microservices security in action pdf

microservices security in action pdf is a sought-after resource for developers, architects, and security professionals navigating the complexities of securing distributed systems. This article delves deep into the practical application of microservices security principles, offering insights akin to what you'd find in a comprehensive "microservices security in action pdf." We will explore common vulnerabilities, effective defense strategies, and best practices for building resilient and secure microservice architectures. From authentication and authorization to data protection and API gateway security, this guide aims to equip you with the knowledge to implement robust security measures for your microservices.

Understanding the Microservices Security Landscape

The shift towards microservices has revolutionized software development, enabling agility, scalability, and independent deployment. However, this distributed nature introduces a unique set of security challenges that differ significantly from traditional monolithic applications. Each microservice, acting as an independent unit, becomes a potential attack vector. Understanding these inherent complexities is the first step in building a secure microservice ecosystem. The fragmented nature of communication, the proliferation of APIs, and the dynamic scaling of services all demand a proactive and layered security approach.

The Unique Security Challenges of Microservices

Monolithic applications, while possessing their own security concerns, often present a more contained attack surface. In contrast, microservices, by design, expose numerous interfaces and communication channels. This distributed environment means that a security breach in one service could potentially compromise others if proper isolation and communication security are not implemented. The complexity of managing security configurations across a multitude of independent services, each potentially built with different technologies and managed by different teams, adds another layer of difficulty. Furthermore, the rapid pace of development and deployment in microservice architectures can sometimes lead to security best practices being overlooked or implemented hastily, creating vulnerabilities.

Key Threat Vectors in Microservice Architectures

Several key threat vectors target microservices specifically. These include attacks aimed at compromising APIs, which serve as the primary communication channel between services. Insecure inter-service communication, where data is transmitted without adequate encryption or authentication, is another significant risk. Vulnerabilities within individual microservices themselves, such as injection flaws or broken authentication, can also be exploited. Additionally, issues related to access control and identity management across a distributed system can lead to unauthorized access. The rise of containerization and

orchestration platforms, while beneficial for deployment, also introduces its own set of security considerations.

Core Principles of Microservices Security

Building secure microservices requires a fundamental understanding of core security principles adapted to the distributed paradigm. These principles act as a foundation upon which robust security measures can be built. They emphasize a defense-in-depth strategy, where multiple layers of security are employed to protect the system, even if one layer is compromised. This holistic approach is crucial for mitigating the expanded attack surface inherent in microservice architectures. Applying these principles diligently ensures that security is not an afterthought but an integral part of the microservice lifecycle.

Defense in Depth for Microservices

Defense in depth is a security strategy that employs multiple overlapping security controls. In the context of microservices, this means implementing security at various levels: the network, the API gateway, individual service boundaries, within the services themselves, and at the data layer. No single security control is expected to be completely foolproof, so having multiple layers provides redundancy and increases the difficulty for attackers to penetrate the system. This layered approach is particularly effective against sophisticated, multi-stage attacks.

Principle of Least Privilege

The principle of least privilege dictates that every process, user, or service should only have the minimum permissions necessary to perform its intended function. For microservices, this translates to granting each service only the access and resources it absolutely requires to operate. This limits the potential damage if a particular service is compromised, as the attacker's reach will be constrained by the service's limited privileges. Implementing granular access control mechanisms is key to enforcing this principle effectively.

Zero Trust Security Model

The zero trust security model operates on the principle of "never trust, always verify." It assumes that threats can originate from both outside and inside the network perimeter. In a microservice environment, this means that every request, regardless of its origin (even from within the internal network), must be authenticated and authorized. This approach is highly effective in microservices, where inter-service communication is constant and the traditional perimeter security model becomes less relevant.

Implementing Authentication and Authorization

in Microservices

Authentication and authorization are foundational pillars of microservices security. They ensure that only legitimate users and services can access resources and that they have the appropriate permissions. Implementing these mechanisms effectively in a distributed system requires careful consideration of various technologies and patterns. Without robust authentication and authorization, the entire microservice ecosystem is vulnerable to unauthorized access and data breaches, undermining the very benefits of agility and scalability that microservices offer.

Identity and Access Management (IAM) Strategies

Effective IAM in microservices involves managing the identities of users, services, and devices, and defining their access rights. This can be achieved through various mechanisms, such as OAuth 2.0, OpenID Connect, and JSON Web Tokens (JWTs). Centralized identity providers can simplify the management of identities across numerous services, ensuring consistency and reducing the overhead of managing credentials for each individual microservice.

Securing Inter-Service Communication

The communication between microservices is a critical security concern. Employing mutual TLS (mTLS) for authentication and encryption of service-to-service communication is a robust solution. This ensures that both the client and server verify each other's identity before establishing a secure connection. Additionally, using API gateways can help centralize security concerns like authentication and rate limiting for incoming requests.

API Gateway Security Best Practices

The API gateway acts as a single entry point for all client requests to the microservices. It is therefore crucial to secure it effectively. This includes implementing strong authentication and authorization mechanisms for incoming requests, performing input validation, rate limiting to prevent denial-of-service attacks, and logging all requests for auditing purposes. A well-secured API gateway can significantly reduce the attack surface exposed to the outside world.

Data Security and Protection in Microservices

Protecting sensitive data is paramount in any microservice architecture. Given the distributed nature of data storage and processing, implementing comprehensive data security measures is vital. This involves ensuring data confidentiality, integrity, and availability across all services. Neglecting data security can lead to severe consequences, including regulatory fines, reputational damage, and loss of customer trust. This section explores practical approaches to safeguard your data.

Encryption Strategies for Data at Rest and in Transit

Data security in microservices relies heavily on encryption. Data at rest, residing in databases or storage systems, should be encrypted using strong encryption algorithms. Similarly, data in transit, exchanged between services or between clients and services, must be encrypted using protocols like TLS/SSL. This ensures that even if data is intercepted, it remains unreadable to unauthorized parties. Key management is a critical component of any encryption strategy.

Secure Data Storage and Access Control

Each microservice might have its own dedicated data store, making data access control a complex challenge. Implementing granular access control policies for each data store based on the principle of least privilege is essential. This involves defining who can access what data and for what purpose. Regular auditing of data access logs helps detect and prevent unauthorized access attempts. Database security best practices, such as secure configuration and vulnerability patching, are also crucial.

Handling Sensitive Data and Compliance

Microservices often process and store sensitive information, such as personal identifiable information (PII) or financial data. This necessitates adherence to various data privacy regulations like GDPR, CCPA, and HIPAA. Implementing data masking, anonymization, and tokenization techniques can help protect sensitive data while still allowing it to be used for analysis or processing. Regular security audits and compliance checks are indispensable to ensure ongoing adherence to regulatory requirements.

Operational Security and Monitoring for Microservices

Maintaining the security of microservices extends beyond initial implementation; it requires continuous operational vigilance and robust monitoring. The dynamic nature of microservices means that security postures can change rapidly, making ongoing monitoring and rapid response capabilities essential. This section focuses on the practices that keep your microservice ecosystem secure in operation.

Centralized Logging and Auditing

Effective logging and auditing are critical for detecting and investigating security incidents in microservices. Centralizing logs from all microservices provides a unified view of system activity, making it easier to identify suspicious patterns, track down the source of security breaches, and perform forensic analysis. Implementing consistent logging formats and retention policies across all services is crucial for effective analysis.

Security Monitoring and Alerting

Implementing real-time security monitoring and alerting mechanisms is vital for early detection of threats. This involves setting up tools that can detect anomalous behavior, such as unusual traffic patterns, unauthorized access attempts, or sudden spikes in error rates, and trigger immediate alerts to the security team. Continuous monitoring helps to proactively address potential security issues before they escalate into major breaches.

Incident Response and Recovery Planning

Having a well-defined incident response plan is essential for any microservice architecture. This plan outlines the steps to be taken in the event of a security incident, including containment, eradication, and recovery. Regular testing and refinement of the incident response plan ensure that the team is prepared to act swiftly and effectively when a security breach occurs, minimizing downtime and potential damage.

DevSecOps and Security Automation

Integrating security into the software development lifecycle, a practice known as DevSecOps, is crucial for building secure microservices from the ground up. Automation plays a key role in enabling DevSecOps, allowing for security checks and measures to be performed continuously and efficiently. This proactive approach shifts security left, addressing vulnerabilities early in the development process.

Integrating Security into the CI/CD Pipeline

Security should not be an afterthought but an integral part of the Continuous Integration/Continuous Deployment (CI/CD) pipeline. This involves automating security checks at various stages, such as static application security testing (SAST), dynamic application security testing (DAST), software composition analysis (SCA) for identifying vulnerable dependencies, and container security scanning. Automating these checks ensures that security is considered throughout the development and deployment process.

Automated Security Testing and Vulnerability Management

Leveraging automated security testing tools allows for frequent and comprehensive security assessments of microservices. This includes automated penetration testing, fuzz testing, and security configuration audits. Establishing a robust vulnerability management process, which involves identifying, prioritizing, and remediating vulnerabilities discovered through automated testing and other means, is essential for maintaining a secure microservice posture.

Frequently Asked Questions

What are the key security challenges unique to microservices architectures?

Key challenges include increased attack surface due to numerous services, complex inter-service communication, distributed identity and access management, data security across distributed systems, and the need for robust logging and monitoring across a decentralized environment.

How does a 'microservices security in action' PDF typically address authentication and authorization?

It would likely cover strategies like OAuth 2.0 and OpenID Connect for authentication, API gateways for centralized authentication, role-based access control (RBAC) or attribute-based access control (ABAC) for authorization at the service level, and the use of JSON Web Tokens (JWTs) for carrying user identity and permissions.

What are common security patterns for securing inter-service communication in microservices?

Common patterns include mutual TLS (mTLS) for encrypted and authenticated communication between services, service mesh solutions (like Istio or Linkerd) for enforcing security policies and managing traffic, and API gateways acting as a secure entry point and enforcing policies before requests reach services.

How does a PDF on microservices security discuss data protection across distributed services?

It would emphasize strategies like encrypting data at rest and in transit, implementing fine-grained access controls for data, securing secrets (API keys, database credentials) using dedicated secret management tools (e.g., HashiCorp Vault, AWS Secrets Manager), and ensuring data privacy compliance.

What role does an API Gateway play in microservices security, as often detailed in such PDFs?

An API Gateway acts as a single entry point for external requests, centralizing security concerns. It can handle authentication, authorization, rate limiting, input validation, and SSL termination, reducing the security burden on individual microservices.

How does a 'microservices security in action' PDF approach the concept of zero trust?

It would likely advocate for a zero-trust model where no entity (user or service) is implicitly trusted. This involves continuous verification of identity, strict access controls for every

interaction, micro-segmentation, and least privilege principles applied to all services and their communications.

What are the recommended practices for securing microservices during development and deployment?

This includes performing regular security code reviews, using static and dynamic application security testing (SAST/DAST) tools, container security scanning, implementing secure CI/CD pipelines, and using infrastructure-as-code (IaC) with security checks to ensure consistent and secure deployments.

How does the PDF address logging and monitoring for microservices security?

It would stress the importance of centralized logging and monitoring across all services. This includes capturing security-relevant events (e.g., failed logins, unauthorized access attempts), using security information and event management (SIEM) systems for analysis, and setting up alerts for suspicious activities.

What specific vulnerabilities are commonly discussed in relation to microservices security?

Common vulnerabilities include insecure API endpoints, broken authentication and authorization, injection flaws (SQL, command), insecure dependencies, misconfigured containers, and insufficient logging and monitoring, all amplified by the distributed nature of microservices.

How does a practical guide on microservices security often cover secret management?

