Securing a Shared Code Repository

A Presentation By Omar Johnson

Module 11.2 Assignment

Vulnerabilities

- Confidentiality
  - Unsecure code could give out confidential data such as secrets, keys, and private credentials
- Theft
  - Shared repositories have various contributors; if a contributor has their credentials stolen then the repository is at-risk
- Source code security
  - Defects in source code or security issues in dependencies could lead to security threats in the program
- Source code theft
  - An unsecure repository and unprotected code could lead to stolen “intellectual property”

(Gil, 2018)

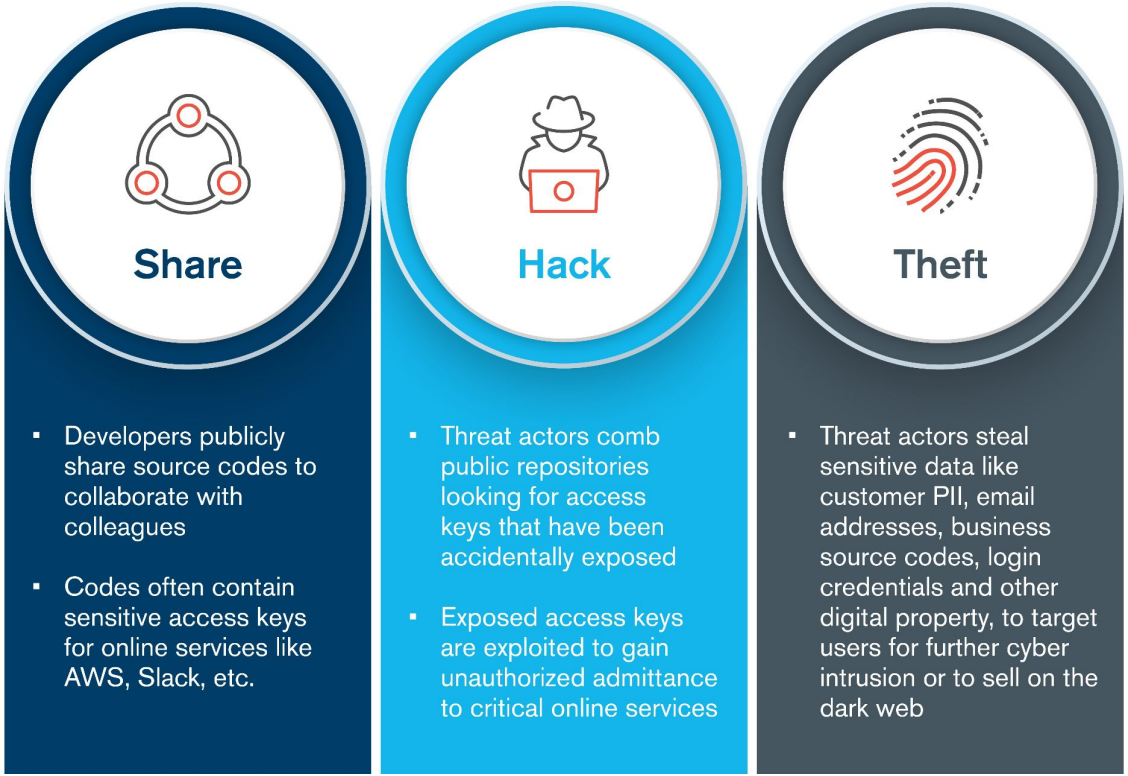
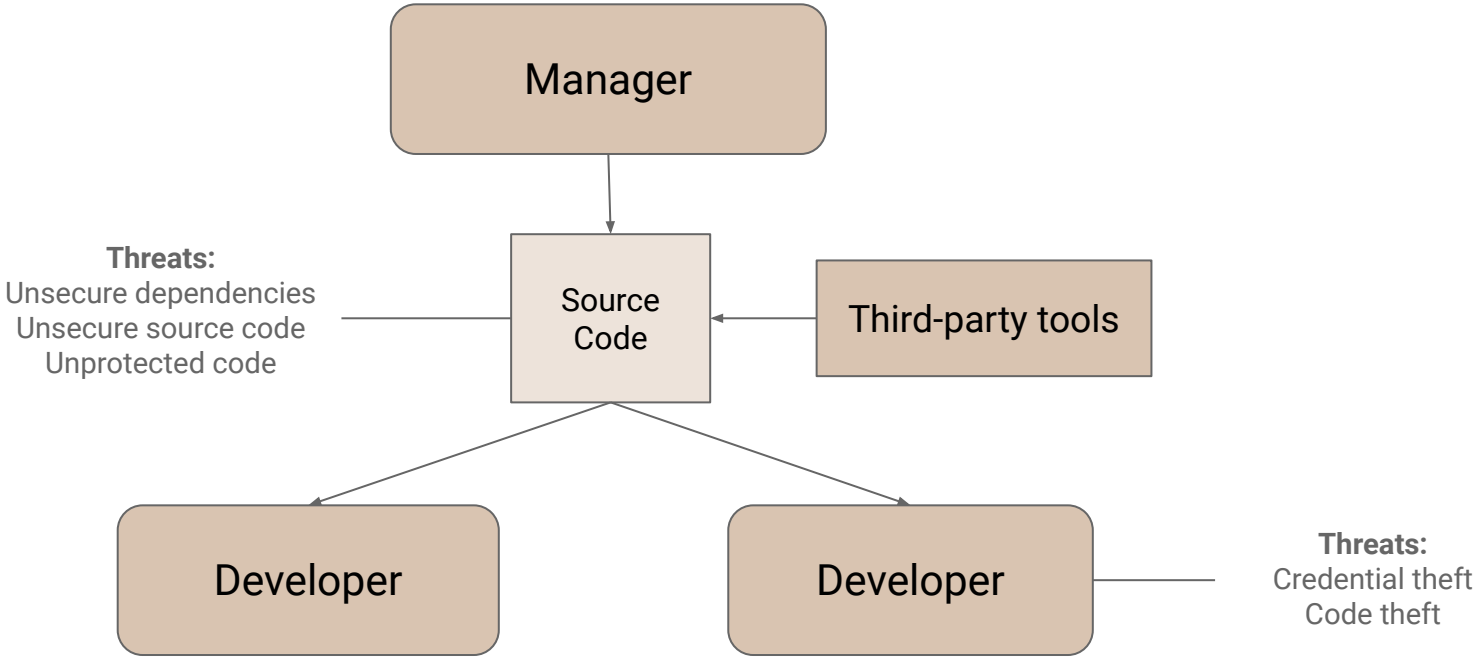


