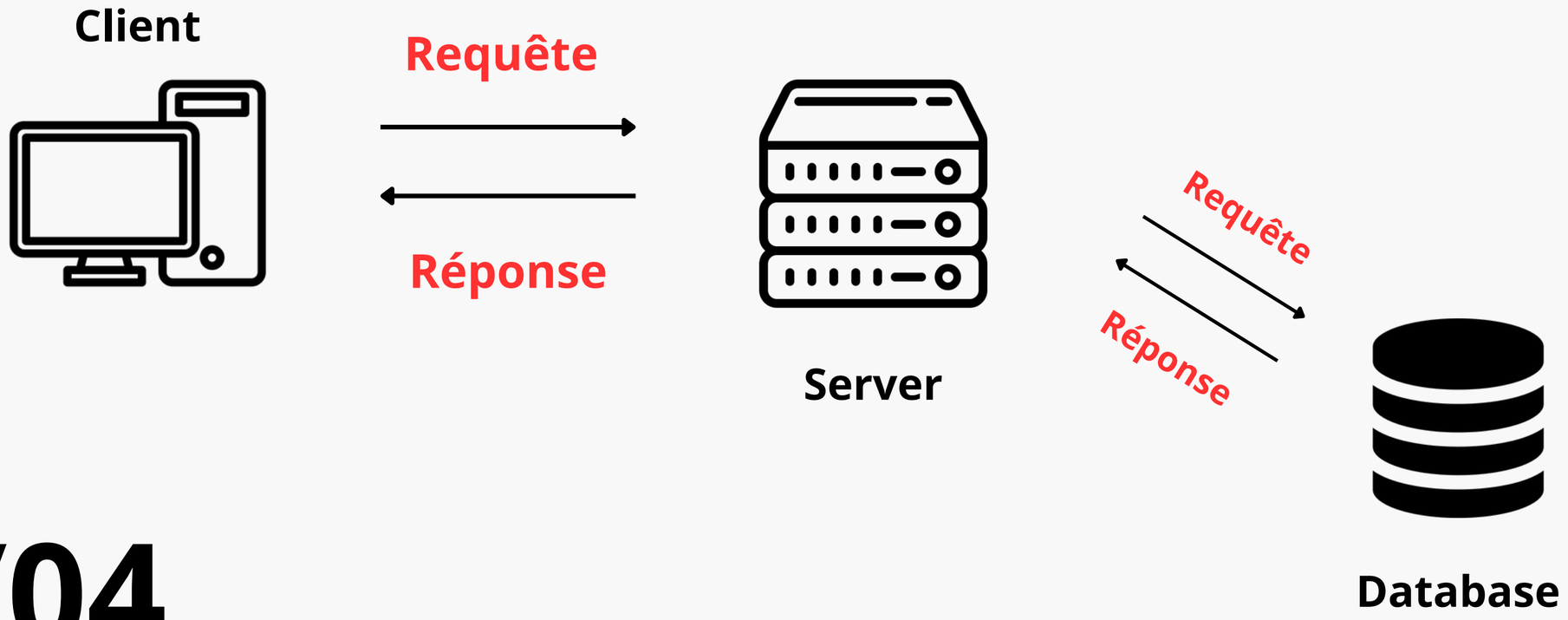


/03

Rappels

- **HTML, CSS, JS**
- **Languages Serveur**
- **Concept de base de données**

Concept de base de données



/04

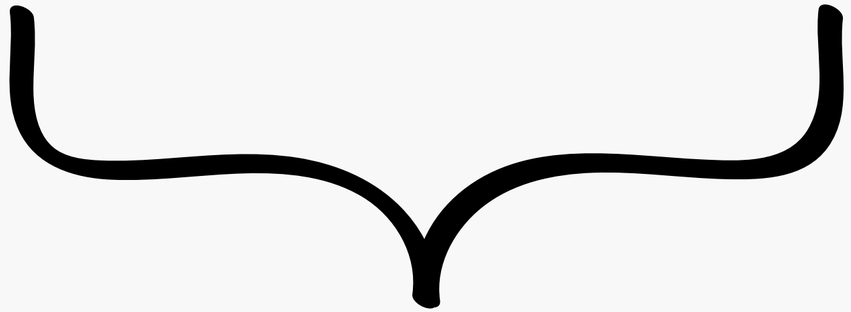
Concept de base de données

e_id	e_name	e_salary	e_age	e_gender	e_dept
1	Sam	95000	45	Male	Operations
2	Bob	80000	21	Male	Support
3	Anne	125000	25	Female	Analytics
4	Julia	73000	30	Female	Analytics
5	Matt	159000	33	Male	Sales
6	Jeff	112000	27	Male	Operations