It would detail secure methods for storing and accessing sensitive information like API keys, database credentials, and certificates. This includes using dedicated secret management tools, rotating secrets regularly, and avoiding hardcoding secrets within application code or configuration files.

Additional Resources

Here are 9 book titles related to microservices security, with descriptions, keeping in mind your request for titles that could be associated with a PDF resource like "microservices security in action pdf":

1. *Securing Your Microservices Architecture: A Practical Guide*
This book offers hands-on advice for implementing robust security measures within a microservices environment. It covers essential topics like authentication, authorization, API gateway security, and data encryption. Readers will find actionable strategies and code examples to fortify their distributed systems against common threats.

2. *Hands-On Microservices Security: From Design to Deployment*
Focusing on the practical aspects of microservices security, this resource guides developers and architects through the entire lifecycle. It delves into secure coding practices, identity and access management (IAM) for services, and vulnerability management. The book emphasizes a proactive security posture from the initial design phases through to continuous deployment.

3. *Microservices Security Patterns in Practice*
This title explores established security patterns and their real-world application in microservices. It breaks down complex security concepts into manageable, implementable solutions. The book provides case studies and best practices for addressing challenges like inter-service communication security and secrets management.

4. *Building Secure Microservices: A Developer's Handbook*
Designed for developers, this book provides the knowledge and tools necessary to build inherently secure microservices. It covers fundamental security principles, common attack vectors, and how to mitigate them at the code level. Expect guidance on secure API design, input validation, and defensive programming techniques.

5. *Microservices Security: Beyond the Perimeter*
This book shifts the focus from traditional perimeter security to the unique challenges of securing individual microservices. It explores concepts like Zero Trust, service mesh security, and fine-grained access control. The goal is to equip readers with strategies to secure services that are often exposed internally and externally.

6. *The Pragmatic Microservices Security Playbook*
Offering a no-nonsense approach to microservices security, this playbook provides actionable steps and checklists. It prioritizes practical solutions that can be implemented with existing toolchains and workflows. The book aims to demystify security for microservices and make it an integral part of everyday development.

7. *Microservices Security Implementation: A Comprehensive Overview*
This comprehensive resource covers a wide range of microservices security considerations, from fundamental principles to advanced techniques. It delves into aspects like secure service-to-service communication, container security, and observability for security monitoring. The book serves as a valuable reference for anyone involved in securing microservices deployments.

8. *Containerized Microservices Security: Best Practices and Tools*
Specifically addressing the security implications of running microservices in containers, this book highlights best practices for platforms like Docker and Kubernetes. It covers secure image building, network policies, runtime security, and secrets management within containerized environments. Readers will gain insights into protecting their containerized microservices infrastructure.

9. *Mastering Microservices Security: A Deep Dive*
This title offers an in-depth exploration of the intricate details of microservices security. It goes beyond the basics to tackle advanced topics such as cryptographic protocols for inter-service communication, advanced threat modeling, and the use of security orchestration tools. The book is ideal for those seeking to achieve a deep understanding and advanced proficiency in securing microservices.

[Microservices Security In Action Pdf]

Microservices Security in Action

Are you struggling to secure your microservices architecture? Feeling overwhelmed by the sheer number of moving parts and the complexities of distributed security? You're not alone. Many organizations face significant challenges in implementing robust security measures across their microservices landscape, leading to vulnerabilities that can expose sensitive data and cripple your operations. This ebook provides practical, actionable strategies to address these challenges head-on.

This guide, "Microservices Security: A Practical Guide," will equip you with the knowledge and tools necessary to build and maintain a secure microservices ecosystem.

Contents:

Microservices Security: A Practical Guide (Article)

Introduction: The Microservices Security Landscape

The adoption of microservices architecture has exploded in recent years, offering benefits like scalability, agility, and independent deployments. However, this distributed nature introduces

significant security challenges not present in monolithic applications. Securing a microservices architecture requires a different approach, demanding a shift in mindset and the implementation of specialized security measures. This introduction sets the stage by outlining the key security concerns inherent in microservices and highlighting the importance of proactive security planning. We will explore the increased attack surface, the complexities of managing access control across multiple services, and the need for comprehensive monitoring and logging.

Chapter 1: Identifying and Assessing Security Risks in Microservices

Identifying and assessing security risks is paramount in securing your microservices architecture. This chapter delves into the specific vulnerabilities prevalent in microservices environments. We'll explore common attack vectors, including:

API Gateway Vulnerabilities: Misconfigurations, lack of input validation, and outdated API gateway software can create entry points for attackers. We will discuss securing API gateways through robust authentication, authorization, and rate limiting.

Data Breaches: Data exposure from individual microservices due to insufficient data protection mechanisms (e.g., weak encryption, lack of access controls). This section will detail best practices for data encryption at rest and in transit, along with proper data access control implementation.

Inter-Service Communication Vulnerabilities: Insecure communication channels between microservices can allow attackers to intercept sensitive data or manipulate service interactions. We will cover securing inter-service communication with technologies like TLS/SSL, mutual TLS, and service meshes.

Dependency Vulnerabilities: Exploiting vulnerabilities in third-party libraries or dependencies used by microservices. We will discuss the importance of regular dependency scanning and updates to mitigate this risk.

Lack of Observability: The distributed nature of microservices makes it difficult to track and analyze events across the entire system. This section will discuss the crucial role of monitoring and logging to identify security incidents and potential threats early on.

This chapter concludes with a framework for conducting a comprehensive security risk assessment specific to a microservices environment, including the utilization of vulnerability scanning tools and penetration testing.

Chapter 2: Authentication and Authorization Strategies for Microservices

This chapter focuses on the critical aspects of authentication and authorization in a microservices context. We will explore various authentication methods, including OAuth 2.0, JWT (JSON Web Tokens), and OpenID Connect. The discussion will cover how to choose the appropriate authentication method based on specific needs and security requirements. Furthermore, we'll delve into authorization strategies, including role-based access control (RBAC), attribute-based access control (ABAC), and policy-based authorization. A key consideration will be how to implement these strategies across multiple services while maintaining consistency and managing complexities. The section will also touch upon techniques for securing API keys and managing secrets effectively.

Chapter 3: Securing Communication Between Microservices

Securing communication between microservices is crucial to prevent data breaches and unauthorized access. This chapter examines various methods for secure inter-service communication. We will discuss:

Using TLS/SSL: Encrypting communication channels between services using Transport Layer Security/Secure Sockets Layer. We'll cover certificate management, key rotation, and choosing appropriate cipher suites.

Mutual TLS: Establishing mutual authentication between services, ensuring that both communicating parties are verified.

Service Meshes: Leveraging service meshes like Istio or Linkerd to manage and secure communication between microservices. This will include a discussion of their features related to security, such as traffic management, authentication, and authorization policies.

API Gateways: Using API gateways as a central point of control and security for all inbound and outbound communication.

This chapter will also discuss best practices for selecting and implementing the most appropriate security measures based on the specific requirements of the microservices architecture.

Chapter 4: Data Security in a Microservices Architecture

This chapter focuses on securing data within a microservices architecture. We will explore strategies for:

Data Encryption: Encrypting data at rest and in transit using appropriate encryption algorithms. We’ll delve into the selection of strong encryption keys and secure key management practices.

Data Access Control: Implementing granular access control mechanisms to ensure that only authorized services and users can access sensitive data.

Data Loss Prevention (DLP): Implementing measures to prevent data leakage, such as data masking and monitoring.

Database Security: Securing databases used by microservices, including the implementation of database security best practices and regular security audits.

This chapter will highlight the importance of consistent data security policies across all microservices and the critical role of data governance in achieving this goal.

Chapter 5: Implementing Robust Monitoring and Logging for Security

Monitoring and logging are essential for detecting security incidents and identifying vulnerabilities. This chapter focuses on building robust monitoring and logging capabilities within a microservices architecture. We will cover:

Centralized Logging: Aggregating logs from various microservices into a centralized logging system for easier analysis and monitoring.

Security Information and Event Management (SIEM): Utilizing SIEM systems to correlate security events and detect suspicious activity.

Real-time Monitoring: Implementing real-time monitoring tools to identify security threats as they occur.

Alerting and Notifications: Setting up alerts and notifications to promptly respond to security incidents.

This chapter will emphasize the importance of designing a comprehensive monitoring and logging strategy from the beginning and the necessity of integrating security considerations into the monitoring infrastructure.

Chapter 6: DevSecOps Practices for Microservices

This chapter explores the implementation of DevSecOps practices to integrate security into the entire software development lifecycle (SDLC). We'll discuss:

Shift-Left Security: Incorporating security considerations early in the development process.

Automated Security Testing: Automating security tests as part of the CI/CD pipeline.

Security Code Reviews: Conducting thorough security code reviews to identify vulnerabilities before

deployment.

Infrastructure as Code (IaC): Using IaC tools to manage and secure infrastructure in a consistent and repeatable manner.

Compliance and Auditing: Adhering to relevant security standards and regulations.

This chapter will highlight how to embed security into the cultural and operational aspects of the organization, ensuring that security is a shared responsibility across development, operations, and security teams.

Chapter 7: Responding to and Recovering from Security Incidents

This chapter addresses how to respond to and recover from security incidents. We will explore incident response planning, including:

Incident Response Plan: Developing a detailed incident response plan outlining procedures for handling security incidents.

Incident Detection and Response: Implementing processes for detecting and responding to security incidents promptly.

Vulnerability Remediation: Developing procedures for patching and remediating vulnerabilities.

Post-Incident Analysis: Conducting post-incident analysis to identify root causes and prevent future incidents.

Communication and Reporting: Establishing clear communication channels and reporting procedures for security incidents.

This chapter stresses the importance of having a comprehensive incident response plan in place and regularly testing and updating it.

Conclusion: Building a Secure Future for Your Microservices

This book provides a comprehensive overview of securing microservices architectures. By applying the principles and techniques discussed, you can significantly strengthen the security posture of your microservices ecosystem. Remember that security is an ongoing process, requiring continuous monitoring, assessment, and adaptation. Stay updated on the latest security threats and best practices to ensure the long-term security and resilience of your microservices deployment.

FAQs

1. What is the difference between authentication and authorization in microservices? Authentication verifies the identity of a user or service, while authorization determines what actions a user or service is permitted to perform.

2. How can I secure communication between microservices deployed across different regions? Employ strong encryption (TLS/SSL or Mutual TLS) and consider using a service mesh for consistent security policies across regions.

3. What are the key benefits of using a service mesh for microservices security? Service meshes offer centralized traffic management, authentication, authorization, and observability, simplifying security management across a large number of microservices.

4. How do I choose the right authentication method for my microservices? The choice depends on your specific requirements, considering factors like scalability, security needs, and integration with existing systems. OAuth 2.0 and JWT are popular choices.

5. What are some common vulnerabilities in microservices APIs? Common vulnerabilities include insecure authentication, lack of input validation, SQL injection, and cross-site scripting (XSS).

6. How can I implement DevSecOps practices effectively in my microservices development? Integrate security testing into your CI/CD pipeline, conduct regular security code reviews, and use Infrastructure as Code (IaC) to manage and secure infrastructure consistently.

7. What are some best practices for securing data in a microservices architecture? Encrypt data at rest and in transit, implement granular access controls, and use data loss prevention (DLP) tools.

8. How can I monitor and log security events effectively in a microservices environment? Use a centralized logging system, integrate with a SIEM, and implement real-time monitoring with alerting capabilities.

9. What should be included in a comprehensive incident response plan for microservices? Include procedures for incident detection, response, remediation, post-incident analysis, and communication.

Related Articles:

1. Securing Microservices with OAuth 2.0: A deep dive into implementing OAuth 2.0 for secure authentication in microservices.

