Oauth 2 Simplified Aaron Parecki

Recognizing the exaggeration ways to acquire this ebook **Oauth 2 Simplified Aaron Parecki** is additionally useful. You have remained in right site to begin getting this info. get the Oauth 2 Simplified Aaron Parecki associate that we offer here and check out the link.

You could purchase lead Oauth 2 Simplified Aaron Parecki or acquire it as soon as feasible. You could speedily download this Oauth 2 Simplified Aaron Parecki after getting deal. So, similar to you require the ebook swiftly, you can straight get it. Its thus definitely simple and in view of that fats, isnt it? You have to favor to in this space

OAuth 2.0 Cookbook - Adolfo Eloy Nascimento 2017-10-18
Efficiently integrate OAuth 2.0 to protect your mobile, desktop, Cloud applications and APIs using Spring Security technologies. About This Book Interact with public OAuth 2.0 protected APIs such as Facebook, LinkedIn and Google. Use Spring Security and Spring Security OAuth2 to implement your own OAuth 2.0 provider Learn how to implement OAuth 2.0 native mobile clients for Android applications Who This Book Is For This book targets software engineers and security experts who are looking to develop their skills in API security and OAuth 2.0. Prior programming knowledge and a basic understanding of developing web applications are necessary. As this book's recipes mostly use Spring Security and Spring Security OAuth2, some prior experience with Spring Framework will be helpful. What You Will Learn Use Redis and relational databases to store issued access tokens and refresh tokens Access resources protected by the OAuth2 Provider using Spring Security Implement a web application that dynamically registers itself to the Authorization Server Improve the safety of your mobile client using dynamic client registration Protect your Android client with Proof Key for Code Exchange Protect the Authorization Server from COMPUTERS / Cloud Computing redirection In Detail OAuth 2.0 is a standard protocol for authorization and focuses on client development simplicity while providing specific authorization flows for web applications, desktop applications, mobile phones, and so on. This book also provides useful recipes for solving real-life problems using Spring Security and creating Android applications. The book starts by presenting you how to interact with some public OAuth 2.0 protected APIs such as Facebook, LinkedIn and Google. You will also be able to implement your own OAuth 2.0 provider with Spring Security OAuth2. Next, the book will cover practical scenarios regarding some important OAuth 2.0 profiles such as Dynamic Client Registration, Token Introspection and how to revoke issued access tokens. You will then be introduced to the usage of JWT, OpenID Connect, and how to safely implement native mobile OAuth 2.0 Clients. By the end of this book, you will be able to ensure that both the server and client are protected against common vulnerabilities. Style and approach With the help of real-world examples, this book provides step by step recipes for troubleshooting and extending your API security. The book also helps you with accessing and securing data on mobile, desktop, and cloud apps with OAuth 2.0.
Bulletproof Ajax - Jeremy Keith 2003-02-27
Step-by-step guide reveals best practices for enhancing Web sites with Ajax A step-by-step guide to enhancing Web sites with Ajax. Uses progressive enhancement techniques to ensure graceful degradation (which makes sites usable in all browsers). Shows readers how to write their own Ajax scripts instead of relying on third-party libraries. Web site designers love the idea of Ajax--of creating Web pages in which information can be updated without refreshing the entire page. But for those who aren't hard-core programmers, enhancing pages using Ajax can be a challenge. Even more of a challenge is making sure those pages work for all users. In Bulletproof Ajax, author Jeremy Keith

demonstrates how developers comfortable with CSS and (X)HTML can build Ajax functionality without frameworks, using the ideas of graceful degradation and progressive enhancement to ensure that the pages work for all users. Throughout this step-by-step guide, his emphasis is on best practices with an approach to building Ajax pages called Hijax, which improves flexibility and avoids worst-case scenarios.

Solving Identity and Access Management in Modern Applications - Yvonne Wilson 2020-03-02

Know how to design and use identity management to protect your application and the data it manages. At a time when security breaches result in increasingly onerous penalties, it is paramount that application developers and owners understand identity management and the value it provides when building applications. This book takes you from account provisioning to authentication to authorization, and covers troubleshooting and common problems to avoid. The authors include predictions about why this will be even more important in the future. Application best practices with coding samples are provided. Solving Identity and Access Management in Modern Applications gives you what you need to design identity and access management for your applications and to describe it to stakeholders with confidence. You will be able to explain account creation, session and access management, account termination, and more. What You'll Learn Understand key identity management concepts Incorporate essential design principles Design authentication and access control for a modern application Know the identity management frameworks and protocols used today (OIDC/ OAuth 2.0, SAML 2.0) Review historical failures and know how to avoid them Who This Book Is For Developers, enterprise or application architects, business application or product owners, and anyone involved in an application's identity management solution

Eat Healthy, Be Active Community Workshops: Based on the Dietary Guidelines for Americans 2010 and 2008 Physical Activity Guidelines for Americans - Health and Human Services Dept (U S) 2012-11

NOTE: NO FURTHER DISCOUNT FOR THIS PRINT PRODUCT --OVERSTOCK SALE-- Significantly reduced list price Six one-hour workshops were developed, based on the Dietary Guidelines for Americans, 2010 and 2008 Physical Activity Guidelines for Americans. Each workshop includes a lesson plan, learning objectives, talking points, hands-on activities, videos, and handouts. The workshops are designed for community educators, health promoters, dietitians/nutritionists, cooperative extension agents, and others to teach to adults in a wide variety of community settings. Other related products El Camino Hacia una Vida Saludable Basada en las Guias Alimenticias para los Estadounidenses = The Road to a Healthy Life Based on the Dietary Guidelines for Americans (Bilingual Spanish and English) can be found here: https: //bookstore.gpo.gov/products/sku/017-001-00564 -9 Healthy People 2010, Midcourse Review can be found here: https: //bookstore.gpo.gov/products/sku/017-001-00563 -1 Dietary Guidelines for Americans, 2010 can be found here: https: //bookstore.gpo.gov/products/sku/001-000-04747 -7 Living a Balanced Life With Diabetes: A Toolkit Addressing Psychosocial Issues for American Indian and Alaska Native Populations (Kit) can be found here: https: //bookstore.gpo.gov/products/sku/017-023-00226 -1

