

Application Security Architecture Cheat Sheet

From OWASP

Contents

- 1 Introduction
- 2 Business Requirements
 - 2.1 Business Model
 - 2.2 Data Essentials
 - 2.3 End-Users
 - 2.4 Partners
 - 2.5 Administrators
 - 2.6 Regulations
- 3 Infrastructure Requirements
 - 3.1 Network
 - 3.2 Systems
 - 3.3 Infrastructure Monitoring
 - 3.4 Virtualization and Externalization
- 4 Application Requirements
 - 4.1 Environment
 - 4.2 Data Processing
 - 4.3 Access
 - 4.4 Application Monitoring
 - 4.5 Application Design
- 5 Security Program Requirements
 - 5.1 Operations
 - 5.2 Change Management
 - 5.3 Software Development
 - 5.4 Corporate
- 6 Related Cheat Sheets
- 7 Authors and Primary Editors

Introduction

This cheat sheet offers tips for the initial design and review of an application's security architecture.

Business Requirements

Business Model

- What is the application's primary business purpose?
- How will the application make money?
- What are the planned business milestones for developing or improving the application?
- How is the application marketed?
- What key benefits does application offer its users?
- What business continuity provisions have been defined for the application?
- What geographic areas does the application service?

Data Essentials

- What data does the application receive, produce, and process?
- How can the data be classified into categories according to its sensitivity?
- How might an attacker benefit from capturing or modifying the data?
- What data backup and retention requirements have been defined for the application?

End-Users

- Who are the application's end-users?
- How do the end-users interact with the application?
- What security expectations do the end-users have?

Partners

- Which third-parties supply data to the application?
- Which third-parties receive data from the applications?
- Which third-parties process the application's data?
- What mechanisms are used to share data with third-parties besides the application itself?
- What security requirements do the partners impose?

Administrators

- Who has administrative capabilities in the application?
- What administrative capabilities does the application offer?

Regulations

- In what industries does the application operate?

- What security-related regulations apply?
- What auditing and compliance regulations apply?

Infrastructure Requirements

Network

- What details regarding routing, switching, firewalling, and load-balancing have been defined?
- What network design supports the application?
- What core network devices support the application?
- What network performance requirements exist?
- What private and public network links support the application?

Systems

- What operating systems support the application?
- What hardware requirements have been defined?
- What details regarding required OS components and lock-down needs have been defined?

Infrastructure Monitoring

- What network and system performance monitoring requirements have been defined?
- What mechanisms exist to detect malicious code or compromised application components?
- What network and system security monitoring requirements have been defined?

Virtualization and Externalization

- What aspects of the application lend themselves to virtualization?
- What virtualization requirements have been defined for the application?
- What aspects of the product may or may not be hosted via the cloud computing model?

Application Requirements

Environment

- What frameworks and programming languages have been used to create the application?
- What process, code, or infrastructure dependencies have been defined for the application?

- What databases and application servers support the application?

Data Processing

- What data entry paths does the application support?
- What data output paths does the application support?
- How does data flow across the application's internal components?
- What data input validation requirements have been defined?
- What data does the application store and how?
- What data is or may need to be encrypted and what key management requirements have been defined?
- What capabilities exist to detect the leakage of sensitive data?
- What encryption requirements have been defined for data in transit over WAN and LAN links?

Access

- What user privilege levels does the application support?
- What user identification and authentication requirements have been defined?
- What user authorization requirements have been defined?
- What session management requirements have been defined?
- What access requirements have been defined for URI and Service calls?
- What user access restrictions have been defined?
- How are user identities maintained throughout transaction calls?

Application Monitoring

- What application auditing requirements have been defined?
- What application performance monitoring requirements have been defined?
- What application security monitoring requirements have been defined?
- What application error handling and logging requirements have been defined?
- How are audit and debug logs accessed, stored, and secured?

Application Design

- What application design review practices have been defined and executed?
- How is intermediate or in-process data stored in the application components' memory and in cache?
- How many logical tiers group the application's components?
- What staging, testing, and Quality Assurance requirements have been defined?

Security Program Requirements

Operations

- What is the process for identifying and addressing vulnerabilities in the application?
- What is the process for identifying and addressing vulnerabilities in network and system components?
- What access to system and network administrators have to the application's sensitive data?
- What security incident requirements have been defined?
- How do administrators access production infrastructure to manage it?
- What physical controls restrict access to the application's components and data?
- What is the process for granting access to the environment hosting the application?

Change Management

- How are changes to the code controlled?
- How are changes to the infrastructure controlled?
- How is code deployed to production?
- What mechanisms exist to detect violations of change management practices?

Software Development

- What data is available to developers for testing?
- How do developers assist with troubleshooting and debugging the application?
- What requirements have been defined for controlling access to the applications source code?
- What secure coding processes have been established?

Corporate

- What corporate security program requirements have been defined?
- What security training do developers and administrators undergo?
- Which personnel oversees security processes and requirements related to the application?
- What employee initiation and termination procedures have been defined?
- What application requirements impose the need to enforce the principle of separation of duties?
- What controls exist to protect a compromised in the corporate environment from affecting production?
- What security governance requirements have been defined?

Related Cheat Sheets

OWASP Cheat Sheet Series

- Authentication Cheat Sheet

- [Cross-Site Request Forgery \(CSRF\) Prevention Cheat Sheet](#)
- [Transport Layer Protection Cheat Sheet](#)
- [Cryptographic Storage Cheat Sheet](#)
- [Input Validation Cheat Sheet](#)
- [XSS \(Cross Site Scripting\) Prevention Cheat Sheet](#)
- [DOM based XSS Prevention Cheat Sheet](#)
- [Forgot Password Cheat Sheet](#)
- [SQL Injection Prevention Cheat Sheet](#)
- [Session Management Cheat Sheet](#)
- [HTML5 Security Cheat Sheet](#)
- [Web Service Security Cheat Sheet](#)
- **[Application Security Architecture Cheat Sheet](#)**

Draft OWASP Cheat Sheets

- [PHP Security Cheat Sheet](#)
- [Password Storage Cheat Sheet](#)

Cheat Sheets Project Homepage

- [Cheat Sheets](#)

Authors and Primary Editors

Lenny Zeltser (<http://www.zeltser.com>)

Retrieved from "https://www.owasp.org/index.php/Application_Security_Architecture_Cheat_Sheet"
Category: Cheatsheets

- Powered by MediaWiki OWASP Foundation © 2011