2. Implementing JWT Authentication in Microservices: A practical guide to using JSON Web Tokens for authentication and authorization.

3. Microservices Security Best Practices: A Checklist: A comprehensive checklist of best practices for securing microservices.

4. Service Mesh Security: A Comparative Analysis: A comparison of popular service mesh technologies and their security features.

5. API Gateway Security: Protecting Your Microservices APIs: A focused discussion on securing API gateways to protect microservices APIs.

6. Data Security in Microservices: Encryption and Access Control: A detailed explanation of data encryption and access control techniques for microservices.

7. DevSecOps for Microservices: Implementing a Secure CI/CD Pipeline: A guide to integrating security into the CI/CD pipeline for microservices.

8. Incident Response Planning for Microservices: A Step-by-Step Guide: A step-by-step guide to creating a comprehensive incident response plan for microservices.

9. Microservices Security Monitoring and Logging: Best Practices: A detailed discussion of best practices for monitoring and logging security events in microservices.

microservices security in action pdf: *Microservices Security in Action* Wajjakkara Kankanamge Anthony Nuwan Dias, Prabath Siriwardena, 2020-07-11 ”A complete guide to the challenges and solutions in securing microservices architectures.” —Massimo Siani, FinDynamic Key Features Secure microservices infrastructure and code Monitoring, access control, and microservice-to-microservice communications Deploy securely using Kubernetes, Docker, and the Istio service mesh. Hands-on examples and exercises using Java and Spring Boot Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. Microservices Security in Action teaches you how to address microservices-specific security challenges throughout the system. This practical guide includes plentiful hands-on exercises using industry-leading open-source tools and examples using Java and Spring Boot. About The Book Design and implement security into your microservices from the start. Microservices Security in Action teaches you to assess and address security challenges at every level of a Microservices application, from APIs to infrastructure. You’ll find effective solutions to common security problems, including throttling and monitoring, access control at the API gateway, and microservice-to-microservice communication. Detailed Java code samples, exercises, and real-world business use cases ensure you can put what you’ve learned into action immediately. What You Will Learn Microservice security concepts Edge services with an API gateway Deployments with Docker, Kubernetes, and Istio Security testing at the code level Communications with HTTP, gRPC, and Kafka This Book Is Written For For experienced microservices developers with intermediate Java skills. About The Author Prabath Siriwardena is the vice president of security architecture at WSO2. Nuwan Dias is the director of API architecture at WSO2. They have designed secure systems for many Fortune 500 companies. Table of Contents PART 1 OVERVIEW 1 Microservices security landscape 2 First steps in securing microservices PART 2 EDGE SECURITY 3 Securing north/south traffic with an API gateway 4 Accessing a secured microservice via a single-page application 5 Engaging throttling, monitoring, and access control PART 3 SERVICE-TO-SERVICE COMMUNICATIONS 6 Securing east/west traffic with certificates 7 Securing east/west traffic with JWT 8 Securing east/west traffic over gRPC 9

Securing reactive microservices PART 4 SECURE DEPLOYMENT 10 Conquering container security with Docker 11 Securing microservices on Kubernetes 12 Securing microservices with Istio service mesh PART 5 SECURE DEVELOPMENT 13 Secure coding practices and automation

microservices security in action pdf: API Security in Action Neil Madden, 2020-12-08 API Security in Action teaches you how to create secure APIs for any situation. By following this hands-on guide you'll build a social network API while mastering techniques for flexible multi-user security, cloud key management, and lightweight cryptography. Summary A web API is an efficient way to communicate with an application or service. However, this convenience opens your systems to new security risks. API Security in Action gives you the skills to build strong, safe APIs you can confidently expose to the world. Inside, you'll learn to construct secure and scalable REST APIs, deliver machine-to-machine interaction in a microservices architecture, and provide protection in resource-constrained IoT (Internet of Things) environments. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the technology APIs control data sharing in every service, server, data store, and web client. Modern data-centric designs—including microservices and cloud-native applications—demand a comprehensive, multi-layered approach to security for both private and public-facing APIs. About the book API Security in Action teaches you how to create secure APIs for any situation. By following this hands-on guide you'll build a social network API while mastering techniques for flexible multi-user security, cloud key management, and lightweight cryptography. When you're done, you'll be able to create APIs that stand up to complex threat models and hostile environments. What's inside Authentication Authorization Audit logging Rate limiting Encryption About the reader For developers with experience building RESTful APIs. Examples are in Java. About the author Neil Madden has in-depth knowledge of applied cryptography, application security, and current API security technologies. He holds a Ph.D. in Computer Science. Table of Contents PART 1 - FOUNDATIONS 1 What is API security? 2 Secure API development 3 Securing the Natter API PART 2 - TOKEN-BASED AUTHENTICATION 4 Session cookie authentication 5 Modern token-based authentication 6 Self-contained tokens and JWTs PART 3 - AUTHORIZATION 7 OAuth2 and OpenID Connect 8 Identity-based access control 9 Capability-based security and macaroons PART 4 - MICROSERVICE APIs IN KUBERNETES 10 Microservice APIs in Kubernetes 11 Securing service-to-service APIs PART 5 - APIs FOR THE INTERNET OF THINGS 12 Securing IoT communications 13 Securing IoT APIs

microservices security in action pdf: Spring Security in Action Laurentiu Spilca, 2020-11-03 Spring Security in Action shows you how to prevent cross-site scripting and request forgery attacks before they do damage. You'll start with the basics, simulating password upgrades and adding multiple types of authorization. As your skills grow, you'll adapt Spring Security to new architectures and create advanced OAuth2 configurations. By the time you're done, you'll have a customized Spring Security configuration that protects against threats both common and extraordinary. Summary While creating secure applications is critically important, it can also be tedious and time-consuming to stitch together the required collection of tools. For Java developers, the powerful Spring Security framework makes it easy for you to bake security into your software from the very beginning. Filled with code samples and practical examples, Spring Security in Action teaches you how to secure your apps from the most common threats, ranging from injection attacks to lackluster monitoring. In it, you'll learn how to manage system users, configure secure endpoints, and use OAuth2 and OpenID Connect for authentication and authorization. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the technology Security is non-negotiable. You rely on Spring applications to transmit data, verify credentials, and prevent attacks. Adopting secure by design principles will protect your network from data theft and unauthorized intrusions. About the book Spring Security in Action shows you how to prevent cross-site scripting and request forgery attacks before they do damage. You'll start with the basics, simulating password upgrades and adding multiple types of authorization. As your skills grow, you'll adapt Spring Security to new architectures and create advanced OAuth2

configurations. By the time you're done, you'll have a customized Spring Security configuration that protects against threats both common and extraordinary. What's inside Encoding passwords and authenticating users Securing endpoints Automating security testing Setting up a standalone authorization server About the reader For experienced Java and Spring developers. About the author Laurentiu Spilca is a dedicated development lead and trainer at Endava, with over ten years of Java experience. Table of Contents PART 1 - FIRST STEPS 1 Security Today 2 Hello Spring Security PART 2 - IMPLEMENTATION 3 Managing users 4 Dealing with passwords 5 Implementing authentication 6 Hands-on: A small secured web application 7 Configuring authorization: Restricting access 8 Configuring authorization: Applying restrictions 9 Implementing filters 10 Applying CSRF protection and CORS 11 Hands-on: A separation of responsibilities 12 How does OAuth 2 work? 13 OAuth 2: Implementing the authorization server 14 OAuth 2: Implementing the resource server 15 OAuth 2: Using JWT and cryptographic signatures 16 Global method security: Pre- and postauthorizations 17 Global method security: Pre- and postfiltering 18 Hands-on: An OAuth 2 application 19 Spring Security for reactive apps 20 Spring Security testing

microservices security in action pdf: Microservices in Action Morgan Bruce, Paulo A Pereira, 2018-10-03 The one [and only] book on implementing microservices with a real-world, cover-to-cover example you can relate to. - Christian Bach, Swiss Re Microservices in Action is a practical book about building and deploying microservice-based applications. Written for developers and architects with a solid grasp of service-oriented development, it tackles the challenge of putting microservices into production. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Technology Invest your time in designing great applications, improving infrastructure, and making the most out of your dev teams. Microservices are easier to write, scale, and maintain than traditional enterprise applications because they're built as a system of independent components. Master a few important new patterns and processes, and you'll be ready to develop, deploy, and run production-quality microservices. About the Book Microservices in Action teaches you how to write and maintain microservice-based applications. Created with day-to-day development in mind, this informative guide immerses you in real-world use cases from design to deployment. You'll discover how microservices enable an efficient continuous delivery pipeline, and explore examples using Kubernetes, Docker, and Google Container Engine. What's inside An overview of microservice architecture Building a delivery pipeline Best practices for designing multi-service transactions and queries Deploying with containers Monitoring your microservices About the Reader Written for intermediate developers familiar with enterprise architecture and cloud platforms like AWS and GCP. About the Author Morgan Bruce and Paulo A. Pereira are experienced engineering leaders. They work daily with microservices in a production environment, using the techniques detailed in this book. Table of Contents Designing and running microservices Microservices at SimpleBank Architecture of a microservice application Designing new features Transactions and queries in microservices Designing reliable services Building a reusable microservice framework Deploying microservices Deployment with containers and schedulers Building a delivery pipeline for microservices Building a monitoring system Using logs and traces to understand behavior Building microservice teams PART 1 - The lay of the land PART 2 - Design PART 3 - Deployment PART 4 - Observability and ownership

microservices security in action pdf: Spring Microservices in Action John Carnell, Kalpit Patel, 2017-06-11 Summary Spring Microservices in Action teaches you how to build microservice-based applications using Java and the Spring platform. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the technology Microservices break up your code into small, distributed, and independent services that require careful forethought and design. Fortunately, Spring Boot and Spring Cloud simplify your microservice applications, just as the Spring Framework simplifies enterprise Java development. Spring Boot removes the boilerplate code involved with writing a REST-based service. Spring Cloud provides a suite of tools for the discovery, routing, and deployment of microservices to the enterprise and the cloud. About the Book Spring Microservices in Action teaches you how to build

microservice-based applications using Java and the Spring platform. You'll learn to do microservice design as you build and deploy your first Spring Cloud application. Throughout the book, carefully selected real-life examples expose microservice-based patterns for configuring, routing, scaling, and deploying your services. You'll see how Spring's intuitive tooling can help augment and refactor existing applications with micro services. What's Inside Core microservice design principles Managing configuration with Spring Cloud Config Client-side resiliency with Spring, Hystrix, and Ribbon Intelligent routing using Netflix Zuul Deploying Spring Cloud applications About the Reader This book is written for developers with Java and Spring experience. About the Author John Carnell is a senior cloud engineer with twenty years of experience in Java. Table of contents Welcome to the cloud, Spring Building microservices with Spring Boot Controlling your configuration with Spring Cloud configuration server On service discovery When bad things happen: client resiliency patterns with Spring Cloud and Netflix Hystrix Service routing with Spring Cloud and Zuul Securing your microservices Event-driven architecture with Spring Cloud Stream Distributed tracing with Spring Cloud Sleuth and Zipkin Deploying your microservices

microservices security in action pdf: Security and Microservice Architecture on AWS Gaurav Raje, 2021-09-08 Security is usually an afterthought when organizations design microservices for cloud systems. Most companies today are exposed to potential security threats, but their response is more reactive than proactive. That leads to unnecessarily complicated architecture that's harder to implement and even harder to manage and scale. Author Gaurav Raje shows you how to build highly secure systems on AWS without increasing overhead. Ideal for cloud solution architects and software developers with AWS experience, this practical book starts with a high-level architecture and design discussion, then explains how to implement your solution in the cloud in a secure but frictionless manner. By leveraging the AWS Shared Responsibility Model, you'll be able to: Achieve complete mediation in microservices at the infrastructure level Implement a secure and reliable audit trail of all events within the system Develop architecture that aims to simplify compliance with various regulations in finance, medicine, and legal services Put systems in place that detect anomalous behavior and alert the proper administrators in case of a breach Scale security mechanisms on individual microservices independent of each other.

