Printed by: shikridat@gmail.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

	g and Countermeasures g Essential Concepts - II	Exam 312-50 Certified Ethical Hacker
Ga	thering Security Requirements	C EH
•	Eliciting software security requirements takes different approaches	
9	Security Requirements should be enumerated separately from the function can be separately reviewed and tested	ial requirement so that they
	Mixing the security requirement with the functional requirement can make	e the security requirement
•	gathering process more complicated and less accurate	
9	Functional requirements are positive requirements specifying what the softwo	
9	Security requirements are negative requirements specifying what the software	reshould not do
	It is the natural tendency of people to be clear about what they want but to things they don't want	find it difficult to understand
9	mings and don't mant	and it difficult to difficulties
9	Software needs to be viewed in a more negative, critical, and destructive was use and its associated security requirements	
9	Software needs to be viewed in a more negative, critical, and destructive was use and its associated security requirements	y to reveal its non-intended
Notes:	Software needs to be viewed in a more negative, critical, and destructive was use and its associated security requirements	
9	Software needs to be viewed in a more negative, critical, and destructive was use and its associated security requirements	y to reveal its non-intended
9	Software needs to be viewed in a more negative, critical, and destructive was use and its associated security requirements	y to reveal its non-intended

Printed by: shikridat@gmail.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Key Benefits of Addressing Security at the Requirement Phase



- Addressing security at the requirement phase can save billions of dollars compared to addressing security at a later phase of software development
- It also specifies the security mechanisms that need to be implemented in order to comply with regulations, standards or requirements for the secure application development and attack protection
- Security requirements give the developer an overview about the key security controls required to build a secure application
- Correctly understood security requirements can help in implementing security in the design, development, and testing stages

warriets (C. b., 15. Carrell, All Bioles Research Reproduction in Strictly Brobbits of

Secure Application Design and Architecture



- A security negligence in the design and architecture phase may lead to vulnerabilities that are difficult to detect and expensive to fix in production
- Security vigilance in the design phase enables the detection of potential security flaws early in the software development lifecycle
- Secure design of an application is based on the security requirements identified in the previous phase of the SDLC
- Secure design is a challenging process as designing required security controls may obstruct business functionality requirements

Copyright $\, \mathfrak{S} \,$ by \mathfrak{W} -Cosscil. All Rights Reserved. Reproduction is Strictly Problemed.

Notes:				

Appendix B Page 3762

Ethical Hacking and Countermeasures Copyright © by **EC-Council**All Rights Reserved. Reproduction is Strictly Prohibited.