1. Record Nr. UNINA9910427050303321

Autore	Norberg Scott
Titolo	Advanced ASP.NET Core 3 Security : Understanding Hacks, Attacks, and Vulnerabilities to Secure Your Website / / by Scott Norberg
Pubbl/distr/stampa	Berkeley, CA : , : Apress : , : Imprint : Apress, , 2020
ISBN	1-4842-6014-7
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (XX, 405 p. 30 illus.)
Disciplina	005.8
Soggetti	Microsoft software Microsoft .NET Framework Data protection Microsoft Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Chapter 1: Introducing ASP.NET Core -- Chapter 2: General Security Concepts -- Chapter 3: Cryptography -- Chapter 4: Web Security Concepts -- Chapter 5: Understanding Common Attacks -- Chapter 6: Processing User Input -- Chapter 7: Authentication and Authorization -- Chapter 8: Data Access and Storage. - Chapter 9: Logging and Error Handling -- Chapter 10: Setup and Configuration -- Chapter 11: Secure Application Life Cycle Management.
Sommario/riassunto	Incorporate security best practices into ASP.NET Core. This book covers security-related features available within the framework, explains where these feature may fall short, and delves into security topics rarely covered elsewhere. Get ready to dive deep into ASP.NET Core 3.1 source code, clarifying how particular features work and addressing how to fix problems. For straightforward use cases, the ASP.NET Core framework does a good job in preventing certain types of attacks from happening. But for some types of attacks, or situations that are not straightforward, there is very little guidance available on how to safely implement solutions. And worse, there is a lot of bad advice online on how to implement functionality, be it encrypting unsafely hard-coded parameters that need to be generated at runtime, or articles which

advocate for certain solutions that are vulnerable to obvious injection attacks. Even more concerning is the functions in ASP.NET Core that are not as secure as they should be by default. Advanced ASP.NET Core 3 Security is designed to train developers to avoid these problems. Unlike the vast majority of security books that are targeted to network administrators, system administrators, or managers, this book is targeted specifically to ASP.NET developers. Author Scott Norberg begins by teaching developers how ASP.NET Core works behind the scenes by going directly into the framework's source code. Then he talks about how various attacks are performed using the very tools that penetration testers would use to hack into an application. He shows developers how to prevent these attacks. Finally, he covers the concepts developers need to know to do some testing on their own, without the help of a security professional. What You Will Learn Discern which attacks are easy to prevent, and which are more challenging, in the framework Dig into ASP.NET Core 3.1 source code to understand how the security services work Establish a baseline for understanding how to design more secure software Properly apply cryptography in software development Take a deep dive into web security concepts Validate input in a way that allows legitimate traffic but blocks malicious traffic Understand parameterized queries and why they are so important to ASP.NET Core Fix issues in a well-implemented solution Know how the new logging system in ASP.NET Core falls short of security needs Incorporate security into your software development process This book is for software developers who have experience creating websites in ASP.NET and want to know how to make their websites secure from hackers and security professionals who work with a development team that uses ASP.NET Core. A basic understanding of web technologies such as HTML, JavaScript, and CSS is assumed, as is knowledge of how to create a website, and how to read and write C#. You do not need knowledge of security concepts, even those that are often covered in ASP.NET Core documentation. Scott Norberg is a web security specialist currently based in the Seattle, Washington area. He has almost 15 years of experience successfully delivering software products in a wide range of roles. As a security consultant, he has experience with many testing tools and techniques, including Dynamic (DAST) and Static (SAST) testing, as well as manual testing and reviewing source code. Along with the many websites he has designed and built with various versions of ASP.NET, he has performed security assessments for many more. While his language of choice is C#, he has also built websites, components, and other tools in F#, VB.NET, Python, R, Java, and Pascal. He holds several certifications, including Microsoft Certified Technology Specialist (MCTS), certifications for ASP.NET and SQL Server, and a Certified Information Systems Security Professional (CISSP) certification. He also has an MBA from Indiana University.