SQL INJECTION

SENAI

Sumário

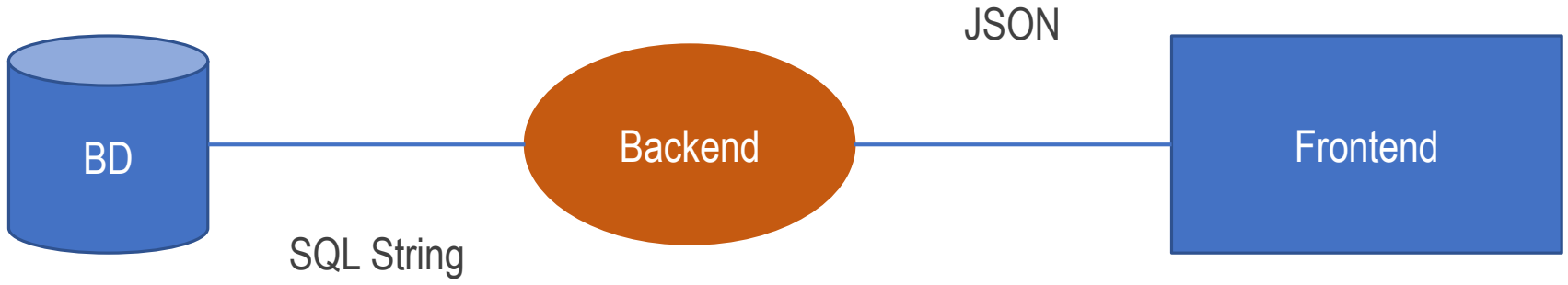
- O que é SQL Injection?
- Fluxo dos dados
- Como funciona o ataque?
- Medidas contra o SQL Injection
- Criação de Blacklist na validação do Formulário

O que é SQL Injection?

SQL Injection é um tipo de ataque onde o invasor pode inserir ou manipular consultas criadas pela aplicação, que são enviadas diretamente para o banco de dados relacional.

Fluxo dos dados

BD – Banco de Dados



Como funciona essa comunicação?

```
let requestBody = {
    email: "thiago@email.com",
    senha: "discodefreio2021"
}

let stringSql = "SELECT * FROM Users WHERE UserEmail = " + requestBody.email + " AND UserPassword = " + requestBody.senha;

// SELECT * FROM Users WHERE UserEmail = thiago@email.com AND UserPassword = discodefreio2021
```

Como funciona o ataque?

- Esse ataque funciona pela inserção de código SQL, para obter dados ou manipular o banco de uma forma não permitida.

Como funciona o ataque?

```
let requestBody = {
    email: "thiago@email.com;--",
    senha: "discodefreio2021"
}

let stringSql = "SELECT * FROM Users WHERE UserEmail = " + requestBody.email + " AND UserPassword = " + requestBody.senha;

// SELECT * FROM Users WHERE UserEmail = thiago@email.com;-- AND UserPassword = discodefreio2021
```

Como funciona o ataque?

```
let requestBody = {
    email: "' OR 1=1;--",
    senha: "discodefreio2021"
}

let stringSql = "SELECT * FROM Users WHERE UserEmail = " + requestBody.email + " AND UserPassword = " + requestBody.senha;

// SELECT * FROM Users WHERE UserEmail = '' OR 1=1;-- AND UserPassword = discodefreio2021
```

Maneiras de proteger o sistema

- Parametrização das Consultas – Backend
- Usar Stored Procedures – BD e Backend
- Limitar Privilégios - BD

Maneiras de proteger o sistema

- Criação de Blacklist no Front
  - O que é uma blacklist?
    - Blacklist é uma lista de proibição, no nosso caso criaremos uma lista de palavras que não serão aceitas no formulário

Maneiras de proteger o sistema

Criação de Blacklist no Front

Bons estudos e até breve!