Microservices: Up and Running - Ronnie Mitra 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

Security for Web Developers - John Paul Mueller 2015-11-10

As a web developer, you may not want to spend time making your web app secure, but it definitely comes with the territory. This practical guide provides you with the latest information on how to thwart security threats at several levels, including new areas such as microservices. You'll learn how to help protect your app no matter where it runs, from the latest smartphone to an older desktop, and everything in between. Author John Paul Mueller delivers specific advice as well as several security programming examples for developers with a good knowledge of CSS3, HTML5, and JavaScript. In five separate sections, this book shows you how to protect against viruses, DDoS attacks, security breaches, and other nasty intrusions. Create a security plan for your organization that takes the latest devices and user needs into account Develop secure interfaces, and safely incorporate third-party code from libraries, APIs, and microservices Use sandboxing techniques, in-house and third-party testing techniques, and learn to think like a hacker Implement a maintenance cycle by determining when and how to update your application software Learn techniques for efficiently tracking security threats as well as training requirements that your organization can use

97 Things Every Java Programmer Should Know - Kevlin Henney 2020-05-15

If you want to push your Java skills to the next level, this book provides expert advice from Java leaders and practitioners. You'll be encouraged to look at problems in new ways, take broader responsibility for your work, stretch yourself by learning new techniques, and become as good at the entire craft of development as you possibly can. Edited by Kevlin Henney and Trisha Gee, 97 Things Every Java Programmer Should Know reflects lifetimes of experience writing Java software and living with the process of software development. Great programmers share their collected wisdom to help you rethink Java practices, whether working with legacy code or incorporating changes since Java 8. A few of the 97 things you should know: "Behavior Is Easy, State Is Hard"—Edson Yanaga "Learn Java Idioms and Cache in Your Brain"—Jeanne Boyarsky "Java Programming from a JVM Performance Perspective"—Monica Beckwith "Garbage Collection Is Your Friend"—Holly K Cummins "Java's Unspeakable Types"—Ben Evans "The Rebirth of Java"—Sander Mak "Do You Know What Time It Is?"—Christin Gorman

OpenID Connect in Action - Prabath Siriwardena 2022-05-31

An example-driven guide to securing access to your applications with OpenID Connect, the OAuth-based identity layer that keeps billions of user interactions safe every day. Login security is a complex problem with a simple solution: OpenID Connect. OpenID Connect in Action takes you under the hood of this reliable identity layer, showing you how to integrate OpenID Connect into a server-side web application, a single-page application (SPA), a native mobile application, APIs, and more. OpenID Connect in Action teaches you to deploy OpenID Connect to secure access to your apps. Ten-year access management veteran Prabath Siriwardena takes you in-depth with the widely adopted technology, showing you how to optimize OpenID Connect for your application's specific use cases. You'll work to secure end-to-end example applications created with React and React Native, and even develop solutions for Smart TVs and APIs. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications.

Scripted GUI Testing with Ruby - Ian Dees 2008

Scripted GUI Testing with Ruby is a practical, quick-moving tutorial based on real life, and real-world GUI applications. Right out of the gate you'll start working with code to drive a desktop GUI. You'll discover the kinds of gotchas and edge cases that don't exist in simple, toy

programs. As you add more tests, you'll learn how to organize your test code and write lucid examples. The result is a series of "smoke tests" team will run on Continuous Integration servers. Next, we'll explore a variety of different testing tips and tricks. You'll employ a series of increasingly random and punishing test monkeys to try to crash programs. Table-driven techniques will show you how to check dozens of different input combinations. See how to use longer acceptance tests (in the form of stories) to represent the way a typical customer would use your program. The book uses examples from Windows, OS X, and cross-platform Java desktop programs as well as Web applications. You'll develop test scripts in Ruby; you don't need to be a Ruby expert, but basic comfort with the language will be helpful.

Keycloak - Identity and Access Management for Modern Applications - Stian Thorgersen 2021-06-11

Learn to leverage the advanced capabilities of Keycloak, an open-source identity and access management solution, to enable authentication and authorization in applications Key FeaturesGet up to speed with Keycloak, OAuth 2.0, and OpenID Connect using practical examplesConfigure, manage, and extend Keycloak for optimized securityLeverage Keycloak features to secure different application typesBook Description Implementing authentication and authorization for applications can be a daunting experience, often leaving them exposed to security vulnerabilities. Keycloak is an open-source solution for identity management and access management for modern applications, which can make a world of difference if you learn how to use it. Keycloak, helping you get started with using it and securing your applications. Complete with hands-on tutorials, best practices, and self-assessment questions, this easy-to-follow guide will show you how to secure a sample application and then move on to securing different application types. As you progress, you will understand how to configure and manage Keycloak as well as how to leverage some of its more advanced capabilities. Finally, you'll gain insights into securely using Keycloak in production. By the end of this book, you will have learned how to install and manage Keycloak as well as how to secure new and existing applications. What you will learnUnderstand how to install, configure, and manage KeycloakSecure your new and existing applications with KeycloakGain a basic understanding of OAuth 2.0 and OpenID ConnectUnderstand how to configure Keycloak to make it ready for production useDiscover how to leverage additional features and how to customize Keycloak to fit your needsGet to grips with securing Keycloak servers and protecting applicationsWho this book is for Developers, sysadmins, security engineers, or anyone who wants to leverage Keycloak and its capabilities for application security will find this book useful. Beginner-level knowledge of app development and authentication and authorization is expected.