/05

Syntaxe SQL

SELECT columns FROM table WHERE condition



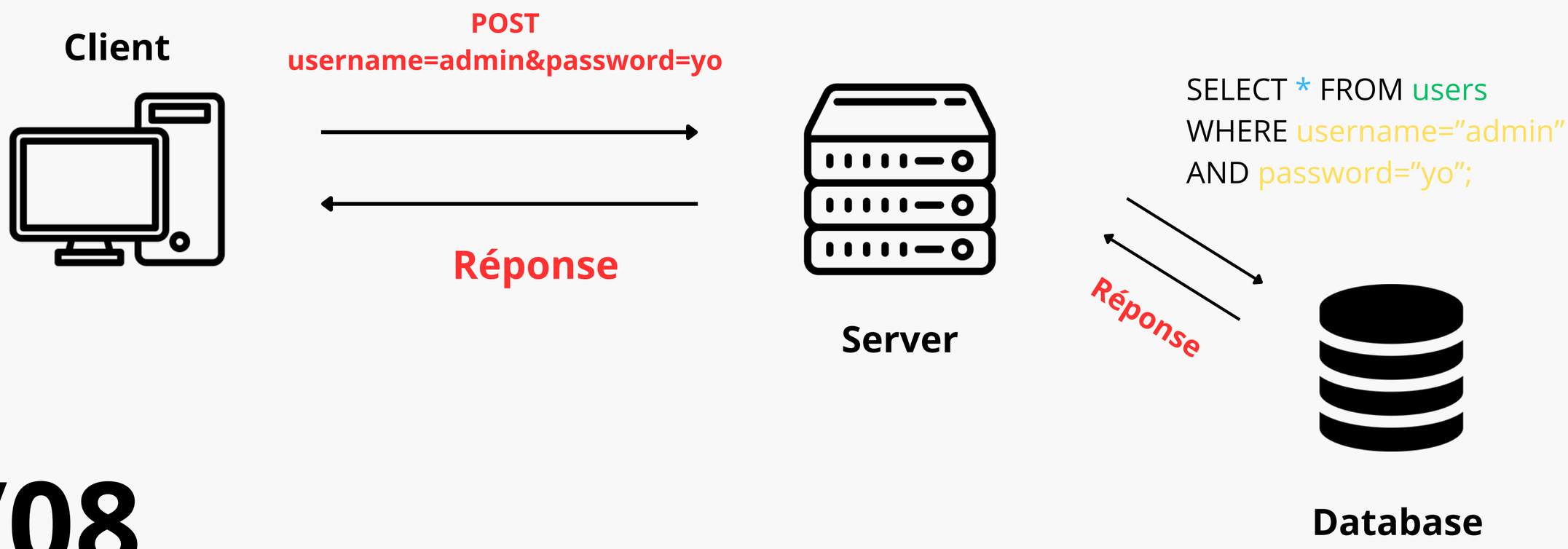
OPTIONNEL

Syntaxe SQL

Exemples

- SELECT age, prenom FROM eleves WHERE classe=“première“;
- SELECT * FROM eleves WHERE nom LIKE “M%“ OR nom LIKE “%E”;
- SELECT * FROM users WHERE username=”admin” AND password=”yo”;

Schéma récapitulatif



/08

Let’s hack… ethically

Ce diaporama est à titre éducatif et préventif UNIQUEMENT, en aucun cas il n’incite à transgresser les lois.

Article 323-1 du Code pénal
Le fait d’accéder ou de se maintenir, frauduleusement, dans tout ou partie d’un système de traitement automatisé de données est puni de deux ans d’emprisonnement et de 30000 euros d’amende.

SQL Injection

SELECT * FROM users WHERE username=‘{user}‘ AND password=‘{pass}‘;

Que se passe-t-il si user=”test‘; #“ ?

/10

SQL Injection

```
SELECT * FROM users WHERE username='test'; #' AND password='{pass}';
SELECT * FROM users WHERE username='test'; #' AND password='{pass}';
SELECT * FROM users WHERE username='test';
```

Que se passe-t-il si user="test'; #" ?

SQL Injection

SELECT * FROM users WHERE username=‘{user}‘ AND password=‘{pass}‘;

Que se passe-t-il si pass=”test‘ OR ‘1‘=‘1“ ?

/12

SQL Injection

```
SELECT * FROM users WHERE username='x' AND password='test' OR '1'='1';
SELECT * FROM users WHERE username='x' AND password='test' OR '1'='1';
```

Que se passe-t-il si pass="test' OR '1'='1" ?

/13

UNION based

Permet de récupérer plus d’infos que prévu par le développeur => faire fuiter la base de données.

Time based

Lorsue l’on a pas de retour visuel du site, utilisation de fonctions précises pour faire fuiter tout de même.

Error based

Faire fuiter des infos à partir d’une erreur affichée.

Out-of-band

Afficher des fichiers ou prendre le contrôle du serveur en passant par SQL.. oui oui.

Login bypass is c00l but...

Merci de votre attention !

Demo time