1. Record Nr. UNINA9910369901303321

Autore	Siriwardena Prabath
Titolo	Advanced API Security [[electronic resource]] : OAuth 2.0 and Beyond / / by Prabath Siriwardena
Pubbl/distr/stampa	Berkeley, CA : , : Apress : , : Imprint : Apress, , 2020
ISBN	1-4842-2050-1
Edizione	[2nd ed. 2020.]
Descrizione fisica	1 online resource (xix, 449 pages) : illustrations
Collana	Books for professionals by professionals
Disciplina	005.1068
Soggetti	Data protection Special purpose computers Computer security Programming languages (Electronic computers) Security Special Purpose and Application-Based Systems Systems and Data Security Programming Languages, Compilers, Interpreters
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	1. APIs Rule!.-2. Designing Security for APIs.-3. Securing APIs with Transport Layer Security (TLS).-4. OAuth 2.0 Fundamentals.-5. Edge Security with an API Gateway.-6. OpenID Connect (OIDC).-7. Message Level Security with JSON Web Signature.-8. Message Level Security with JSON Web Encryption.-9. OAuth 2.0 Profiles.-10. Accessing APIs via Native Mobile Apps.-11. OAuth 2.0 Token Binding.-12. Federating Access to APIs.-13. User Managed Access.-14. OAuth 2.0 Security -- 15. Patterns and Practices -- 16: A. The Evolution of Identity Delegation -- 17: B. OAuth 1.0 -- 18: C. How Transport Layer Security Works -- 19: D. UMA Evolution -- 20: E. Base64URL Encoding -- 21: F. Basic/Digest Authentication -- 22: G. OAuth 2.0 MAC Token Profile.
Sommario/riassunto	Prepare for the next wave of challenges in enterprise security. Learn to better protect, monitor, and manage your public and private APIs. Enterprise APIs have become the common way of exposing business functions to the outside world. Exposing functionality is convenient, but of course comes with a risk of exploitation. This book teaches you

about TLS Token Binding, User Managed Access (UMA) 2.0, Cross Origin Resource Sharing (CORS), Incremental Authorization, Proof Key for Code Exchange (PKCE), and Token Exchange. Benefit from lessons learned from analyzing multiple attacks that have taken place by exploiting security vulnerabilities in various OAuth 2.0 implementations. Explore root causes, and improve your security practices to mitigate against similar future exploits. Security must be an integral part of any development project. This book shares best practices in designing APIs for rock-solid security. API security has evolved since the first edition of this book, and the growth of standards has been exponential. OAuth 2.0 is the most widely adopted framework that is used as the foundation for standards, and this book shows you how to apply OAuth 2.0 to your own situation in order to secure and protect your enterprise APIs from exploitation and attack. You will: Securely design, develop, and deploy enterprise APIs Pick security standards and protocols to match business needs Mitigate security exploits by understanding the OAuth 2.0 threat landscape Federate identities to expand business APIs beyond the corporate firewall Protect microservices at the edge by securing their APIs Develop native mobile applications to access APIs securely Integrate applications with SaaS APIs protected with OAuth 2.0.