Ecotrain Green Career Guide - 2009-09

Ecotrain Green Career Guide#13;#13;#13;#13;Ecotrain Media Group presents the most comprehensive green career and business guide in the world. Co-founder provides 17 years of personal interest in ?sustainability,? and green research into a green career resource with over 125 pages of useful information, directories, and green industry contacts. Our guide will save you thousands of hours of personal research, time and money allowing you to spend your time landing that green job, green career, or green project first. Ecotrain Green Career Guide is for Individuals, Educators, Business, and Entrepreneurs.#13;#13;#13;#13;Ecotrain Green Career Guide provides 3 sections vital to your success no matter who, what, when, how, and where you are at in your transition to a GREEN future.#13;#13;#13;#13;Green Industry and Employment Breakdowns pp. 6-65#13;#13;This comprehensive section will step you through a non biased approach and summary background to the growing cleantech economy, and five industry sectors: the 1) Green Economy as a whole, 2) Renewable Energy, 3) Green Building

OAuth 2.0 Simplified: A Guide to Building OAuth 2.0 Servers - Aaron Parecki 2018-05-16

The OAuth 2.0 authorization framework has become the industry standard in providing secure access to web APIs. It allows users to grant external applications access to their data,

such as profile data, photos, and email, without compromising security. OAuth 2.0 Simplified is a guide to building an OAuth 2.0 server. Through high-level overviews, step-by-step instructions, and real-world examples, you will learn how to take advantage of the OAuth 2.0 framework while building a secure API.

React and Libraries - Elad Elrom 2021-03-26

Harness the power of React and the related libraries that you need to know to deliver successful front-end implementations. Whether you are a beginner getting started or an existing React developer, this book will provide you with the must-have knowledge you need in your toolbox to build a complete app. Start by learning how to create and style your own components, add state management, and manage routing. You'll also learn how to work with the backend using the MERN stack (MongoDB, Express, React, and Node.js). Once you have completed building your app you will learn how to deliver quality software by conducting unit testing, integration testing, and end-to-end (E2E) testing, as well as learn techniques to debug, profile, and optimize your React app. Libraries and tools covered include TypeScript, Material-UI, Styled Components, SCSS, React Router, Redux Toolkit, Recoil, Jest, Enzyme, Sinon, MongoDB, NodeJS, Express, Serve, Grunt, Puppeteer, ESLint, Prettier and many others. And, you'll get access to bonus material and learn how to conduct and nail React interview questions. Each chapter in this book can be used independently so you can pick and choose the information you'd like to learn. Use it to get deep into your React development world and find out why React has been rated the most loved framework by front-end developers for three years in a row. What You'll Learn Review the basics of DOM, React Virtual DOM, JSX, Babel, ES5/ES6, CRA, package manager, Yarn, Webpack, and build tools Write your own custom React components and learn about hooks and props. Apply routing and state management with React Route, Recoil, and Redux Toolkit Deliver quality software and reduce QA load by learning unit testing integration testing and end-to-end testing with libraries such as Jest, Jest-dom, Enzyme, Sinon, and Puppeteer Set an ultimate React automated development and CI cycle with ESLint, Prettier, Husky, Jest, Puppeteer, GitHub Actions, Codecov.io, Coveralls, Travis, and DeepScan Publish your code on Ubuntu Server with the help of Grunt Optimize your React app with pure components, lazy loading, prerender, precache, code splitting, tree shaking, reduce media size, and prefetching Who This Book Is For? This book is for new developers looking to start working on React applications, and React developers looking to expand on their existing knowledge. It is also suitable for developers coming from other front-end frameworks such as Angular and Vue who would like to add React to their toolbox.

The Once-Only Principle - Robert Krimmer 2021-07-02

This open access State-of-the-Art Survey describes and documents the developments and results of the Once-Only Principle Project (TOOP). The Once-Only Principle (OOP) is part of the seven underlying principles of the eGovernment Action Plan 2016-2020. It aims to make the government more effective and to reduce administrative burdens by asking citizens and companies to provide certain standard information to the public authorities only once. The project was horizontal and policy-driven with the aim of showing that the implementation of OOP in a cross-border and cross-sector setting is feasible. The book summarizes the results of the project from policy, organizational, architectural, and technical points of view.

Security and Usability - Lorrie Faith Cranor 2005-08-25

Human factors and usability issues have traditionally played a limited role in security research and secure systems development. Security experts have largely ignored usability issues--both because they often failed to recognize the importance of human factors and because they lacked the expertise to address them. But there is a growing recognition that today's security problems can be solved only by addressing issues of usability and human factors. Increasingly, well-publicized security breaches are attributed to human errors that might have been prevented through more usable software. Indeed, the world's future cyber-security depends upon the deployment of security technology that can be broadly used by untrained computer users. Still, many people believe there is an inherent tradeoff between

computer security and usability. It's true that a computer without passwords is usable, but not very secure. A computer that makes you authenticate every five minutes with a password and a fresh drop of blood might be very secure, but nobody would use it. Clearly, people need computers, and if they can't use one that's secure, they'll use one that isn't. Unfortunately, unsecured systems aren't usable for long, either. They get hacked, compromised, and otherwise rendered useless. There is increasing agreement that we need to design secure systems that people can actually use, but less agreement about how to reach this goal. Security & Usability is the first book-length work describing the current state of the art in this emerging field. Edited by security experts Dr. Lorrie Faith Cranor and Dr. Simson Garfinkel, and authored by cutting-edge security and human-computerinteraction (HCI) researchers world-wide, this volume is expected to become both a classic reference and an inspiration for future research. Security & Usability groups 34 essays into six parts: Realigning Usability and Security---with careful attention to user-centered design principles, security and usability can be synergistic. Authentication Mechanisms--techniques for identifying and authenticating computer users. Secure Systems--how system software can deliver or destroy a secure user experience. Privacy and Anonymity Systems--methods for allowing people to control the release of personal information. Commercializing Usability: The Vendor Perspective--specific experiences of security and software vendors (e.g.,IBM, Microsoft, Lotus, Firefox, and Zone Labs) in addressing usability. The Classics--groundbreaking papers that sparked the field of security and usability. This book is expected to start an avalanche of discussion, new ideas, and further advances in this important field.

