DevSecOps: Automated Security TESTING

Opportunities & Barriers

Naveen Kumar

Robin Poston

Agenda

- Introduction
- Background
- Covid-19 and Key Apps
- Security Issues
- Methods of Security Testing
- DevSecOps: Automated Security Testing
- Summary and Conclusion

Covid-19 and Digital World

- People turning to the digital world
  - Teleworking
  - Telemedicine appointments
  - Information gathering and dissemination about pandemic

- Increase in Internet usage and web browsing by 70% and social media usage by 61% (Kantar, 2020).

Key Covid-19 Apps

Take

- Brazilian leader in chatbots
- Developed a bot to connect potential patients to medical teams to avoid overloading Brazilian hospitals

DarwinAI

- Proposed an AI solution that can detect covid-19 from chest x-ray images

Key Covid-19 Apps

NYU Covid-19 Mobile App

- Currently being used in New York City to aid clinicians with covid-19 diagnosis.
- Created a model to assign a severity score based off the biomarkers.
- A higher score means higher chance of mortality from Covid-19.

BenevolentAI

- Created an algorithm that proposes new compounds to fight Covid-19.
- Currently working with the US government to run trials and see the effects of some of the proposed solutions.

Key Covid-19 Apps

Amazon 'Distance Assistant'

- To help site leaders identify high traffic areas and implement additional measures to improve social distancing
  - Solution applies artificial intelligence and machine learning to the camera footage in buildings.

- Promote social distancing behavior in real-time
  - Using AI and augmented reality to create a magic-mirror-like tool that helps associates see their physical distancing from other

Security Issues

- Majority of the users are accessing the technology and apps from home (Anderson & Vogels, 2020).
- Home network systems are often not fully secured.
- Risk associated with security-related incidents using apps on the devices have gone up significantly.

App Development Life Cycle

- Requirements Collection
- Application/System Design
- Development
- Testing and Deployment
- Support/Maintenance

Shift Left Testing

- Shift the security testing to the earlier phases of the app development process

Test Driven Security and App Development

- Define security requirements
- Develop and run the test case
- Implement the security controls
- Rerun the security test case

Methods of Security Testing

- Static Application Security Testing
- Dynamic Application Security Testing

Automated Security Testing

- Execution of security test cases (to detect vulnerabilities) without any manual intervention

Vulnerability Scanners

- Check or scan all the assets
- Develop a list of vulnerabilities or weaknesses
- Compare these vulnerabilities to the known vulnerabilities or weaknesses

Key Advantages

- Automated Security Testing System
  - Scalable
  - Repeatable
  - Enforce security test driven culture

- Quick time to market

Use Cases

- Incremental testing
- Comply with standards
- Security benchmarking

Drawbacks

- ROI
- Dynamic/Fast changing requirements
- Multiple languages and technologies

Key Challenges

- Security testing test cases run time
- Customized test cases
- False positives

Automated Security Testing

- Part of the organization culture
- Embed in the app development life cycle
  - Pre-commit and commit phase
  - Build phase
  - Deployment phase
- Quick time to market

Summary and Conclusion