Improving Web Application Security: Threats And Countermeasures
**Synopsis**

Gain a solid foundation for designing, building, and configuring security-enhanced, hack-resistant Microsoft® ASP.NET Web applications. This expert guide describes a systematic, task-based approach to security that can be applied to both new and existing applications. It addresses security considerations at the network, host, and application layers for each physical tier—Web server, remote application server, and database server—detailing the security configurations and countermeasures that can help mitigate risks. The information is organized into sections that correspond to both the product life cycle and the roles involved, making it easy for architects, designers, and developers to find the answers they need. All PATTERNS & PRACTICES guides are reviewed and approved by Microsoft engineering teams, consultants, partners, and customers; delivering accurate, real-world information that’s been technically validated and tested.

**Book Information**

Paperback: 960 pages  
Publisher: Microsoft Press; 1 edition (September 2, 2003)  
Language: English  
ISBN-10: 0735618429  
Product Dimensions: 7.3 x 2.2 x 9.1 inches  
Shipping Weight: 4.1 pounds  
Average Customer Review: 4.5 out of 5 stars See all reviews (6 customer reviews)  

**Customer Reviews**

If you are designing, building and deploying Web based applications using Microsoft’s .NET Framework run and get this book. Currently, there is no other book that can match the breath and depth of the topic covered in this book. Contrary to what the title may imply, in addition to ASP.NET this book also covers how security should be addressed in the building of Serviced components, Web Services and Remoting. The chapters on Code Access Security are among the clearest that can be found anywhere. This book takes a holistic approach to Security in that it addresses threats
to the network, host and application layers. The old adage of a chain is only as strong as its weakest link is taken to heart in the book so guidance is provided on how security should be addressed across tiers and at multiple layers. Secure app development across the entire software development and deployment lifecycle is considered within the scope of this book. In addition to Secure Coding guidelines, Extensive guidelines are provided that show how the Network, Web Server, Application Server and Database Server should be secured. One of the things that I like about this book is that the guidance that is provided is task and role based. So even though the book is 800+ pages, it can be very easily used as a ready reference. Multiple checklists that deal with Design, Build, Securing and Assessment are given and can be used out of the box. In short, don't wait. Go get it now! From the book's introduction: Part I, "Introduction to Threats and Countermeasures," identifies and illustrates the various threats facing the network, host, and application layers. The process of threat modeling helps you to identify those threats that can harm your application.

**Download to continue reading...**

Generally Accepted Accounting Principles) ASP.NET Core Application Development: Building an application in four sprints (Developer Reference)

Dmca