Oauth 2.0 Servers - Aaron Parecki 2016

Mastering OAuth 2.0 - Charles Bihis 2015-12-15

Create powerful applications to interact with popular service providers such as Facebook, Google, Twitter, and more by leveraging the OAuth 2.0 Authorization Framework About This Book Learn how to use the OAuth 2.0 protocol to interact with the world's most popular service providers, such as Facebook, Google, Instagram, Slack, Box, and more Master the finer details of this complex protocol to maximize the potential of your application while maintaining the utmost of security Step through the construction of a real-world working application that logs you in with your Facebook account to create a compelling infographic about the most important person in the world—you! Who This Book Is For If you are an application developer, software architect, security engineer, or even a casual programmer looking to leverage the power of OAuth, Mastering OAuth 2.0 is for you. Covering basic topics such as registering your application and choosing an appropriate workflow, to advanced topics such as security considerations and extensions to the specification, this book has something for everyone. A basic knowledge of programming and OAuth is recommended. What You Will Learn Discover the power and prevalence of OAuth 2.0 and use it to improve your application's capabilities Step through the process of creating a real-world application that interacts with Facebook using OAuth 2.0 Examine the various workflows described by the specification, looking at what they are and when to use them Learn about the many security considerations involved with creating an application that interacts with other service providers Develop your debugging skills with dedicated pages for tooling and troubleshooting Build your own rich, powerful applications by leveraging world-class technologies from companies around the world In Detail OAuth 2.0 is a powerful authentication and authorization framework that has been adopted as a standard in the technical community. Proper use of this protocol will enable your application to interact with the world's most popular service providers, allowing you to leverage their world-class technologies in your own application. Want to log your user in to your application with their Facebook account? Want to display an interactive Google Map in your application? How about posting an update to your user's LinkedIn feed? This is all achievable through the power of OAuth. With a focus on practicality and security, this book takes a detailed and hands-on approach to explaining the protocol, highlighting important pieces of information along the way.

At the beginning, you will learn what OAuth is, how it works at a high level, and the steps involved in creating an application. After obtaining an overview of OAuth, you will move on to the second part of the book where you will learn the need for and importance of registering your application and types of supported workflows. You will discover more about the access token, how you can use it with your application, and how to refresh it after expiration. By the end of the book, you will know how to make your application architecture robust. You will explore the security considerations and effective methods to debug your applications using appropriate tools. You will also have a look at special considerations to integrate with OAuth service providers via native mobile applications. In addition, you will also come across support resources for OAuth and credentials grant. Style and approach With a focus on practicality and security, Mastering OAuth 2.0 takes a top-down approach at exploring the protocol. Discussed first at a high level, examining the importance and overall structure of the protocol, the book then dives into each subject, adding more depth as we proceed. This all culminates in an example application that will be built, step by step, using the valuable and practical knowledge you have gained.

Decoupled Django - Valentino Gagliardi 2021-07-03

Apply decoupling patterns, properly test a decoupled project, and integrate a Django API with React, and Vue.js. This book covers decoupled architectures in Django, with Django REST framework and GraphQL. With practical and simple examples, you'll see firsthand how, why, and when to decouple a Django project. Starting with an introduction to decoupled architectures versus monoliths, with a strong focus on the modern JavaScript scene, you'll implement REST and GraphQL APIs with Django, add authentication to a decoupled project, and test the backend. You'll then review functional testing for JavaScript frontends with Cypress. You will also learn how to integrate GraphQL in a Django project, with a focus on the benefits and drawbacks of this new query language. By the end of this book, you will be able to discern and apply all the different decoupling strategies to any Django project, regardless of its size. What You'll Learn Choose the right approach for decoupling a Django project Build REST APIs with Django and a Django REST framework Integrate Vue.js and GraphQL in a Django project Consume a Django REST API with Next.js Test decoupled Django projects Who This Book Is For Software developers with basic Django skills keen to learn decoupled architectures with Django. JavaScript developers interested in learning full-stack development and decoupled architectures with Django.

Modern Authentication with Azure Active Directory for Web Applications - Vittorio Bertocci 2015-12-17

Build advanced authentication solutions for any cloud or web environment Active Directory has been transformed to reflect the cloud revolution, modern protocols, and today's newest SaaS paradigms. This is an authoritative, deep-dive guide to building Active Directory authentication solutions for these new environments. Author Vittorio Bertocci drove these technologies from initial concept to general availability, playing key roles in everything from technical design to documentation. In this book, he delivers comprehensive guidance for building complete solutions. For each app type, Bertocci presents high-level scenarios and quick implementation steps, illuminates key concepts in greater depth, and helps you refine your solution to improve performance and reliability. He helps you make sense of highly abstract architectural diagrams and nitty-gritty protocol and implementation details. This is the book for people motivated to become experts. Active Directory Program Manager Vittorio Bertocci shows you how to: Address authentication challenges in the cloud or on-premises Systematically protect apps with Azure AD and AD Federation Services Power sign-in flows with OpenID Connect, Azure AD, and AD libraries Make the most of OpenID Connect's middleware and supporting classes Work with the Azure AD representation of apps and their relationships Provide fine-grained app access control via roles, groups, and permissions Consume and expose Web APIs protected by Azure AD Understand new authentication protocols without reading complex spec documents

