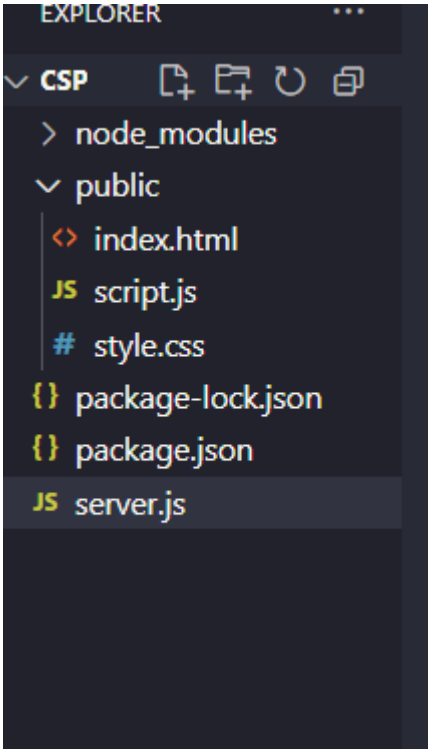
npm init -y

npm install express helmet



SERVER.JS `//scriptSrc: ["'self'", "'unsafe-inline'"],`

server.js

```js
const express = require("express");
const helmet = require("helmet");

const app = express();
const PORT = 3000;

// Middleware para definir Content-Security-Policy
app.use(
    helmet({
        contentSecurityPolicy: {
            directives: {
                defaultSrc: ["'self'"], // Apenas recursos do próprio domínio
                scriptSrc: ["'self'"], // Bloqueia scripts inline e externos não autorizados
                styleSrc: ["'self'", "https://fonts.googleapis.com"], // Permite estilos internos e Google Fo
                fontSrc: ["'self'", "https://fonts.gstatic.com"], // Permite fontes do Google
            },
        },
    })
);

// Servir arquivos estáticos da pasta public/
app.use(express.static("public"));

app.listen(PORT, () => {
    console.log(`Servidor rodando em http://localhost:${PORT}`);
});

```

INDEX.HTML

index.html

```html
<!DOCTYPE html>
<html lang="pt-BR">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Página Segura com CSP</title>
    <link rel="stylesheet" href="style.css">
</head>
<body>
    <h1>Exemplo de Content Security Policy (CSP)</h1>

    <p>Tente rodar um script malicioso no console ou injetar via DevTools!</p>

    <button id="btnExecutar">Clique para Executar Script</button>

    <script src="script.js"></script>
</body>
</html>

```

SCRIPT.JS

script.js

```js
document.getElementById("btnExecutar").addEventListener("click", function () {
    alert("Script externo permitido pela CSP!");
});

```

CSS

```css
body {
    font-family: Arial, sans-serif;
    background-color: #e3f2fd;
    color: #0d47a1;
    text-align: center;
    margin: 0;
    padding: 20px;
}


h1 {
    color: #1565c0;
    font-size: 2em;
}


p {
    font-size: 1.2em;
    margin-bottom: 20px;
}


button {
    background-color: #2196f3;
    color: white;
    border: none;
    padding: 10px 20px;
    font-size: 1.1em;
    cursor: pointer;
    border-radius: 8px;
    transition: background-color 0.3s ease-in-out;
}

button:hover {
    background-color: #1976d2;
}


.container {
    max-width: 600px;
    background: white;
```

```
    padding: 20px;
    border-radius: 10px;
    box-shadow: 0 4px 8px rgba(0, 0, 0, 0.2);
    margin: auto;
}
```

document.write("<script>alert('XSS')</script>");

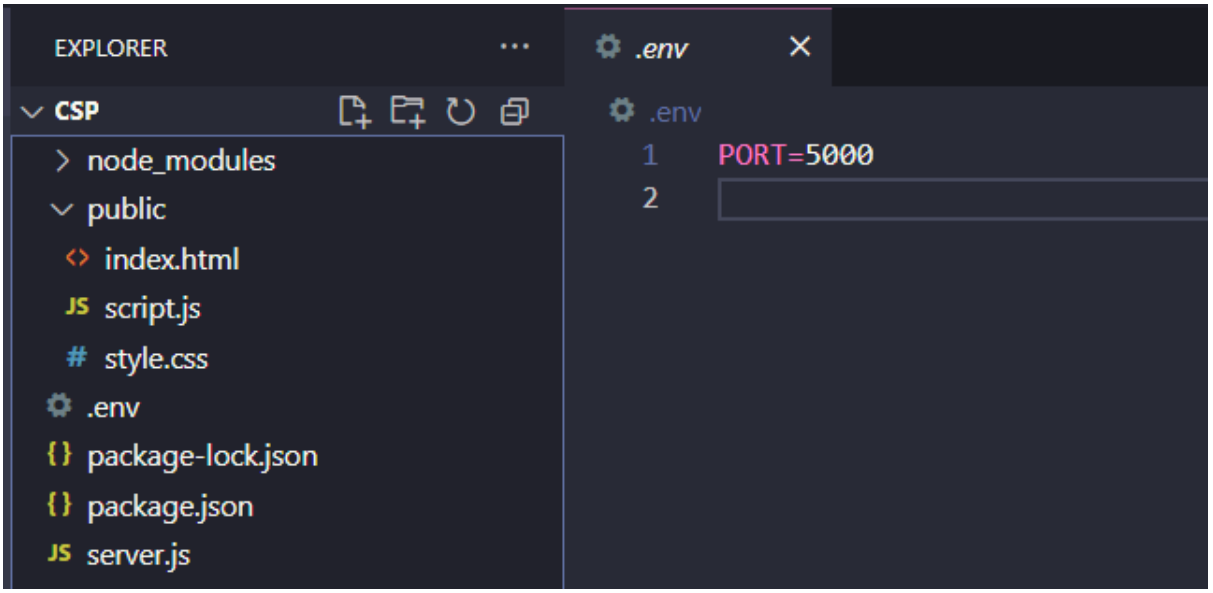
Gerenciamento de variáveis de ambiente

INCLUINDO O PACOTE dotenv

npm i dotenv

server.js

.env



.gitignore