Figure 1. Repository threats

Threat Tree


Manager
Threats:
Unsecure dependencies
Unsecure source code
Unprotected code
Source Code
Third-party tools
Developer
Developer
Threats:
Credential theft
Code theft

Importance of Security

- An unsecure repository can lead to:
  - Data breaches
  - Stolen ideas and programs
  - Stolen credentials and keys
  - Compromised user safety
- It is a threat to the organization, its developers, and its users
- May harm the company’s public reputation and future

How to Improve Security

- Repository Tools
  - SAST applications
  - Dependency scanners
  - Secret detection
  - Examples:
    - OWASP Zap Baseline Scan
    - GitGuardian
- Repository Management
  - Enforcing/automating code checks
  - Tracking security tasks
  - Monitoring repository status
- Authorization and access
  - Principle of “Least privilege”
  - Mandate two-factor authentication
  - Protect the main branch

(Moisset, 2022)

Security Pipeline

- 2FA
- Access control

Developer

- Code analysis
- Checks

Pull Request

- Review
- Approval

Repository Manager

- Main branch remains protected

Merge

References

Gil. (2018, July 2022). “What You Need to Know About Code Repository Threats”. Cyberint. https://cyberint.com/blog/threat-intelligence/what-you-need-to-know-about-code-repository-threats/

Moisset, S. (2022, September 2). “GitHub Security 101: Best Practices for Securing your Repository”. GitGuardian. https://blog.gitguardian.com/github-security-101/

Sette, N. (2019). Repository Threats [Graphic]. Kroll. https://www.kroll.com/-/media/kroll/images/publications/the-monitor/issue-10/the-monitor-issue-10-image-1.jpg