Android Programming - Erik Hellman 2013-11-04
Unleash the power of the Android OS and build the kinds of brilliant, innovative apps users love to use If you already know your way around the Android OS and can build a simple Android app in under an hour, this book is for you. If you're itching to see just how far you can push it and discover what Android is really capable of, it's for you. And if you're ready to learn how to build advanced, intuitive, innovative apps that are a blast to use, this book is definitely for you. From custom views and advanced multi-touch gestures, to integrating online web services and exploiting the latest geofencing and activity recognition features, ace Android developer, Erik Hellman, delivers expert tips, tricks and little-known techniques for pushing the Android envelope so you can: Optimize your components for the smoothest user experience possible Create your own custom Views Push the boundaries of the Android SDK Master Android Studio and Gradle Make optimal use of the Android audio, video and graphics APIs Program in Text-To-Speech and Speech Recognition Make the most of the new Android maps and location API Use Android connectivity technologies to communicate with remote devices Perform background processing Use Android cryptography APIs Find and safely use hidden Android APIs Cloud-enable your applications with Google Play Services Distribute and sell your applications on Google Play Store Learn how to unleash the power of Android and transform your apps from good to great in Android Programming: Pushing the Limits.

Identity and Data Security for Web Development - Jonathan LeBlanc 2016-06-06
Developers, designers, engineers, and creators can no longer afford to pass responsibility for identity and data security onto others. Web developers who don't understand how to obscure data in transmission, for instance, can open security flaws on a site without realizing it. With this practical guide, you'll learn how and why everyone working on a system needs to ensure that users and data are protected. Authors Jonathan LeBlanc and Tim Messerschmidt provide a deep dive into the concepts, technology, and programming methodologies necessary to build a secure interface for data and identity—without compromising usability. You'll learn how to plug holes in existing systems, protect against viable attack vectors, and work in environments that sometimes are naturally insecure. Understand the state of web and application security today Design security password encryption, and combat password attack vectors Create digital fingerprints to identify users through browser, device, and paired device detection Build secure data transmission systems through OAuth and OpenID Connect Use alternate methods of identification for a second factor of authentication Harden your web applications against attack Create a secure data transmission system using SSL/TLS, and synchronous and asynchronous cryptography

Usable Security - Simson Garfinkel 2014-10-01
There has been roughly 15 years of research into approaches for aligning research in Human Computer Interaction with computer Security, more colloquially known as ``usable security.'' Although usability and security were once thought to be inherently antagonistic, today there is wide consensus that systems that are not usable will inevitably suffer security failures when they are deployed into the real world. Only by simultaneously addressing both usability and security concerns will we be able to build systems that are truly secure. This book presents the historical context of the work to date on usable security and privacy, creates a taxonomy for organizing that work, outlines current research objectives, presents lessons learned, and makes suggestions for future research.

Getting Started with OAuth 2.0 - Ryan Boyd 2012-02-22
Whether you develop web applications or mobile apps, the OAuth 2.0 protocol will save a lot of headaches. This concise introduction shows you how OAuth provides a single authorization technology across numerous APIs on the Web, so you can securely access users' data—such as user profiles, photos, videos, and contact lists—to improve their experience of your application. Through code examples, step-by-step instructions, and use-case examples, you'll learn how to apply OAuth 2.0 to your server-side web application, client-side app, or mobile app. Find out what it takes to access social graphs, store data in a user's online filesystem, and

perform many other tasks. Understand OAuth 2.0's role in authentication and authorization Learn how OAuth's Authorization Code flow helps you integrate data from different business applications Discover why native mobile apps use OAuth differently than mobile web apps Use OpenID Connect and eliminate the need to build your own authentication system

Human-Computer Interaction: Interaction Modalities and Techniques - Masaaki Kurosu 2013-07-01

The five-volume set LNCS 8004--8008 constitutes the refereed proceedings of the 15th International Conference on Human-Computer Interaction, HCII 2013, held in Las Vegas, NV, USA in July 2013. The total of 1666 papers and 303 posters presented at the HCII 2013 conferences was carefully reviewed and selected from 5210 submissions. These papers address the latest research and development efforts and highlight the human aspects of design and use of computing systems. The papers accepted for presentation thoroughly cover the entire field of human-computer interaction, addressing major advances in knowledge and effective use of computers in a variety of application areas. This volume contains papers in the thematic area of human-computer interaction, addressing the following major topics: speech, natural language and auditory interfaces; gesture and eye-gaze based Interaction; touch-based interaction; haptic interaction; graphical user interfaces and visualisation.

Digital Identity Management - Maryline Laurent 2015-04-02

In the past four decades, information technology has altered chains of value production, distribution, and information access at a significant rate. These changes, although they have shaken up numerous economic models, have so far not radically challenged the bases of our society. This book addresses our current progress and viewpoints on digital identity management in different fields (social networks, cloud computing, Internet of Things (IoT), with input from experts in computer science, law, economics and sociology. Within this multidisciplinary and scientific context, having crossed analysis on the digital ID issue, it describes the different technical and legal approaches to protect digital identities with a focus on authentication systems, identity federation techniques and privacy preservation solutions. The limitations of these solutions and research issues in this field are also discussed to further understand the changes that are taking place. Offers a state of the discussions and work places on the management of digital identities in various contexts, such as social networking, cloud computing and the Internet of Things Describes the advanced technical and legal measures to protect digital identities Contains a strong emphasis of authentication techniques, identity federation tools and technical protection of privacy

