DHIS2 PENTEST PROJECT

Pål Brandsvoll & John Riland
Who are we?

● Group consists of master students Pål Brandsvoll and John Riland

● Master Topics:
  ○ **Pål** - Analyze DHIS2 up against Open Web Application Security Project (OWASP) Top 10 Security Risks
  ○ **John** - How can a penetration testing process be integrated into the DHIS2 development cycle?

● Working together on overlapping parts such as investigation and penetration testing of DHIS2
Penetration Testing 101

- Imitate a hacker to discover and report vulnerabilities and security issues
- Realistic approach
- Methodical
- The goal is to increase the overall state of security
- Every web application should be tested before release
Scope and focus areas

- Own DHIS2 instance running on a Linode server
- All attacks are conducted through the web application (i.e. OS and surrounding framework vulnerabilities are irrelevant)
- Focusing on OWASP Top 10 Security Risks
What we have done

- Used OWASP Zed Attack Proxy (ZAP) for automated testing
- Manual testing with assistance from tools like BurpSuite, SQLmap etc.
- Static code analysis with SonarQube
  - Manual inspection of key areas in the source code to some extent
Automated Testing

- Application mapping
- Automated scanner
- Handling alerts
  - False positives
  - Time consuming
- Difficult to configure

Example run of OWASP ZAP
Manual Testing

- According to security experts, about 40% of vulnerabilities are not detected by automatic scanners
- Logical errors are not detected by automated scanners
- Knowledge-based and time-consuming
Results

- We have found some weaknesses in DHIS2 (Don’t worry, weaknesses exist in all systems)
- They vary in severity and complexity
- Weakness is tested on the three most recent versions
- Results and steps to reproduce are logged
What we plan to do

- Continue to pentest DHIS2
- Rate and classify the results
- Recommend solutions for eliminating or mitigating the risk of attacks
- Find the best possible approach to integrate a pentesting process into the existing DHIS2 development cycle
How can our work benefit DHIS2?

- We want to contribute to a robust and secure application
- A development cycle more focused on secure development
- Suggested areas of research:
  - What risk do third-party apps add?
  - Security in different configuration and hosting options for DHIS2 (cloud-based, local server, Postgres, MySQL)
Feedback, comments or questions?
Email us at: paalmbr@ifi.uio.no, jkriland@ifi.uio.no