microservices security in action pdf: Istio in Action Christian E. Posta, Rinor Maloku, 2022-05-03 Solve difficult service-to-service communication challenges around security, observability, routing, and resilience with an Istio-based service mesh. Istio allows you to define these traffic policies as configuration and enforce them consistently without needing any service-code changes. In Istio in Action you will learn: Why and when to use a service mesh Envoy's role in Istio's service mesh Allowing North-South traffic into a mesh Fine-grained traffic routing Make your services robust to network failures Gain observability over your system with telemetry golden signals How Istio makes your services secure by default Integrate cloud-native applications with legacy workloads such as in VMs Reduce the operational complexity of your microservices with an Istio-powered service mesh! Istio in Action shows you how to implement this powerful new architecture and move your application-networking concerns to a dedicated infrastructure layer. Non-functional concerns stay separate from your application, so your code is easier to understand, maintain, and adapt regardless of programming language. In this practical guide, you'll go hands-on with the full-featured Istio service mesh to manage microservices communication. Helpful diagrams, example configuration, and examples make it easy to understand how to control routing, secure container applications, and monitor network traffic. Foreword by Eric Brewer. About the technology Offload complex microservice communication layer challenges to Istio! The industry-standard Istio service mesh radically simplifies security, routing, observability, and other service-to-service communication challenges. With Istio, you use a straightforward declarative configuration style to establish application-level network policies. By separating communication from business logic, your services are easier to write, maintain, and modify. About the book Istio in Action teaches you how to implement an Istio-based service mesh that can handle complex routing scenarios, traffic encryption, authorization, and other common network-related tasks. You'll start by defining a basic service mesh

and exploring the data plane with Istio's service proxy, Envoy. Then, you'll dive into core topics like traffic routing and visualization and service-to-service authentication, as you expand your service mesh to workloads on multiple clusters and legacy VMs. What's inside Comprehensive coverage of Istio resources Practical examples to showcase service mesh capabilities Implementation of multi-cluster service meshes How to extend Istio with WebAssembly Traffic routing and observability VM integration into the mesh About the reader For developers, architects, and operations engineers. About the author Christian Posta is a well-known architect, speaker, and contributor. Rinor Maloku is an engineer at Solo.io working on application networking solutions. ToC PART 1 UNDERSTANDING ISTIO 1 Introducing the Istio service mesh 2 First steps with Istio 3 Istio's data plane: The Envoy proxy PART 2 SECURING, OBSERVING, AND CONTROLLING YOUR SERVICE'S NETWORK TRAFFIC 4 Istio gateways: Getting traffic into a cluster 5 Traffic control: Fine-grained traffic routing 6 Resilience: Solving application networking challenges 7 Observability: Understanding the behavior of your services 8 Observability: Visualizing network behavior with Grafana, Jaeger, and Kiali 9 Securing microservice communication PART 3 ISTIO DAY-2 OPERATIONS 10 Troubleshooting the data plane 11 Performance-tuning the control plane PART 4 ISTIO IN YOUR ORGANIZATION 12 Scaling Istio in your organization 13 Incorporating virtual machine workloads into the mesh 14 Extending Istio on the request path

microservices security in action pdf: *Microservices from Theory to Practice: Creating Applications in IBM Bluemix Using the Microservices Approach* Shahir Daya, Nguyen Van Duy, Kameswara Eati, Carlos M Ferreira, Dejan Glozic, Vasfi Gucer, Manav Gupta, Sunil Joshi, Valerie Lampkin, Marcelo Martins, Shishir Narain, Ramratan Vennam, IBM Redbooks, 2016-04-04 Microservices is an architectural style in which large, complex software applications are composed of one or more smaller services. Each of these microservices focuses on completing one task that represents a small business capability. These microservices can be developed in any programming language. They communicate with each other using language-neutral protocols, such as Representational State Transfer (REST), or messaging applications, such as IBM® MQ Light. This IBM Redbooks® publication gives a broad understanding of this increasingly popular architectural style, and provides some real-life examples of how you can develop applications using the microservices approach with IBM BluemixTM. The source code for all of these sample scenarios can be found on GitHub (https://github.com/). The book also presents some case studies from IBM products. We explain the architectural decisions made, our experiences, and lessons learned when redesigning these products using the microservices approach. Information technology (IT) professionals interested in learning about microservices and how to develop or redesign an application in Bluemix using microservices can benefit from this book.

microservices security in action pdf: Microservices Patterns Chris Richardson, 2018-10-27 A comprehensive overview of the challenges teams face when moving to microservices, with industry-tested solutions to these problems. - Tim Moore, Lightbend 44 reusable patterns to develop and deploy reliable production-quality microservices-based applications, with worked examples in Java Key Features 44 design patterns for building and deploying microservices applications Drawing on decades of unique experience from author and microservice architecture pioneer Chris Richardson A pragmatic approach to the benefits and the drawbacks of microservices architecture Solve service decomposition, transaction management, and inter-service communication Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About The Book Microservices Patterns teaches you 44 reusable patterns to reliably develop and deploy production-quality microservices-based applications. This invaluable set of design patterns builds on decades of distributed system experience, adding new patterns for composing services into systems that scale and perform under real-world conditions. More than just a patterns catalog, this practical guide with worked examples offers industry-tested advice to help you design, implement, test, and deploy your microservices-based application. What You Will Learn How (and why!) to use microservices architecture Service decomposition strategies Transaction management and querying patterns Effective testing strategies Deployment patterns This Book Is Written For Written for

enterprise developers familiar with standard enterprise application architecture. Examples are in Java. About The Author Chris Richardson is a Java Champion, a JavaOne rock star, author of Manning’s POJOs in Action, and creator of the original CloudFoundry.com. Table of Contents Escaping monolithic hell Decomposition strategies Interprocess communication in a microservice architecture Managing transactions with sagas Designing business logic in a microservice architecture Developing business logic with event sourcing Implementing queries in a microservice architecture External API patterns Testing microservices: part 1 Testing microservices: part 2 Developing production-ready services Deploying microservices Refactoring to microservices

microservices security in action pdf: Learn Microservices with Spring Boot Moises Macero, 2017-12-08 Build a microservices architecture with Spring Boot, by evolving an application from a small monolith to an event-driven architecture composed of several services. This book follows an incremental approach to teach microservice structure, test-driven development, Eureka, Ribbon, Zuul, and end-to-end tests with Cucumber. Author Moises Macero follows a very pragmatic approach to explain the benefits of using this type of software architecture, instead of keeping you distracted with theoretical concepts. He covers some of the state-of-the-art techniques in computer programming, from a practical point of view. You’ll focus on what's important, starting with the minimum viable product but keeping the flexibility to evolve it. What You'll Learn Build microservices with Spring Boot Use event-driven architecture and messaging with RabbitMQ Create RESTful services with Spring Master service discovery with Eureka and load balancing with Ribbon Route requests with Zuul as your API gateway Write end-to-end rests for an event-driven architecture using Cucumber Carry out continuous integration and deployment Who This Book Is For Those with at least some prior experience with Java programming. Some prior exposure to Spring Boot recommended but not required.

microservices security in action pdf: Building Microservices with Go Nic Jackson, 2017-07-27 Your one-stop guide to the common patterns and practices, showing you how to apply these using the Go programming language About This Book This short, concise, and practical guide is packed with real-world examples of building microservices with Go It is easy to read and will benefit smaller teams who want to extend the functionality of their existing systems Using this practical approach will save your money in terms of maintaining a monolithic architecture and demonstrate capabilities in ease of use Who This Book Is For You should have a working knowledge of programming in Go, including writing and compiling basic applications. However, no knowledge of RESTful architecture, microservices, or web services is expected. If you are looking to apply techniques to your own projects, taking your first steps into microservice architecture, this book is for you. What You Will Learn Plan a microservice architecture and design a microservice Write a microservice with a RESTful API and a database Understand the common idioms and common patterns in microservices architecture Leverage tools and automation that helps microservices become horizontally scalable Get a grounding in containerization with Docker and Docker-Compose, which will greatly accelerate your development lifecycle Manage and secure Microservices at scale with monitoring, logging, service discovery, and automation Test microservices and integrate API tests in Go In Detail Microservice architecture is sweeping the world as the de facto pattern to build web-based applications. Golang is a language particularly well suited to building them. Its strong community, encouragement of idiomatic style, and statically-linked binary artifacts make integrating it with other technologies and managing microservices at scale consistent and intuitive. This book will teach you the common patterns and practices, showing you how to apply these using the Go programming language. It will teach you the fundamental concepts of architectural design and RESTful communication, and show you patterns that provide manageable code that is supportable in development and at scale in production. We will provide you with examples on how to put these concepts and patterns into practice with Go. Whether you are planning a new application or working in an existing monolith, this book will explain and illustrate with practical examples how teams of all sizes can start solving problems with microservices. It will help you understand Docker and Docker-Compose and how it can be used to isolate microservice dependencies and build

environments. We finish off by showing you various techniques to monitor, test, and secure your microservices. By the end, you will know the benefits of system resilience of a microservice and the advantages of Go stack. Style and approach The step-by-step tutorial focuses on building microservices. Each chapter expands upon the previous one, teaching you the main skills and techniques required to be a successful microservice practitioner.

microservices security in action pdf: Enterprise Java Microservices Kenneth Finnigan, 2018-09-27 Summary Enterprise Java Microservices is an example-rich tutorial that shows how to design and manage large-scale Java applications as a collection of microservices. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Technology Large applications are easier to develop and maintain when you build them from small, simple components. Java developers now enjoy a wide range of tools that support microservices application development, including right-sized app servers, open source frameworks, and well-defined patterns. Best of all, you can build microservices applications using your existing Java skills. About the Book Enterprise Java Microservices teaches you to design and build JVM-based microservices applications. You'll start by learning how microservices designs compare to traditional Java EE applications. Always practical, author Ken Finnigan introduces big-picture concepts along with the tools and techniques you'll need to implement them. You'll discover ecosystem components like Netflix Hystrix for fault tolerance and master the Just enough Application Server (JeAS) approach. To ensure smooth operations, you'll also examine monitoring, security, testing, and deploying to the cloud. What's inside The microservices mental model Cloud-native development Strategies for fault tolerance and monitoring Securing your finished applications About the Reader This book is for Java developers familiar with Java EE. About the Author Ken Finnigan leads the Thorntail project at Red Hat, which seeks to make developing microservices for the cloud with Java and Java EE as easy as possible. Table of Contents PART 1 MICROSERVICES BASICS Enterprise Java microservices Developing a simple RESTful microservice Just enough Application Server for microservices Microservices testing Cloud native development PART 2 - IMPLEMENTING ENTERPRISE JAVA MICROSERVICES Consuming microservices Discovering microservices for consumption Strategies for fault tolerance and monitoring Securing a microservice Architecting a microservice hybrid Data streaming with Apache Kafka

microservices security in action pdf: Microservices Eberhard Wolff, 2016-10-03 The Most Complete, Practical, and Actionable Guide to Microservices Going beyond mere theory and marketing hype, Eberhard Wolff presents all the knowledge you need to capture the full benefits of this emerging paradigm. He illuminates microservice concepts, architectures, and scenarios from a technology-neutral standpoint, and demonstrates how to implement them with today’s leading technologies such as Docker, Java, Spring Boot, the Netflix stack, and Spring Cloud. The author fully explains the benefits and tradeoffs associated with microservices, and guides you through the entire project lifecycle: development, testing, deployment, operations, and more. You’ll find best practices for architecting microservice-based systems, individual microservices, and nanoservices, each illuminated with pragmatic examples. The author supplements opinions based on his experience with concise essays from other experts, enriching your understanding and illuminating areas where experts disagree. Readers are challenged to experiment on their own the concepts explained in the book to gain hands-on experience. Discover what microservices are, and how they differ from other forms of modularization Modernize legacy applications and efficiently build new systems Drive more value from continuous delivery with microservices Learn how microservices differ from SOA Optimize the microservices project lifecycle Plan, visualize, manage, and evolve architecture Integrate and communicate among microservices Apply advanced architectural techniques, including CQRS and Event Sourcing Maximize resilience and stability Operate and monitor microservices in production Build a full implementation with Docker, Java, Spring Boot, the Netflix stack, and Spring Cloud Explore nanoservices with Amazon Lambda, OSGi, Java EE, Vert.x, Erlang, and Seneca Understand microservices’ impact on teams, technical leaders, product owners, and stakeholders Managers will discover better ways to support microservices, and learn how adopting

the method affects the entire organization. Developers will master the technical skills and concepts they need to be effective. Architects will gain a deep understanding of key issues in creating or migrating toward microservices, and exactly what it will take to transform their plans into reality.