The Art of Scalability - Martin L. Abbott 2015-05-23

The Comprehensive, Proven Approach to IT Scalability–Updated with New Strategies, Technologies, and Case Studies In The Art of Scalability, Second Edition, leading scalability consultants Martin L. Abbott and Michael T. Fisher cover everything you need to know to smoothly scale products and services for any requirement. This extensively revised edition reflects new technologies, strategies, and lessons, as well as new case studies from the authors' pioneering consulting practice, AKF Partners. Writing for technical and nontechnical decision-makers, Abbott and Fisher cover everything that impacts scalability, including architecture, process, people, organization, and technology. Their insights and recommendations reflect more than thirty years of experience at companies ranging from eBay to Visa, and Salesforce.com to Apple. You'll find updated strategies for structuring organizations to maximize agility and scalability, as well as new insights into the cloud (IaaS/PaaS) transition, NoSQL, DevOps, business metrics, and more. Using this guide's tools and advice, you can systematically clear away obstacles to scalability–and achieve unprecedented IT and business performance. Coverage includes • Why scalability problems start with organizations and people, not technology, and what to do about it • Actionable lessons from real successes and failures • Staffing, structuring, and leading the agile, scalable organization • Scaling processes for hyper-growth environments • Architecting scalability: proprietary models for clarifying needs and making choices–including 15 key

success principles • Emerging technologies and challenges: data cost, datacenter planning, cloud evolution, and customer-aligned monitoring • Measuring availability, capacity, load, and performance

Identity and Data Security for Web Development - Jonathan LeBlanc 2016-06-06

Developers, designers, engineers, and creators can no longer afford to pass responsibility for identity and data security onto others. Web developers who don't understand how to obscure data in transmission, for instance, can open security flaws on a site without realizing it. With this practical guide, you'll learn how and why everyone working on a system needs to ensure that users and data are protected. Authors Jonathan LeBlanc and Tim Messerschmidt provide a deep dive into the concepts, technology, and programming methodologies necessary to build a secure interface for data and identity—without compromising usability. You'll learn how to plug holes in existing systems, protect against viable attack vectors, and work in environments that sometimes are naturally insecure. Understand the state of web and application security today Design security password encryption, and combat password attack vectors Create digital fingerprints to identify users through browser, device, and paired device detection Build secure data transmission systems through OAuth and OpenID Connect Use alternate methods of identification for a second factor of authentication Harden your web applications against attack Create a secure data transmission system using SSL/TLS, and synchronous and asynchronous cryptography

OAuth 2.0: The Definitive Guide - Aaron Parecki 2012-09-15

This is a definitive guide to the OAuth 2 protocol. It covers the latest version of the OAuth 2 core specification (currently the spec is at draft 21 but very little will change between now and the final version). The book will help beginners get started writing client applications to interface with a number of APIs currently using OAuth 2, and will help experts develop and improve their server-side solutions. It is for both developers and engineering managers who want to develop web services with secure APIs, and covers high level overviews as well as details on the security implications of the protocol.

Staff Engineer - Will Larson 2021-02-28

At most technology companies, you'll reach Senior Software Engineer, the career level for software engineers, in five to eight years. At that career level, you'll no longer be required to work towards the next pro? motion, and being promoted beyond it is exceptional rather than ex? pected. At that point your career path will branch, and you have to decide between remaining at your current level, continuing down the path of technical excellence to become a Staff Engineer, or switching into engineering management. Of course, the specific titles vary by company, and you can replace "Senior Engineer" and "Staff Engineer" with whatever titles your company prefers.Over the past few years we've seen a flurry of books unlocking the en? gineering management career path, like Camille Fournier's The Man? ager's Path, Julie Zhuo's The Making of a Manager, Lara Hogan's Re? silient Management and my own, An Elegant Puzzle. The manage? ment career isn't an easy one, but increasingly there are maps avail? able for navigating it.On the other hand, the transition into Staff Engineer, and its further evolutions like Principal and Distinguished Engineer, remains chal? lenging and undocumented. What are the skills you need to develop to reach Staff Engineer? Are technical abilities alone sufficient to reach and succeed in that role? How do most folks reach this role? What is your manager's role in helping you along the way? Will you enjoy being a Staff Engineer or you will toil for years to achieve a role that doesn't suit you?"Staff Engineer: Leadership beyond the management track" is a pragmatic look at attaining and operate in these Staff-plus roles.

OAuth 2 in Action - Justin Richer 2017-03-06

Summary OAuth 2 in Action teaches you the practical use and deployment of this HTTP-based protocol from the perspectives of a client, authorization server, and resource server. You'll learn how to confidently and securely build and deploy OAuth on both the client and server sides. Foreword by Ian Glazer. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Technology Think of OAuth 2 as the web version of a valet key. It is an HTTP-based

security protocol that allows users of a service to enable applications to use that service on their behalf without handing over full control. And OAuth is used everywhere, from Facebook and Google, to startups and cloud services. About the Book OAuth 2 in Action teaches you practical use and deployment of OAuth 2 from the perspectives of a client, an authorization server, and a resource server. You'll begin with an overview of OAuth and its components and interactions. Next, you'll get hands-on and build an OAuth client, an authorization server, and a protected resource. Then you'll dig into tokens, dynamic client registration, and more advanced topics. By the end, you'll be able to confidently and securely build and deploy OAuth on both the client and server sides. What's Inside Covers OAuth 2 protocol and design Authorization with OAuth 2 OpenID Connect and User-Managed Access Implementation risks JOSE, introspection, revocation, and registration Protecting and accessing REST APIs About the Reader Readers need basic programming skills and knowledge of HTTP and JSON. About the Author Justin Richer is a systems architect and software engineer. Antonio Sanso is a security software engineer and a security researcher. Both authors contribute to open standards and open source. Table of Contents Part 1 - First steps What is OAuth 2.0 and why should you care? The OAuth dance Part 2 - Building an OAuth 2 environment Building a simple OAuth client Building a simple OAuth protected resource Building a simple OAuth authorization server OAuth 2.0 in the real world Part 3 - OAuth 2 implementation and vulnerabilities Common client vulnerabilities Common protected resources vulnerabilities Common authorization server vulnerabilities Common OAuth token vulnerabilities Part 4 - Taking OAuth further OAuth tokens Dynamic client registration User authentication with OAuth 2.0 Protocols and profiles using OAuth 2.0 Beyond bearer tokens Summary and conclusions

System Design Interview - An Insider's Guide - Alex Xu 2020-06-12

The system design interview is considered to be the most complex and most difficult technical job interview by many. Those questions are intimidating, but don't worry. It's just that nobody has taken the time to prepare you systematically. We take the time. We go slow. We draw lots of diagrams and use lots of examples. You'll learn step-by-step, one question at a time.Don't miss out.What's inside?- An insider's take on what interviewers really look for and why.- A 4-step framework for solving any system design interview question.- 16 real system design interview questions with detailed solutions.- 188 diagrams to visually explain how different systems work.

