Cyber Security Presentation

Human Resouce Mangement System

Aamina Mariam 22100062

Ali Adnan Arif 22100303

Mohammad Yousuf 22100289

Talha Nasir 22100260

Javeria Tariq 22100230

Project Overview

Our project streamlines the complex process of managing and recruiting employees in an organization. We provide a "one stop solution" for Small and medium-sized enterprises (SMEs) that caters to the HR needs of an organization.

A01: Broken Access Control

- Violation of the principle of least privilege or deny by default
- Accessing API with missing access controls for POST, PUT and DELETE.
- Elevation of privilege. Acting as a user without being logged in or acting as an admin when logged in as a user.

- An attacker might be able to change or delete content
- Perform unauthorized functions
- Attacker can take over site administration.

A02: Cryprographic Failures

All employee passwords are encrypted and then stored. If the cryptographic algorithms are weak or old it can lead to attackers gaining access to our system

As with broken access control the attacker can change or delete information or perform unauthorized actions

A07: Idenification and Autentication Failures

As mentioned before if the attacker has a list of valid usernames and passwords they can access our system without raising any red flags and have access to all of the company information.

Controls

1 Broken Access Control

- Minimize Cross-Origin Resource Sharing (CORS) usage.
- Rate limit API and controller access to minimize the harm from automated attack tooling

2 Cryptographic failures

- Store passwords using strong adaptive and salted hashing functions with a work factor (delay factor), such as scrypt or bcrypt
- Always use authenticated encryption instead of just encryption.

3 Identification and Authentication failures

- Implement multi-factor authentication
- Enforce a password policy to prevent users from setting weak passwords
- Use session tokens

All of these are protective controls

Tools Selection: Static and Dynamic Security Scanning

coverity®

Se

APIsec

Do you have any questions?