microservices security in action pdf: *Secure by Design* Daniel Sawano, Dan Bergh Johnsson, Daniel Deogun, 2019-09-03 Summary Secure by Design teaches developers how to use design to drive security in software development. This book is full of patterns, best practices, and mindsets that you can directly apply to your real world development. You'll also learn to spot weaknesses in legacy code and how to address them. About the technology Security should be the natural outcome of your development process. As applications increase in complexity, it becomes more important to bake security-mindedness into every step. The secure-by-design approach teaches best practices to implement essential software features using design as the primary driver for security. About the book Secure by Design teaches you principles and best practices for writing highly secure software. At the code level, you'll discover security-promoting constructs like safe error handling, secure validation, and domain primitives. You'll also master security-centric techniques you can apply throughout your build-test-deploy pipeline, including the unique concerns of modern microservices and cloud-native designs. What's inside Secure-by-design concepts Spotting hidden security problems Secure code constructs Assessing security by identifying common design flaws Securing legacy and microservices architectures About the reader Readers should have some experience in designing applications in Java, C#, .NET, or a similar language. About the author Dan Bergh Johnsson, Daniel Deogun, and Daniel Sawano are acclaimed speakers who often present at international conferences on topics of high-quality development, as well as security and design.

microservices security in action pdf: *Learn Kubernetes Security* Kaizhe Huang, Pranjal Jumde, 2020-07-09 Secure your container environment against cyberattacks and deliver robust deployments with this practical guide Key FeaturesExplore a variety of Kubernetes components that help you to prevent cyberattacksPerform effective resource management and monitoring with Prometheus and built-in Kubernetes toolsLearn techniques to prevent attackers from compromising applications and accessing resources for crypto-coin miningBook Description Kubernetes is an open source orchestration platform for managing containerized applications. Despite widespread adoption of the technology, DevOps engineers might be unaware of the pitfalls of containerized environments. With this comprehensive book, you'll learn how to use the different security integrations available on the Kubernetes platform to safeguard your deployments in a variety of scenarios. Learn Kubernetes Security starts by taking you through the Kubernetes architecture and the networking model. You'll then learn about the Kubernetes threat model and get to grips with securing clusters. Throughout the book, you'll cover various security aspects such as authentication, authorization, image scanning, and resource monitoring. As you advance, you'll learn about securing cluster components (the kube-apiserver, CoreDNS, and kubelet) and pods (hardening image, security context, and PodSecurityPolicy). With the help of hands-on examples, you'll also learn how to use open source tools such as Anchore, Prometheus, OPA, and Falco to protect your deployments. By the end of this Kubernetes book, you'll have gained a solid understanding of container security and be able to protect your clusters from cyberattacks and mitigate cybersecurity threats. What you will learnUnderstand the basics of Kubernetes architecture and networkingGain insights into different security integrations provided by the Kubernetes platformDelve into Kubernetes' threat modeling and security domainsExplore different security configurations from a variety of practical examplesGet to grips with using and deploying open source tools to protect your deploymentsDiscover techniques to mitigate or prevent known Kubernetes hacksWho this book is for This book is for security consultants, cloud administrators, system administrators, and DevOps engineers interested in securing their container deployments. If you're looking to secure your Kubernetes clusters and cloud-based deployments, you'll find this book useful. A basic understanding of cloud computing and containerization is necessary to make the most of this book.

microservices security in action pdf: Kubernetes Native Microservices with Quarkus and MicroProfile John Clingan, Ken Finnigan, 2022-03-01 Build fast, efficient Kubernetes-based

Java applications using the Quarkus framework, MicroProfile, and Java standards. In Kubernetes Native Microservices with Quarkus and MicroProfile you'll learn how to: Deploy enterprise Java applications on Kubernetes Develop applications using the Quarkus runtime Compile natively using GraalVM for blazing speed Create efficient microservices applications Take advantage of MicroProfile specifications Popular Java frameworks like Spring were designed long before Kubernetes and the microservices revolution. Kubernetes Native Microservices with Quarkus and MicroProfile introduces next generation tools that have been cloud-native and Kubernetes-aware right from the beginning. Written by veteran Java developers John Clingan and Ken Finnigan, this book shares expert insight into Quarkus and MicroProfile directly from contributors at Red Hat. You'll learn how to utilize these modern tools to create efficient enterprise Java applications that are easy to deploy, maintain, and expand. About the technology Build microservices efficiently with modern Kubernetes-first tools! Quarkus works naturally with containers and Kubernetes, radically simplifying the development and deployment of microservices. This powerful framework minimizes startup time and memory use, accelerating performance and reducing hosting cost. And because it's Java from the ground up, it integrates seamlessly with your existing JVM codebase. About the book Kubernetes Native Microservices with Quarkus and MicroProfile teaches you to build microservices using containers, Kubernetes, and the Quarkus framework. You'll immediately start developing a deployable application using Quarkus and the MicroProfile APIs. Then, you'll explore the startup and runtime gains Quarkus delivers out of the box and also learn how to supercharge performance by compiling natively using GraalVM. Along the way, you'll see how to integrate a Quarkus application with Spring and pick up pro tips for monitoring and managing your microservices. What's inside Deploy enterprise Java applications on Kubernetes Develop applications using the Quarkus runtime framework Compile natively using GraalVM for blazing speed Take advantage of MicroProfile specifications About the reader For intermediate Java developers comfortable with Java EE, Jakarta EE, or Spring. Some experience with Docker and Kubernetes required. About the author John Clingan is a senior principal product manager at Red Hat, where he works on enterprise Java standards and Quarkus. Ken Finnigan is a senior principal software engineer at Workday, previously at Red Hat working on Quarkus. Table of Contents PART 1 INTRODUCTION 1 Introduction to Quarkus, MicroProfile, and Kubernetes 2 Your first Quarkus application PART 2 DEVELOPING MICROSERVICES 3 Configuring microservices 4 Database access with Panache 5 Clients for consuming other microservices 6 Application health 7 Resilience strategies 8 Reactive in an imperative world 9 Developing Spring microservices with Quarkus PART 3 OBSERVABILITY, API DEFINITION, AND SECURITY OF MICROSERVICES 10 Capturing metrics 11 Tracing microservices 12 API visualization 13 Securing a microservice

microservices security in action pdf: Practical Microservices Architectural Patterns Binildas Christudas, 2019-06-25 Take your distributed applications to the next level and see what the reference architectures associated with microservices can do for you. This book begins by showing you the distributed computing architecture landscape and provides an in-depth view of microservices architecture. Following this, you will work with CQRS, an essential pattern for microservices, and get a view of how distributed messaging works. Moving on, you will take a deep dive into Spring Boot and Spring Cloud. Coming back to CQRS, you will learn how event-driven microservices work with this pattern, using the Axon 2 framework. This takes you on to how transactions work with microservices followed by advanced architectures to address non-functional aspects such as high availability and scalability. In the concluding part of the book you develop your own enterprise-grade microservices application using the Axon framework and true BASE transactions, while making it as secure as possible. What You Will Learn Shift from monolith architecture to microservices Work with distributed and ACID transactionsBuild solid architectures without two-phase commit transactions Discover the high availability principles in microservices Who This Book Is For Java developers with basic knowledge of distributed and multi-threaded application architecture, and no knowledge of Spring Boot or Spring Cloud. Knowledge of CQRS and event-driven architecture is not mandatory as this book will cover these in depth.

microservices security in action pdf: Building Microservices with .NET Core Gaurav Kumar Aroraa, Lalit Kale, Kanwar Manish, 2017-06-14 Architect your .NET applications by breaking them into really small pieces—microservices—using this practical, example-based guide About This Book Start your microservices journey and understand a broader perspective of microservices development Build, deploy, and test microservices using ASP.Net MVC, Web API, and Microsoft Azure Cloud Get started with reactive microservices and understand the fundamentals behind it Who This Book Is For This book is for .NET Core developers who want to learn and understand microservices architecture and implement it in their .NET Core applications. It's ideal for developers who are completely new to microservices or have just a theoretical understanding of this architectural approach and want to gain a practical perspective in order to better manage application complexity. What You Will Learn Compare microservices with monolithic applications and SOA Identify the appropriate service boundaries by mapping them to the relevant bounded contexts Define the service interface and implement the APIs using ASP.NET Web API Integrate the services via synchronous and asynchronous mechanisms Implement microservices security using Azure Active Directory, OpenID Connect, and OAuth 2.0 Understand the operations and scaling of microservices in .NET Core Understand the testing pyramid and implement consumer-driven contract using pact net core Understand what the key features of reactive microservices are and implement them using reactive extension In Detail Microservices is an architectural style that promotes the development of complex applications as a suite of small services based on business capabilities. This book will help you identify the appropriate service boundaries within the business. We'll start by looking at what microservices are, and what the main characteristics are. Moving forward, you will be introduced to real-life application scenarios, and after assessing the current issues, we will begin the journey of transforming this application by splitting it into a suite of microservices. You will identify the service boundaries, split the application into multiple microservices, and define the service contracts. You will find out how to configure, deploy, and monitor microservices, and configure scaling to allow the application to quickly adapt to increased demand in the future. With an introduction to the reactive microservices, you strategically gain further value to keep your code base simple, focusing on what is more important rather than the messy asynchronous calls. Style and approach This guide serves as a stepping stone that helps .NET Core developers in their microservices architecture. This book provides just enough theory to understand the concepts and apply the examples.

