**HADIA MAZHAR**

**DHC-486**

**WEEK – 4**

1. **SECURE WITH API:**

//express rate

const rateLimit = require('express-rate-limit');

// Limit login attempts to 5 per 15 minutes per IP

const loginLimiter = rateLimit({

    windowMs: 15 \* 60 \* 1000, // 15 minutes

    max: 5,

    message: 'Too many login attempts from this IP, please try again later.',

    standardHeaders: true,

    legacyHeaders: false,

});

app.post('/login', loginLimiter, async (req, res) => {

    // your login logic here

});

1. **SECURE WITH CORS:**

//cors

const cors = require('cors');

const allowedOrigins = ['https://yourdomain.com', 'https://another-safe-site.com'];

app.use(cors({

    origin: function (origin, callback) {

        if (!origin || allowedOrigins.includes(origin)) {

            callback(null, true);

        } else {

            callback(new Error('Not allowed by CORS'));

        }

    },

    credentials: true,

}));

1. **API KEY:**

x-api-key: a3f1c9e8b7d6a2f4e9c3d1a7b8e6f2c9d4e1a3b7c9f2d6e8a1c3b5d7f9e2a4c6;

//api key

const API\_KEY = 'a3f1c9e8b7d6a2f4e9c3d1a7b8e6f2c9d4e1a3b7c9f2d6e8a1c3b5d7f9e2a4c6';

function apiKeyMiddleware(req, res, next) {

    const key = req.headers['x-api-key'];

    if (key === API\_KEY) {

        next();

    } else {

        res.status(403).json({ error: 'Forbidden: Invalid API Key' });

    }

}

// Apply to sensitive routes

app.use('/admin', apiKeyMiddleware);

1. **Security headers and CSP implementation:**

//cross-site scripting

app.use(

  helmet.contentSecurityPolicy({

    directives: {

      defaultSrc: ["'self'"],

      scriptSrc: ["'self'", "https://trusted.cdn.com"], // Add trusted script sources

      styleSrc: ["'self'", "https://fonts.googleapis.com"],

      fontSrc: ["'self'", "https://fonts.gstatic.com"],

      imgSrc: ["'self'", "data:"],

      connectSrc: ["'self'"],

      objectSrc: ["'none'"],

      upgradeInsecureRequests: [],

    },

  })

);

//only use https

app.use(

  helmet.hsts({

    maxAge: 31536000, // 1 year in seconds

    includeSubDomains: true,

    preload: true,

  })

);