The FreeBSD Corporate Networker's Guide - Ted Mittelstaedt 2001

FreeBSD is the engine that runs on some of today's largest Internet servers, such as Yahoo , Microsoft's Hotmail, and Walnut Creek. The power, flexibility, and cost effectiveness of FreeBSD make it the preferred server platform of many corporate networks, including networks in which the Windows OS predominates.

POJOs in Action - Chris Richardson 2006-02-02

The standard platform for enterprise application development has been EJB but the difficulties of working with it caused it to become unpopular. They also gave rise to lightweight technologies such as Hibernate, Spring, JDO, iBATIS and others, all of which allow the developer to work directly with the simpler POJOs. Now EJB version 3 solves the problems that gave EJB 2 a black eye-it too works with POJOs. POJOs in Action describes the new, easier ways to develop enterprise Java applications. It describes how to make key design decisions when developing business logic using POJOs, including how to organize and encapsulate the business logic, access the database, manage transactions, and handle database concurrency. This book is a new-generation Java applications guide: it enables readers to successfully build lightweight applications that are easier to develop, test, and maintain.

Enterprise Application Architecture with .NET Core - Ganesan Senthilvel 2017-04-25

Architect and design highly scalable, robust, clean and highly performant applications in .NET Core About This Book Incorporate architectural soft-skills such as DevOps and Agile methodologies to enhance program-level objectives Gain knowledge of architectural approaches on the likes of SOA architecture and microservices to provide traceability and rationale for architectural decisions Explore a

variety of practical use cases and code examples to implement the tools and techniques described in the book Who This Book Is For This book is for experienced .NET developers who are aspiring to become architects of enterprise-grade applications, as well as software architects who would like to leverage .NET to create effective blueprints of applications. What You Will Learn Grasp the important aspects and best practices of application lifecycle management Leverage the popular ALM tools, application insights, and their usage to monitor performance, testability, and optimization tools in an enterprise Explore various authentication models such as social media-based authentication, 2FA and OpenID Connect, learn authorization techniques Explore Azure with various solution approaches for Microservices and Serverless architecture along with Docker containers Gain knowledge about the recent market trends and practices and how they can be achieved with .NET Core and Microsoft tools and technologies In Detail If you want to design and develop enterprise applications using .NET Core as the development framework and learn about industry-wide best practices and guidelines, then this book is for you. The book starts with a brief introduction to enterprise architecture, which will help you to understand what enterprise architecture is and what the key components are. It will then teach you about the types of patterns and the principles of software development, and explain the various aspects of distributed computing to keep your applications effective and scalable. These chapters act as a catalyst to start the practical implementation, and design and develop applications using different architectural approaches, such as layered architecture, service oriented architecture, microservices and cloud-specific solutions. Gradually, you will learn about the different approaches and models of the Security framework and explore various authentication models and authorization techniques, such as social media-based authentication and safe storage using app secrets. By the end of the book, you will get to know the concepts and usage of the emerging fields, such as DevOps, BigData, architectural practices, and Artificial Intelligence. Style and approach Filled with examples and use cases, this guide takes a no-nonsense approach to show you the best tools and techniques required to become a successful software architect.

Oauth 2.0 Simplified - Aaron Parecki 2018-06-16

The OAuth 2.0 authorization framework has become the industry standard in providing secure access to web APIs. It allows users to grant external applications access to their data, such as profile data, photos, and email, without compromising security. OAuth 2.0 Simplified is a guide to building an OAuth 2.0 server. Through high-level overviews, step-by-step instructions, and real-world examples, you will learn how to take advantage of the OAuth 2.0 framework while building a secure API.

Advanced API Security - Prabath Siriwardena 2017-10-08

This book will prepare you to meet the next wave of challenges in enterprise security, guiding you through and sharing best practices for designing APIs for rock-solid security. It will explore different security standards and protocols, helping you choose the right option for your needs. Advanced API Security, Second Edition explains in depth how to secure APIs from traditional HTTP Basic Authentication to OAuth 2.0 and the standards built around it. Keep your business thriving while keeping enemies away. Build APIs with rock-solid security. The book takes you through the best practices in designing APIs for rock-solid security, provides an in depth understanding of most widely adopted security standards for API security and teaches you how to compare and contrast different security standards/protocols to find out what suits your business needs, the best. This new edition enhances all the topics discussed in its predecessor with the latest up to date information, and provides more focus on beginners to REST, JSON, Microservices and API security. Additionally, it covers how to secure APIs for the Internet of Things (IoT). Audience: The Advanced API Security 2nd Edition is for Enterprise Security Architects and Developers who are designing, building and managing APIs. The book will provide guidelines, best practices in designing APIs and threat mitigation techniques for Enterprise Security Architects while developers would be able to gain hands-on experience by developing API clients against Facebook, Twitter, Salesforce and many other

cloud service providers. What you'll learn • Build APIs with rock-solid security by understanding best practices and design guidelines.• Compare and contrast different security standards/protocols to find out what suits your business needs, the best.• Expand business APIs to partners and outsiders with Identity Federation.• Get hands-on experience in developing clients against Facebook, Twitter, and Salesforce APIs.• Understand and learn how to secure Internet of Things.