microservices security in action pdf: Microservice APIs Jose Haro Peralta, 2023-03-07 Strategies, best practices, and patterns that will help you design resilient microservices architecture and streamline your API integrations. In Microservice APIs, you'll discover: Service decomposition strategies for microservices Documentation-driven development for APIs Best practices for designing REST and GraphQL APIs Documenting REST APIs with the OpenAPI specification (formerly Swagger) Documenting GraphQL APIs using the Schema Definition Language Building microservices APIs with Flask, FastAPI, Ariadne, and other frameworks Service implementation patterns for loosely coupled services Property-based testing to validate your APIs, and using automated API testing frameworks like schemathesis and Dredd Adding authentication and authorization to your microservice APIs using OAuth and OpenID Connect (OIDC) Deploying and operating microservices in AWS with Docker and Kubernetes Microservice APIs teaches you practical techniques for designing robust microservices with APIs that are easy to understand, consume, and maintain. You'll benefit from author José Haro Peralta's years of experience experimenting with microservices architecture, dodging pitfalls and learning from mistakes he's made. Inside you'll find strategies for delivering successful API integrations, implementing services with clear boundaries, managing cloud deployments, and handling microservices security. Written in a framework-agnostic manner, its universal principles can easily be applied to your favorite stack and toolset. About the technology Clean, clear APIs are essential to the success of microservice applications. Well-designed APIs enable reliable integrations between services and help simplify maintenance, scaling, and redesigns. Th is book teaches you the patterns, protocols, and strategies

you need to design, build, and deploy effective REST and GraphQL microservices APIs. About the book Microservice APIs gathers proven techniques for creating and building easy-to-consume APIs for microservices applications. Rich with proven advice and Python-based examples, this practical book focuses on implementation over philosophy. You'll learn how to build robust microservice APIs, test and protect them, and deploy them to the cloud following principles and patterns that work in any language. What's inside Service decomposition strategies for microservices Best practices for designing and building REST and GraphQL APIs Service implementation patterns for loosely coupled components API authorization with OAuth and OIDC Deployments with AWS and Kubernetes About the reader For developers familiar with the basics of web development. Examples are in Python. About the author José Haro Peralta is a consultant, author, and instructor. He's also the founder of microapis.io. Table of Contents PART 1 INTRODUCING MICROSERVICE APIS 1 What are microservice APIs? 2 A basic API implementation 3 Designing microservices PART 2 DESIGNING AND BUILDING REST APIS 4 Principles of REST API design 5 Documenting REST APIs with OpenAPI 6 Building REST APIs with Python 7 Service implementation patterns for microservices PART 3 DESIGNING AND BUILDING GRAPHQL APIS 8 Designing GraphQL APIs 9 Consuming GraphQL APIs 10 Building GraphQL APIs with Python PART 4 SECURING, TESTING, AND DEPLOYING MICROSERVICE APIS 11 API authorization and authentication 12 Testing and validating APIs 13 Dockerizing microservice APIs 14 Deploying microservice APIs with Kubernetes

microservices security in action pdf: Practical Cloud Security Chris Dotson, 2019-03-04 With their rapidly changing architecture and API-driven automation, cloud platforms come with unique security challenges and opportunities. This hands-on book guides you through security best practices for multivendor cloud environments, whether your company plans to move legacy on-premises projects to the cloud or build a new infrastructure from the ground up. Developers, IT architects, and security professionals will learn cloud-specific techniques for securing popular cloud platforms such as Amazon Web Services, Microsoft Azure, and IBM Cloud. Chris Dotson—an IBM senior technical staff member—shows you how to establish data asset management, identity and access management, vulnerability management, network security, and incident response in your cloud environment.

microservices security in action pdf: Microservices for the Enterprise Kasun Indrasiri, Prabath Siriwardena, 2018-11-14 Understand the key challenges and solutions around building microservices in the enterprise application environment. This book provides a comprehensive understanding of microservices architectural principles and how to use microservices in real-world scenarios. Architectural challenges using microservices with service integration and API management are presented and you learn how to eliminate the use of centralized integration products such as the enterprise service bus (ESB) through the use of composite/integration microservices. Concepts in the book are supported with use cases, and emphasis is put on the reality that most of you are implementing in a "brownfield" environment in which you must implement microservices alongside legacy applications with minimal disruption to your business. Microservices for the Enterprise covers state-of-the-art techniques around microservices messaging, service development and description, service discovery, governance, and data management technologies and guides you through the microservices design process. Also included is the importance of organizing services as core versus atomic, composite versus integration, and API versus edge, and how such organization helps to eliminate the use of a central ESB and expose services through an API gateway. What You'll LearnDesign and develop microservices architectures with confidence Put into practice the most modern techniques around messaging technologies Apply the Service Mesh pattern to overcome inter-service communication challenges Apply battle-tested microservices security patterns to address real-world scenarios Handle API management, decentralized data management, and observability Who This Book Is For Developers and DevOps engineers responsible for implementing applications around a microservices architecture, and architects and analysts who are designing such systems

microservices security in action pdf: HTTP/2 in Action Barry Pollard, 2019-03-06 Summary

HTTP/2 in Action is a complete guide to HTTP/2, one of the core protocols of the web. Because HTTP/2 has been designed to be easy to transition to, including keeping it backwards compatible, adoption is rapid and expected to increase over the next few years. Concentrating on practical matters, this interesting book presents key HTTP/2 concepts such as frames, streams, and multiplexing and explores how they affect the performance and behavior of your websites. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Technology HTTP—Hypertext Transfer Protocol—is the standard for exchanging messages between websites and browsers. And after 20 years, it's gotten a much-needed upgrade. With support for streams, server push, header compression, and prioritization, HTTP/2 delivers vast improvements in speed, security, and efficiency. About the Book HTTP/2 in Action teaches you everything you need to know to use HTTP/2 effectively. You'll learn how to optimize web performance with new features like frames, multiplexing, and push. You'll also explore real-world examples on advanced topics like flow control and dependencies. With ready-to-implement tips and best practices, this practical guide is sure to get you—and your websites—up to speed! What's Inside HTTP/2 for web developers Upgrading and troubleshooting Real-world examples and case studies QUIC and HTTP/3 About the Reader Written for web developers and site administrators. About the Authors Barry Pollard is a professional developer with two decades of experience developing, supporting, and tuning software and infrastructure. Table of Contents PART 1 MOVING TO HTTP/2 Web technologies and HTTP The road to HTTP/2 Upgrading to HTTP/2 PART 2 USING HTTP/2 HTTP/2 protocol basics Implementing HTTP/2 push Optimizing for HTTP/2 PART 3 ADVANCED HTTP/2 Advanced HTTP/2 concepts HPACK header compression PART 4 THE FUTURE OF HTTP TCP, QUIC, and HTTP/3 Where HTTP goes from here

microservices security in action pdf: Spring Microservices Rajesh RV, 2016-06-28 Build scalable microservices with Spring, Docker, and Mesos About This Book Learn how to efficiently build and implement microservices in Spring, and how to use Docker and Mesos to push the boundaries of what you thought possible Examine a number of real-world use cases and hands-on code examples. Distribute your microservices in a completely new way Who This Book Is For If you are a Spring developers and want to build cloud-ready, internet-scale applications to meet modern business demands, then this book is for you Developers will understand how to build simple Restful services and organically grow them to truly enterprise grade microservices ecosystems. What You Will Learn Get to know the microservices development lifecycle process See how to implement microservices governance Familiarize yourself with the microservices architecture and its benefits Use Spring Boot to develop microservices Find out how to avoid common pitfalls when developing microservices Be introduced to end-to-end microservices written in Spring Framework and Spring Boot In Detail The Spring Framework is an application framework and inversion of the control container for the Java platform. The framework's core features can be used by any Java application, but there are extensions to build web applications on top of the Java EE platform. This book will help you implement the microservice architecture in Spring Framework, Spring Boot, and Spring Cloud. Written to the latest specifications of Spring, you'll be able to build modern, Internet-scale Java applications in no time. We would start off with the guidelines to implement responsive microservices at scale. We will then deep dive into Spring Boot, Spring Cloud, Docker, Mesos, and Marathon. Next you will understand how Spring Boot is used to deploy autonomous services, server-less by removing the need to have a heavy-weight application server. Later you will learn how to go further by deploying your microservices to Docker and manage it with Mesos. By the end of the book, you'll will gain more clarity on how to implement microservices using Spring Framework and use them in Internet-scale deployments through real-world examples. Style and approach The book follows a step by step approach on how to develop microservices using Spring Framework, Spring Boot, and a set of Spring Cloud components that will help you scale your applications.

microservices security in action pdf: Spring Boot in Practice Somnath Musib, 2022-07-12 Spring Boot in Practice is full of practical recipes for common development problems in Spring Boot. Author Somnath Musib has spent years building applications with Spring, and he shares that

extensive experience in this focused guide. You'll master techniques for using Spring Data, Spring Security, and other Spring-centric solutions. Learn how to work with Spring Boot and Kotlin, handling connections for multiple platforms, and how Spring Boot can simplify building microservices and APIs. Each recipe is built around a real-world problem, complete with a full solution and thoughtful discussion.

microservices security in action pdf: Spring in Action Craig Walls, 2018-10-05 Summary Spring in Action, 5th Edition is the fully updated revision of Manning's bestselling Spring in Action. This new edition includes all Spring 5.0 updates, along with new examples on reactive programming, Spring WebFlux, and microservices. You'll also find the latest Spring best practices, including Spring Boot for application setup and configuration. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Technology Spring Framework makes life easier for Java developers. New features in Spring 5 bring its productivity-focused approach to microservices, reactive development, and other modern application designs. With Spring Boot now fully integrated, you can start even complex projects with minimal configuration code. And the upgraded WebFlux framework supports reactive apps right out of the box! About the Book Spring in Action, 5th Edition guides you through Spring's core features, explained in Craig Walls' famously clear style. You'll roll up your sleeves and build a secure database-backed web app step by step. Along the way, you'll explore reactive programming, microservices, service discovery, RESTful APIs, deployment, and expert best practices. Whether you're just discovering Spring or leveling up to Spring 5.0, this Manning classic is your ticket! What's inside Building reactive applications Spring MVC for web apps and RESTful web services Securing applications with Spring Security Covers Spring 5.0 Over 100,000 copies sold! About the Reader For intermediate Java developers. About the Author Craig Walls is a principal software engineer at Pivotal, a popular author, an enthusiastic supporter of Spring Framework, and a frequent conference speaker. Table of Contents PART 1 - FOUNDATIONAL SPRING Getting started with Spring Developing web applications Working with data Securing Spring Working with configuration properties PART 2 - INTEGRATED SPRING Creating REST services Consuming REST services Sending messages asynchronously Integrating Spring PART 3 - REACTIVE SPRING Introducing Reactor Developing reactive APIs Persisting data reactively PART 4 CLOUD-NATIVE SPRING Discovering services Managing configuration Handling failure and latency PART 5 - DEPLOYED SPRING Working with Spring Boot Actuator Administering Spring Monitoring Spring with JMX Deploying Spring

microservices security in action pdf: Building Microservices Sam Newman, 2015-02-02 Annotation Over the past 10 years, distributed systems have become more fine-grained. From the large multi-million line long monolithic applications, we are now seeing the benefits of smaller self-contained services. Rather than heavy-weight, hard to change Service Oriented Architectures, we are now seeing systems consisting of collaborating microservices. Easier to change, deploy, and if required retire, organizations which are in the right position to take advantage of them are yielding significant benefits. This book takes an holistic view of the things you need to be cognizant of in order to pull this off. It covers just enough understanding of technology, architecture, operations and organization to show you how to move towards finer-grained systems.

microservices security in action pdf: Terraform in Action Scott Winkler, 2021-08-24 An outstanding source of knowledge for Terraform enthusiasts of all levels. - Anton Babenko, Betajob Terraform in Action shows you how to automate and scale infrastructure programmatically using the Terraform toolkit. Summary In Terraform in Action you will learn: Cloud architecture with Terraform Terraform module sharing and the private module registry Terraform security in a multitenant environment Strategies for performing blue/green deployments Refactoring for code maintenance and reusability Running Terraform at scale Creating your own Terraform provider Using Terraform as a continuous development/continuous delivery platform Terraform in Action introduces the infrastructure-as-code (IaC) model that lets you instantaneously create new components and respond efficiently to changes in demand. You'll use the Terraform automation tool to design and manage servers that can be provisioned, shared, changed, tested, and deployed with a single command.

Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the technology Provision, deploy, scale, and clone your entire stack to the cloud at the touch of a button. In Terraform, you create a collection of simple declarative scripts that define and manage application infrastructure. This powerful infrastructure-as-code approach automates key tasks like versioning and testing for everything from low-level networking to cloud services. About the book Terraform in Action shows you how to automate and scale infrastructure programmatically using the Terraform toolkit. Using practical, relevant examples, you'll use Terraform to provision a Kubernetes cluster, deploy a multiplayer game, and configure other hands-on projects. As you progress to advanced techniques like zero-downtime deployments, you'll discover how to think in Terraform rather than just copying and pasting scripts. What's inside Cloud architecture with Terraform Terraform module sharing and the private module registry Terraform security in a multitenant environment Strategies for performing blue/green deployments About the reader For readers experienced with a major cloud platform such as AWS. Examples in JavaScript and Golang. About the author Scott Winkler is a DevOps engineer and a distinguished Terraform expert. He has spoken multiple times at HashiTalks and HashiConf, and was selected as a HashiCorp Ambassador and Core Contributor in 2020. Table of Contents PART 1 TERRAFORM BOOTCAMP 1 Getting started with Terraform 2 Life cycle of a Terraform resource 3 Functional programming 4 Deploying a multi-tiered web application in AWS PART 2 TERRAFORM IN THE WILD 5 Serverless made easy 6 Terraform with friends 7 CI/CD pipelines as code 8 A multi-cloud MMORPG PART 3 MASTERING TERRAFORM 9 Zero-downtime deployments 10 Testing and refactoring 11 Extending Terraform by writing a custom provider 12 Automating Terraform 13 Security and secrets management

microservices security in action pdf: Microservices: Up and Running Ronnie Mitra, Irakli Nadareishvili, 2020-11-25 Microservices architectures offer faster change speeds, better scalability, and cleaner, evolvable system designs. But implementing your first microservices architecture is difficult. How do you make myriad choices, educate your team on all the technical details, and navigate the organization to a successful execution to maximize your chance of success? With this book, authors Ronnie Mitra and Irakli Nadareishvili provide step-by-step guidance for building an effective microservices architecture. Architects and engineers will follow an implementation journey based on techniques and architectures that have proven to work for microservices systems. You'll build an operating model, a microservices design, an infrastructure foundation, and two working microservices, then put those pieces together as a single implementation. For anyone tasked with building microservices or a microservices architecture, this guide is invaluable. Learn an effective and explicit end-to-end microservices system design Define teams, their responsibilities, and guidelines for working together Understand how to slice a big application into a collection of microservices Examine how to isolate and embed data into corresponding microservices Build a simple yet powerful CI/CD pipeline for infrastructure changes Write code for sample microservices Deploy a working microservices application on Amazon Web Services

microservices security in action pdf: *Microservices and Containers* Parminder Singh Kocher, 2018-03-16 Transition to Microservices and DevOps to Transform Your Software Development Effectiveness Thanks to the tech sector's latest game-changing innovations—the Internet of Things (IoT), software-enabled networking, and software as a service (SaaS), to name a few—there is now a seemingly insatiable demand for platforms and architectures that can improve the process of application development and deployment. In Microservices and Containers, longtime systems architect and engineering team leader Parminder Kocher analyzes two of the hottest new technology trends: microservices and containers. Together, as Kocher demonstrates, microservices and Docker containers can bring unprecedented agility and scalability to application development and deployment, especially in large, complex projects where speed is crucial but small errors can be disastrous. Learn how to leverage microservices and Docker to drive modular architectural design, on-demand scalability, application performance and reliability, time-to-market, code reuse, and exponential improvements in DevOps effectiveness. Kocher offers detailed guidance and a complete

roadmap for transitioning from monolithic architectures, as well as an in-depth case study that walks the reader through the migration of an enterprise-class SOA system. Understand how microservices enable you to organize applications into standalone components that are easier to manage, update, and scale Decide whether microservices and containers are worth your investment, and manage the organizational learning curve associated with them Apply best practices for interprocess communication among microservices Migrate monolithic systems in an orderly fashion Understand Docker containers, installation, and interfaces Network, orchestrate, and manage Docker containers effectively Use Docker to maximize scalability in microservices-based applications Apply your learning with an in-depth, hands-on case study Whether you are a software architect/developer or systems professional looking to move on from older approaches or a manager trying to maximize the business value of these technologies, Microservices and Containers will be an invaluable addition to your library. Register your product at informit.com/register for convenient access to downloads, updates, and/or corrections as they become available.

microservices security in action pdf: Securing DevOps Julien Vehent, 2018-08-20 Summary Securing DevOps explores how the techniques of DevOps and security should be applied together to make cloud services safer. This introductory book reviews the latest practices used in securing web applications and their infrastructure and teaches you techniques to integrate security directly into your product. You'll also learn the core concepts of DevOps, such as continuous integration, continuous delivery, and infrastructure as a service. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Technology An application running in the cloud can benefit from incredible efficiencies, but they come with unique security threats too. A DevOps team's highest priority is understanding those risks and hardening the system against them. About the Book Securing DevOps teaches you the essential techniques to secure your cloud services. Using compelling case studies, it shows you how to build security into automated testing, continuous delivery, and other core DevOps processes. This experience-rich book is filled with mission-critical strategies to protect web applications against attacks, deter fraud attempts, and make your services safer when operating at scale. You'll also learn to identify, assess, and secure the unique vulnerabilities posed by cloud deployments and automation tools commonly used in modern infrastructures. What's inside An approach to continuous security Implementing test-driven security in DevOps Security techniques for cloud services Watching for fraud and responding to incidents Security testing and risk assessment About the Reader Readers should be comfortable with Linux and standard DevOps practices like CI, CD, and unit testing. About the Author Julien Vehent is a security architect and DevOps advocate. He leads the Firefox Operations Security team at Mozilla, and is responsible for the security of Firefox's high-traffic cloud services and public websites. Table of Contents Securing DevOps PART 1 - Case study: applying layers of security to a simple DevOps pipeline Building a barebones DevOps pipeline Security layer 1: protecting web applications Security layer 2: protecting cloud infrastructures Security layer 3: securing communications Security layer 4: securing the delivery pipeline PART 2 - Watching for anomalies and protecting services against attacks Collecting and storing logs Analyzing logs for fraud and attacks Detecting intrusions The Caribbean breach: a case study in incident response PART 3 - Maturing DevOps security Assessing risks Testing security Continuous security

microservices security in action pdf: *Mastering Microservices with Java 9* Sourabh Sharma, 2017-12-07 Master the art of implementing scalable microservices in your production environment with ease About This Book Use domain-driven design to build microservices Use Spring Cloud to use Service Discovery and Registeration Use Kafka, Avro and Spring Streams for implementing event based microservices Who This Book Is For This book is for Java developers who are familiar with the microservices architecture and now wants to take a deeper dive into effectively implementing microservices at an enterprise level. A reasonable knowledge level and understanding of core microservice elements and applications is expected. What You Will Learn Use domain-driven design to design and implement microservices Secure microservices using Spring Security Learn to develop REST service development Deploy and test microservices Troubleshoot and debug the issues faced

during development Learning best practices and common principals about microservices In Detail Microservices are the next big thing in designing scalable, easy-to-maintain applications. It not only makes app development easier, but also offers great flexibility to utilize various resources optimally. If you want to build an enterprise-ready implementation of the microservices architecture, then this is the book for you! Starting off by understanding the core concepts and framework, you will then focus on the high-level design of large software projects. You will gradually move on to setting up the development environment and configuring it before implementing continuous integration to deploy your microservice architecture. Using Spring security, you will secure microservices and test them effectively using REST Java clients and other tools like RxJava 2.0. We'll show you the best patterns, practices and common principals of microservice design and you'll learn to troubleshoot and debug the issues faced during development. We'll show you how to design and implement reactive microservices. Finally, we'll show you how to migrate a monolithic application to microservices based application. By the end of the book, you will know how to build smaller, lighter, and faster services that can be implemented easily in a production environment. Style and approach This book starts from the basics, including environment setup and provides easy-to-follow steps to implement the sample project using microservices.

microservices security in action pdf: Testing Java Microservices Jason Porter, Alex Soto, Andrew Gumbrecht, 2018-08-03 Summary Testing Java Microservices teaches you to implement unit and integration tests for microservice systems running on the JVM. You'll work with a microservice environment built using Java EE, WildFly Swarm, and Docker. You'll learn how to increase your test coverage and productivity, and gain confidence that your system will work as you expect. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Technology Microservice applications present special testing challenges. Even simple services need to handle unpredictable loads, and distributed message-based designs pose unique security and performance concerns. These challenges increase when you throw in asynchronous communication and containers. About the Book Testing Java Microservices teaches you to implement unit and integration tests for microservice systems running on the JVM. You'll work with a microservice environment built using Java EE, WildFly Swarm, and Docker. You'll advance from writing simple unit tests for individual services to more-advanced practices like chaos or integration tests. As you move towards a continuous-delivery pipeline, you'll also master live system testing using technologies like the Arquillian, Wiremock, and Mockito frameworks, along with techniques like contract testing and over-the-wire service virtualization. Master these microservice-specific practices and tools and you'll greatly increase your test coverage and productivity, and gain confidence that your system will work as you expect. What's Inside Test automation Integration testing microservice systems Testing container-centric systems Service virtualization About the Reader Written for Java developers familiar with Java EE, EE4J, Spring, or Spring Boot. About the Authors Alex Soto Bueno and Jason Porter are Arquillian team members. Andy Gumbrecht is an Apache TomEE developer and PMC. They all have extensive enterprise-testing experience. Table of Contents An introduction to microservices Application under test Unit-testing microservices Component-testing microservices Integration-testing microservices Contract tests End-to-end testing Docker and testing Service virtualization Continuous delivery in microservices

microservices security in action pdf: *Apache Pulsar in Action* David Kjerrumgaard, 2021-12-14 Distributed applications demand reliable, high-performance messaging. The Apache Pulsar server-to-server messaging system provides a secure, stable platform without the need for a stream processing engine like Spark. Contributed by Yahoo to the Apache Foundation, Pulsar is mature and battle-tested, handling millions of messages per second for over three years at Yahoo. Apache Pulsar in Action is a comprehensive and practical guide to building high-traffic applications with Pulsar, delivering extreme levels of speed and durability. about the technology Pulsar is a streaming messaging system designed for high performance server-to-server messaging. Built and tested under intense conditions at Yahoo, Pulsar has been proven in production and can handle millions of messages per second. Now free and open-source, Pulsar''s unique architecture helps

solve some of the challenges of modern development. Pulsar avoids latency in streaming data transmission, making it a powerful tool for IoT Edge analytics. Its unified messaging model improves the performance of microservices architecture, and its tiered storage capabilities allow for larger volumes of data to be handled without fear of data loss. Pulsar''s flexible API interface works with Java, C++, Python, and Go, making it easy to incorporate Pulsar into your stack. about the book Apache Pulsar in Action is a hands-on guide to building scalable streaming messaging systems for distributed applications and microservices systems. You''ll start with Pulsar''s fundamentals, each illustrated by real-world examples, as you get to grips with Pulsar''s unique architecture. Pulsar contributor David Kjerrumgaard teaches the skills you need to deploy a Pulsar server, ingest data from third-party systems, and deploy lightweight computing logic with simple functions. You''ll learn to employ Pulsar''s seamless scalability through relatable case studies, including an IOT analytics application that can be deployed within a resource constrained environment and a microservices application based on Pulsar functions. At the end of this practical book, you''ll be ready to fully take advantage of Pulsar to create high-traffic message-driven applications. what''s inside Publish from Apache Pulsar into third-party data repositories and platforms Design and develop Apache Pulsar functions Perform interactive SQL queries against data stored in Apache Pulsar Examples of Pulsar-based microservices that you can download and try yourself about the reader Written for experienced Java developers. No prior knowledge of Pulsar is needed. about the author David Kjerrumgaard is the Director of Solution Architecture at Streamlio, and a contributor to the Apache Pulsar and Apache NiFi projects.

