COMP.SEC.300
Exercise work presentation

Martin Yordanov
martin.yordanov@tuni.fi

Overview

- A Minimalistic CRUD web application
- Core functionality of a social media platform
- JavaScript, MERN stack
- Attention to usability
- Docker

martin.yordanov@tuni.fi

Vulnerability assessment

- Static analysis - Trivy, Snyk
- GitHub Dependabot - Secrets and dependencies repository scan
- Tenable Nessus - Automated vulnerability scanning
- Metasploit & ExploitDB vulnerability records

martin.yordanov@tuni.fi

Vulnerability assessment results

- Nessus did not find any vulnerabilities but it warned for a permissive header -> clickjacking.
- No exploits for the used mongodb version were found in ExploitDB and Metasploit's records
- Trivy found 23 vulnerabilities in the used docker image dependencies with known fixes.
- 22 HIGH, 1 MEDIUM severity.

martin.yordanov@tuni.fi

Penetration test

- White box, local network test
- Tools - Nmap, Metasploit, Wireshark, Postman, Kali Linux, Hashcat
- Successful exploits - NoSQLi, MITM, Unauthorized database access
- Failed exploit attempts - brute force, XSS, Broken Auth

martin.yordanov@tuni.fi

Remediation

- Sanitization implemented against NoSQLi
- Session cookies were configured to be sameSite, preventing CSRF attacks
- Database authentication was implemented
- “npm audit fix” was ran to update vulnerable dependencies’ version

martin.yordanov@tuni.fi

Questions?

martin.yordanov@tuni.fi