<p class="pinDescription">
Dance problems.
<div class="Module SocialIconsCounts" id="Soci
<div class="pinSocialMeta">
<a class="socialItem"
href="/pin/297026537901201080/repins/" data-ele
<em class="repinIconSmall"></em>
<em class="socialMetaCount repinCount
<a class="socialItem likes" href="/pin/2970265
ta-element-type="175">
<em class="likeIconSmall"></em>
</div>
<button class="Button DropdownButton Module UserEducationDropdownButton borderless
moreFooter footerIcon userEducationTutorialButton" data-element-type="245" id="UserEd
onDropdownButton-202" type="button">

JAVA
CASE
Certified Application Security Engineer

CASE Java

Exam Blueprint
(Version 1)

Domain	Objectives/ Sub-Domain	Weightage
1. Understanding Application Security, Threats, and Attacks	▪ Understand the need and benefits of application security ▪ Demonstrate the understanding of common application-level attacks ▪ Explain the causes of application-level vulnerabilities ▪ Explain various components of comprehensive application security ▪ Explain the need and advantages of integrating security in Software Development Life Cycle (SDLC) ▪ Differentiate functional vs security activities in SDLC ▪ Explain Microsoft Security Development Lifecycle (SDL) ▪ Demonstrate the understanding of various software security reference standards, models, and frameworks	18%
2. Security Requirements Gathering	▪ Understand the importance of gathering security requirements ▪ Explain Security Requirement Engineering (SRE) and its phases ▪ Demonstrate the understanding of Abuse Cases and Abuse Case Modeling ▪ Demonstrate the understanding of Security Use Cases and Security Use Case Modeling ▪ Demonstrate the understanding of Abuser and Security Stories ▪ Explain Security Quality Requirements Engineering (SQUARE) Model ▪ Explain Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Model	8%
3. Secure Application Design and Architecture	▪ Understand the importance of secure application design ▪ Explain various secure design principles ▪ Demonstrate the understanding of threat modeling ▪ Explain threat modeling process ▪ Explain STRIDE and DREAD Model ▪ Demonstrate the understanding of Secure Application Architecture Design	12%

Certified Application Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Domain	Objectives/ Sub-Domain	Weightage
4. Secure Coding Practices for Input Validation	▪ Understand the need of input validation ▪ Explain data validation techniques ▪ Explain data validation in strut framework ▪ Explain data validation in Spring framework ▪ Demonstrate the knowledge of common input validation errors ▪ Demonstrate the knowledge of common secure coding practices for input validation	8%
5. Secure Coding Practices for Authentication and Authorization	▪ Understand authentication concepts ▪ Explain authentication implementation in Java ▪ Demonstrate the knowledge of authentication weaknesses and prevention ▪ Understand authorization concepts ▪ Explain Access Control Model ▪ Explain EJB authorization ▪ Explain Java Authentication and Authorization (JAAS) ▪ Demonstrate the knowledge of authorization common mistakes and countermeasures ▪ Explain Java EE security ▪ Demonstrate the knowledge of authentication and authorization in Spring Security Framework ▪ Demonstrate the knowledge of defensive coding practices against broken authentication and authorization	4%
6. Secure Coding Practices for Cryptography	▪ Understand fundamental concepts and need of cryptography in Java ▪ Explain encryption and secret keys ▪ Demonstrate the knowledge of cipher class implementation ▪ Demonstrate the knowledge of digital signature and its implementation ▪ Demonstrate the knowledge of Secure Socket Layer (SSL) and its implementation ▪ Explain Secure Key Management ▪ Demonstrate the knowledge of digital certificate and its implementation	6%

Certified Application Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Domain	Objectives/ Sub-Domain	Weightage
	▪ Demonstrate the knowledge of Hash implementation ▪ Explain Java Card Cryptography ▪ Explain Crypto Module in Spring Security ▪ Demonstrate the understanding of Do's and Don'ts in Java Cryptography	
7. Secure Coding Practices for Session Management	▪ Explain session management in Java ▪ Demonstrate the knowledge of session management in Spring framework ▪ Demonstrate the knowledge of session vulnerabilities and their mitigation techniques ▪ Demonstrate the knowledge of best practices and guidelines for secure session management	10%
8. Secure Coding Practices for Error Handling	▪ Explain Exception and Error Handling in Java ▪ Explain erroneous exceptional behaviors ▪ Demonstrate the knowledge of do's and don'ts in error handling ▪ Explain Spring MVC error handling ▪ Explain Exception Handling in Struts2 ▪ Demonstrate the knowledge of best practices for error handling ▪ Explain to Logging in Java ▪ Demonstrate the knowledge of Log4j for logging ▪ Demonstrate the knowledge of coding techniques for secure logging ▪ Demonstrate the knowledge of best practices for logging	16%
9. Static and Dynamic Application Security Testing (SAST & DAST)	▪ Understand Static Application Security Testing (SAST) ▪ Demonstrate the knowledge of manual secure code review techniques for most common vulnerabilities ▪ Explain Dynamic Application Security Testing ▪ Demonstrate the knowledge of Automated Application Vulnerability Scanning Tools for DAST ▪ Demonstrate the knowledge of Proxy-based Security Testing Tools for DAST	8%

Certified Application Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Domain	Objectives/ Sub-Domain	Weightage
10. Secure Deployment and Maintenance	▪ Understand the importance of secure deployment ▪ Explain security practices at host level ▪ Explain security practices at network level ▪ Explain security practices at application level ▪ Explain security practices at web container level (Tomcat) ▪ Explain security practices at Oracle database level ▪ Demonstrate the knowledge of security maintenance and monitoring activities	10%

Certified Application Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.