Cybersecurity: The Beginner's Guide - Dr. Erdal Ozkaya 2019-05-27

Understand the nitty-gritty of Cybersecurity with ease Key FeaturesAlign your security knowledge with industry leading concepts and toolsAcquire required skills and certifications to survive the ever changing market needsLearn from industry experts to analyse, implement, and maintain a robust environmentBook Description It's not a secret that there is a huge talent gap in the cybersecurity industry. Everyone is talking about it including the prestigious Forbes Magazine, Tech Republic, CSO Online, DarkReading, and SC Magazine, among many others. Additionally, Fortune CEO's like Satya Nadella, McAfee's CEO Chris Young, Cisco's CIO Colin Seward along with organizations like ISSA, research firms like Gartner too shine light on it from time to time. This book put together all the possible information with regards to cybersecurity, why you should choose it, the need for cyber security and how can you be part of it and fill the cybersecurity talent gap bit by bit. Starting with the essential understanding of security and its needs, we will move to security domain changes and how artificial intelligence and machine learning are helping to secure systems. Later, this book will walk you through all the skills and tools that everyone who wants to work as security personal need to be aware of. Then, this book will teach readers how to think like an attacker and explore some advanced security methodologies. Lastly, this book will deep dive into how to build practice labs, explore real-world use cases and get acquainted with various cybersecurity certifications. By the end of this book, readers will be well-versed with the security domain and will be capable of making the right choices in the cybersecurity field. What you will learnGet an overview of what cybersecurity is and learn about the various faces of cybersecurity as well as identify domain that suits you bestPlan your transition into cybersecurity in an efficient and effective wayLearn how to build upon your existing skills and experience in order to prepare for your career in cybersecurityWho this book is for This book is targeted to any IT professional who is looking to venture in to the world cyber attacks and threats. Anyone with some understanding or IT infrastructure workflow will benefit from this book. Cybersecurity experts interested in enhancing their skill set will also find this book useful.

Implementing Oracle API Platform Cloud Service - Andrew Bell 2018-05-31

Work with the newest Oracle API Platform Cloud Service to interface with the increasingly complex array of services your clients want. Key Features Understand the architecture and functionality of the new Oracle API Cloud Service Platform Understand typical use cases for the new platform and how it can work for you Design your own APIs, then deploy and customize your APIs Implement Oauth 2.0 policy and custom policies Migrate from Oracle 12c solutions to the new Oracle API platform Book Description Implementing Oracle API Platform Cloud Service moves from theory to practice using the newest Oracle API management platform. This critical new platform for Oracle developers allows you to interface the complex array of services your clients expect in the modern world. First, you'll learn about Oracle's new platform and get an overview of it, then you'll see a use case showing the functionality and use of this new platform for Oracle customers. Next, you'll see the power of Apiary and begin designing your own APIs. From there, you'll build and run microservices and set up the Oracle API gateways. Moving on, you'll discover how to customize the developer portal and publish your own APIs. You'll spend time looking at configuration management on the new platform, and implementing the Oauth 2.0 policy, as well as custom policies. The latest finance modules from Oracle will be examined, with some of the third party alternatives in sight as well. This broad-scoped book completes your journey with a clear examination of how to transition APIs from Oracle API Management

12c to the new Oracle API Platform, so that you can step into the future confidently. What you will learn Get an overview of the Oracle API Cloud Service Platform See typical use cases of the Oracle API Cloud Service Platform Design your own APIs using Apiary Build and run microservices Set up API gateways with the new API platform from Oracle Customize developer portals Configuration management Implement Oauth 2.0 policies Implement custom policies Get a policy SDK overview Transition from Oracle API Management 12c to the new Oracle API platform Who this book is for This book is for all Oracle developers who are working or plan to work with the Oracle API Platform Cloud Service.

API Security in Action - Neil Madden 2020-11-20

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

Deploying Identity and Access Management with Free Open Source Software - Michael Schwartz 2018-06-02

Learn to leverage existing free open source software to build an identity and access management (IAM) platform that can serve your organization for the long term. With the emergence of open standards and open source software, it's now easier than ever to build and operate your own IAM stack The most common culprit of the largest hacks has been bad personal identification. In terms of bang for your buck, effective access control is the best investment you can make: financially, it's more valuable to prevent than to detect a security breach. That's why Identity and Access Management (IAM) is a critical component of an organization's security infrastructure. In the past, IAM software has been available only from large enterprise software vendors. Commercial IAM offerings are bundled as "suites" because IAM is not just one component: It's a number of components working together, including web, authentication, authorization, and cryptographic and persistence services. Deploying Identity and Access Management with Free Open Source Software documents a recipe to take advantage

of open standards to build an enterprise-class IAM service using free open source software. This recipe can be adapted to meet the needs of both small and large organizations. While not a comprehensive guide for every application, this book provides the key concepts and patterns to help administrators and developers leverage a central security infrastructure. Cloud IAM service providers would have you believe that managing an IAM is too hard. Anything unfamiliar is hard, but with the right road map, it can be mastered. You may find SaaS identity solutions too rigid or too expensive. Or perhaps you don't like the idea of a third party holding the credentials of your users—the keys to your kingdom. Open source IAM provides an alternative. Take control of your IAM infrastructure if digital services are key to your organization's success. What You'll Learn Why to deploy a centralized authentication and policy management infrastructure Use: SAML for single sign-on, OpenID Connect for web and mobile single sign-on, and OAuth2 for API Access Management Synchronize data from existing identity repositories such as Active Directory Deploy two-factor authentication services Who This Book Is For Security architects (CISO, CSO), system engineers/administrators, and software developers