microservices security in action pdf: *Building Microservices with .NET Core 2.0* Gaurav Aroraa, 2017-12-22 Architect your .NET applications by breaking them into really small pieces - microservices -using this practical, example-based guide. Key Features Start your microservices journey and get a broader perspective on microservices development using C# 7.0 with .NET Core 2.0 Build, deploy, and test microservices using ASP.Net Core, ASP.NET Core API, and Microsoft Azure Cloud Get the basics of reactive microservices Book Description The microservices architectural style promotes the development of complex applications as a suite of small services based on business capabilities. This book will help you identify the appropriate service boundaries within your business. We'll start by looking at what microservices are and their main characteristics. Moving forward, you will be introduced to real-life application scenarios; after assessing the current issues, we will begin the journey of transforming this application by splitting it into a suite of microservices using C# 7.0 with .NET Core 2.0. You will identify service boundaries, split the application into multiple microservices, and define service contracts. You will find out how to configure, deploy, and monitor microservices, and configure scaling to allow the application to quickly adapt to increased demand in the future. With an introduction to reactive microservices, you’ll strategically gain further value to keep your code base simple, focusing on what is more important rather than on messy asynchronous calls. What you will learn Get acquainted with Microsoft Azure Service Fabric Compare microservices with monolithic applications and SOA Learn Docker and Azure API management Define a service interface and implement APIs using ASP.NET Core 2.0 Integrate services using a synchronous approach via RESTful APIs with ASP.NET Core 2.0 Implement microservices security using Azure Active Directory, OpenID Connect, and OAuth 2.0 Understand the operation and scaling of microservices in .NET Core 2.0 Understand the key features of reactive microservices and implement them using reactive extensions Who this book is for This book is for .NET Core developers who want to learn and understand the microservices architecture and implement it in their .NET Core applications. It’s ideal for developers who are completely new to microservices or just have a theoretical understanding of this architectural approach and want to gain a practical perspective in order to better manage application complexities.

microservices security in action pdf: *Building Microservices Applications on Microsoft Azure* Harsh Chawla, Hemant Kathuria, 2019-07-17 Implement microservices starting with their architecture and moving on to their deployment, manageability, security, and monitoring. This book

focuses on the key scenarios where microservices architecture is preferred over a monolithic architecture. Building Microservices Applications on Microsoft Azure begins with a survey of microservices architecture compared to monolithic architecture and covers microservices implementation in detail. You'll see the key scenarios where microservices architecture is preferred over a monolithic approach. From there, you will explore the critical components and various deployment options of microservices on platforms such as Microsoft Azure (public cloud) and Azure Stack (hybrid cloud). This includes in-depth coverage of developing, deploying, and monitoring microservices on containers and orchestrating with Azure Service Fabric and Azure Kubernetes Cluster (AKS). This book includes practical experience from large-scale enterprise deployments, therefore it can be a quick reference for solution architects and developers to understand the critical factors while designing a microservices application. What You Will LearnExplore the use cases of microservices and monolithic architecture Discover the architecture patterns to build scalable, agile, and secure microservices applicationsDevelop and deploy microservices using Azure Service Fabric and Azure Kubernetes Service Secure microservices using the gateway patternSee the deployment options for Microservices on Azure StackImplement database patterns to handle the complexities introduced by microservices Who This Book Is For Architects and consultants who work on Microsoft Azure and manage large-scale deployments.

microservices security in action pdf: Micro Frontends in Action Michael Geers, 2020-10-13 Micro Frontends in Action teaches you to apply the microservices approach to the frontend. Summary Browser-based software can quickly become complex and difficult to maintain, especially when it’s implemented as a large single-page application. By adopting the micro frontends approach and designing your web apps as systems of features, you can deliver faster feature development, easier upgrades, and pick and choose the technology you use in your stack. Micro Frontends in Action is your guide to simplifying unwieldy frontends by composing them from small, well-defined units. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Technology Micro frontends deliver the same flexibility and maintainability to browser-based applications that microservices provide for backend systems. You design your project as a set of standalone components that include their own interfaces, logic, and storage. Then you develop these mini-applications independently and compose them in the browser. About the Book Micro Frontends in Action teaches you to apply the microservices approach to the frontend. You’ll start with the core micro frontend design ideas. Then, you’ll build an e-commerce application, working through practical issues like server-side and client-side composition, routing, and maintaining a consistent look and feel. Finally, you’ll explore team workflow patterns that maximize the benefit of developing application components independently. What’s Inside - Create a unified frontend from independent applications - Combine JavaScript code from multiple frameworks - Browser and server-side composition and routing - Implement effective dev teams and project workflow About the Reader For web developers, software architects, and team leaders. About the Author Michael Geers is a software developer specializing in building user interfaces. Table of Contents PART 1 - GETTING STARTED WITH MICRO FRONTENDS 1 What are micro frontends? 2 My first micro frontends project PART 2 - ROUTING, COMPOSITION, AND COMMUNICATION 3 Composition with Ajax and server-side routing 4 Server-side composition 5 Client-side composition 6 Communication patterns 7 Client-side routing and the application shell 8 Composition and universal rendering 9 Which architecture fits my project? PART 3 - HOW TO BE FAST, CONSISTENT, AND EFFECTIVE 10 Asset loading 11 Performance is key 12 User interface and design system 13 Teams and boundaries 14 Migration, local development, and testing

microservices security in action pdf: *Microservices Best Practices for Java* Michael Hofmann, Erin Schnabel, Katherine Stanley, IBM Redbooks, 2017-03-13 Microservices is an architectural style in which large, complex software applications are composed of one or more smaller services. Each of these microservices focuses on completing one task that represents a small business capability. These microservices can be developed in any programming language. This IBM® Redbooks® publication covers Microservices best practices for Java. It focuses on creating cloud native

applications using the latest version of IBM WebSphere® Application Server Liberty, IBM Bluemix® and other Open Source Frameworks in the Microservices ecosystem to highlight Microservices best practices for Java.

microservices security in action pdf: The Tao of Microservices Richard Rodger, 2017-12-11 Summary The Tao of Microservices guides you on the path to understanding how to apply microservice architectures to your own real-world projects. This high-level book offers a conceptual view of microservice design, along with core concepts and their application. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Technology An application, even a complex one, can be designed as a system of independent components, each of which handles a single responsibility. Individual microservices are easy for small teams without extensive knowledge of the entire system design to build and maintain. Microservice applications rely on modern patterns like asynchronous, message-based communication, and they can be optimized to work well in cloud and container-centric environments. About the Book The Tao of Microservices guides you on the path to understanding and building microservices. Based on the invaluable experience of microservices guru Richard Rodger, this book exposes the thinking behind microservice designs. You'll master individual concepts like asynchronous messaging, service APIs, and encapsulation as you learn to apply microservices architecture to real-world projects. Along the way, you'll dig deep into detailed case studies with source code and documentation and explore best practices for team development, planning for change, and tool choice. What's Inside Principles of the microservice architecture Breaking down real-world case studies Implementing large-scale systems When not to use microservices About the Reader This book is for developers and architects. Examples use JavaScript and Node.js. About the Author Richard Rodger, CEO of voxgig, a social network for the events industry, has many years of experience building microservice-based systems for major global companies. Table of Contents PART 1 - BUILDING MICROSERVICES Brave new world Services Messages Data Deployment PART 2 - RUNNING MICROSERVICES Measurement Migration People Case study: Nodezoo.com

microservices security in action pdf: *Application Security Program Handbook* Derek Fisher, 2023-02-28 Stop dangerous threats and secure your vulnerabilities without slowing down delivery. This practical book is a one-stop guide to implementing a robust application security program. In the Application Security Program Handbook you will learn: Why application security is so important to modern software Application security tools you can use throughout the development lifecycle Creating threat models Rating discovered risks Gap analysis on security tools Mitigating web application vulnerabilities Creating a DevSecOps pipeline Application security as a service model Reporting structures that highlight the value of application security Creating a software security ecosystem that benefits development Setting up your program for continuous improvement The Application Security Program Handbook teaches you to implement a robust program of security throughout your development process. It goes well beyond the basics, detailing flexible security fundamentals that can adapt and evolve to new and emerging threats. Its service-oriented approach is perfectly suited to the fast pace of modern development. Your team will quickly switch from viewing security as a chore to an essential part of their daily work. Follow the expert advice in this guide and you'll reliably deliver software that is free from security defects and critical vulnerabilities. About the technology Application security is much more than a protective layer bolted onto your code. Real security requires coordinating practices, people, tools, technology, and processes throughout the life cycle of a software product. This book provides a reproducible, step-by-step road map to building a successful application security program. About the book The Application Security Program Handbook delivers effective guidance on establishing and maturing a comprehensive software security plan. In it, you'll master techniques for assessing your current application security, determining whether vendor tools are delivering what you need, and modeling risks and threats. As you go, you'll learn both how to secure a software application end to end and also how to build a rock-solid process to keep it safe. What's inside Application security tools for the

whole development life cycle Finding and fixing web application vulnerabilities Creating a DevSecOps pipeline Setting up your security program for continuous improvement About the reader For software developers, architects, team leaders, and project managers. About the author Derek Fisher has been working in application security for over a decade, where he has seen numerous security successes and failures firsthand. Table of Contents PART 1 DEFINING APPLICATION SECURITY 1 Why do we need application security? 2 Defining the problem 3 Components of application security PART 2 DEVELOPING THE APPLICATION SECURITY PROGRAM 4 Releasing secure code 5 Security belongs to everyone 6 Application security as a service PART 3 DELIVER AND MEASURE 7 Building a roadmap 8 Measuring success 9 Continuously improving the program

microservices security in action pdf: Docker and Kubernetes for Java Developers Jaroslaw Krochmalski, 2017-08-30 Leverage the lethal combination of Docker and Kubernetes to automate deployment and management of Java applications About This Book Master using Docker and Kubernetes to build, deploy and manage Java applications in a jiff Learn how to create your own Docker image and customize your own cluster using Kubernetes Empower the journey from development to production using this practical guide. Who This Book Is For The book is aimed at Java developers who are eager to build, deploy, and manage applications very quickly using container technology. They need have no knowledge of Docker and Kubernetes. What You Will Learn Package Java applications into Docker images Understand the running of containers locally Explore development and deployment options with Docker Integrate Docker into Maven builds Manage and monitor Java applications running on Kubernetes clusters Create Continuous Delivery pipelines for Java applications deployed to Kubernetes In Detail Imagine creating and testing Java EE applications on Apache Tomcat Server or Wildfly Application server in minutes along with deploying and managing Java applications swiftly. Sounds too good to be true? But you have a reason to cheer as such scenarios are only possible by leveraging Docker and Kubernetes. This book will start by introducing Docker and delve deep into its networking and persistent storage concepts. You will then proceed to learn how to refactor monolith application into separate services by building an application and then packaging it into Docker containers. Next, you will create an image containing Java Enterprise Application and later run it using Docker. Moving on, the book will focus on Kubernetes and its features and you will learn to deploy a Java application to Kubernetes using Maven and monitor a Java application in production. By the end of the book, you will get hands-on with some more advanced topics to further extend your knowledge about Docker and Kubernetes. Style and approach An easy-to-follow, practical guide that will help Java developers develop, deploy, and manage Java applications efficiently.

Back to Home: https://new.teachat.com