Cloud application security in Java for AWS

Category: Networking & Security | **Vendor:** Amazon Web Services

Duration: 40.00 hours (5 days) **32.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

Your cloud application written in Java works as intended, so you are done, right? But did you consider feeding in incorrect values? 16Gbs of data? A null? An apostrophe? Negative numbers, or specifically -1 or -2^31? Because that’s what the bad guys will do – and the list is far from complete.

The cloud has become a critical aspect of online services. No matter which model you’re using (SaaS, PaaS, IaaS), part of your service is now operated by someone else. This may look like a net positive, but it also greatly expands the attack surface and brings in several new risks that may not be obvious. Have you configured all security settings correctly? Are you prepared for supply chain attacks? How can you protect the confidentiality of user data in the cloud? And most importantly: can the bad guys use your exposure to their advantage?

Handling security needs a healthy level of paranoia, and this is what this course provides: a strong emotional engagement by lots of hands-on labs and stories from real life, all to substantially improve code hygiene. Mistakes, consequences, and best practices are our blood, sweat and tears.

The curriculum goes through the common Web application security issues following the OWASP Top Ten but goes far beyond it both in coverage and the details.All this is put in the context of Java, and extended by core programming issues, discussing security pitfalls of the Java language and the AWS cloud platform.

So that you are prepared for the forces of the dark side.

So that nothing unexpected happens.

Nothing.

About This Course

Your cloud application written in Java works as intended, so you are done, right? But did you consider feeding in incorrect values? 16Gbs of data? A null? An apostrophe? Negative numbers, or specifically -1 or -2^31? Because that’s what the bad guys will do – and the list is far from complete.

The cloud has become a critical aspect of online services. No matter which model you’re using (SaaS, PaaS, IaaS), part of your service is now operated by someone else. This may look like a net positive, but it also greatly expands the attack surface and brings in several new risks that may not be obvious. Have you configured all security settings correctly? Are you prepared for supply chain attacks? How can you protect the confidentiality of user data in the cloud? And most importantly: can the bad guys use your exposure to their advantage?

Handling security needs a healthy level of paranoia, and this is what this course provides: a strong emotional engagement by lots of hands-on labs and stories from real life, all to substantially improve code hygiene. Mistakes, consequences, and best practices are our blood, sweat and tears.

The curriculum goes through the common Web application security issues following the OWASP Top Ten but goes far beyond it both in coverage and the details.All this is put in the context of Java, and extended by core programming issues, discussing security pitfalls of the Java language and the AWS cloud platform.

So that you are prepared for the forces of the dark side.

So that nothing unexpected happens.

Nothing.

Who Should Attend

Java developers working on Web applications and AWS

Prerequisites & Entry Requirements

General Prerequisites:

General Java and Web development

Learning Outcomes

Upon successful completion of this course, participants will be able to:

- Understand cloud security specialties
- Getting familiar with essential cyber security concepts
- Understanding how cryptography supports security
- Learning how to use cryptographic APIs correctly in Java
- Understanding Web application security issues
- Detailed analysis of the OWASP Top Ten elements
- Putting Web application security in the context of Java
- Going beyond the low hanging fruits
- Managing vulnerabilities in third party components
- Learn to deal with cloud infrastructure security
- Input validation approaches and principles
- Identify vulnerabilities and their consequences
- Learn the security best practices in Java

Detailed Course Outline

Day 1

- Cyber security basics
- What is security?
- Threat and risk
- Cyber security threat types – the CIA triad
- Cyber security threat types – the STRIDE model
- Consequences of insecure software
- Cloud security basics
- Cloud infrastructure basics
- The Cloud Cube Model and Zero Trust Architecture
- The OWASP Top Ten 2021

- The OWASP Top 10 2021
- A01 - Broken Access Control
- Access control basics
- Failure to restrict URL access
- Confused deputy
- File upload
- Open redirects and forwards
- Cross-site Request Forgery (CSRF)
- A02 - Cryptographic Failures
- Information exposure
- Cryptography for developers

Day 2

- A02 - Cryptographic Failures (continued)
- Cryptography for developers
- Transport security
- A03 - Injection
- Injection principles
- Injection attacks
- SQL injection
- NoSQL injection
- Parameter manipulation
- Code injection
- HTML injection - Cross-site scripting (XSS)

Day 3

- A04 - Insecure Design
- The STRIDE model of threats
- Secure design principles of Saltzer and Schroeder
- Client-side security
- A05 - Security Misconfiguration
- Configuration principles
- Server misconfiguration
- AWS configuration best practices
- Cookie security
- XML entities
- A06 - Vulnerable and Outdated Components
- Using vulnerable components
- Assessing the environment
- Hardening
- Untrusted functionality import
- Vulnerability management
- A07 - Identification and Authentication Failures
- Authentication
- Session management
- Identity and access management (IAM)

Day 4

- A07 - Identification and Authentication Failures (continued)
- Password management
- A08 - Software and Data Integrity Failures
- Integrity protection
- Subresource integrity
- Insecure deserialization
- A09 - Security Logging and Monitoring Failures

- Logging and monitoring principles
- Log forging
- Log forging – best practices
- Case study – Log interpolation in log4j
- Case study – The Log4Shell vulnerability (CVE-2021-44228)
- Case study – Log4Shell follow-ups (CVE-2021-45046, CVE-2021-45105)
- Lab – Log4Shell
- Logging best practices
- Detection and monitoring
- A10 - Server-side Request Forgery (SSRF)
- Server-side Request Forgery (SSRF)
- Case study – SSRF and the Capital One breach

Cloud security

AWS security
- Security considerations
- Data security in the cloud

Day 5

Cloud security
- Container security
- Container security concerns
- Containerization, virtualization and security
- The attack surface
- Docker security
- Kubernetes security

The OWASP Top Ten 2021

Web application security beyond the Top Ten

- Code quality
- Denial of service

Input validation

- Input validation principles
- Denylists and allowlists
- What to validate – the attack surface
- Where to validate – defense in depth
- When to validate – validation vs transformations
- Validation with regex
- Integer handling problems
- Representing signed numbers
- Integer visualization
- Integer overflow
- Lab – Integer overflow
- Signed / unsigned confusion in Java
- Case study – The Stockholm Stock Exchange
- Integer truncation
- Best practices
- Files and streams
- Path traversal
- Lab – Path traversal
- Path traversal-related examples
- Additional challenges in Windows
- Virtual resources

- Path traversal best practices

- Lab – Path canonicalization

- Unsafe reflection

- Reflection without validation

- Lab – Unsafe reflection

- Unsafe native code

- Native code dependence

- Lab – Unsafe native code

- Best practices for dealing with native code

Wrap up

- Secure coding principles

- And now what?

Skills You Will Learn:

- Understand cloud security specialties
- Getting familiar with essential cyber security concepts
- Understanding how cryptography supports security
- Learning how to use cryptographic APIs correctly in Java
- Understanding Web application security issues
- Detailed analysis of the OWASP Top Ten elements
- Putting Web application security in the context of Java
- Going beyond the low hanging fruits
- Managing vulnerabilities in third party components
- Learn to deal with cloud infrastructure security
- Input validation approaches and principles
- Identify vulnerabilities and their consequences
- Learn the security best practices in Java

Frequently Asked Questions

Q: What delivery options are available for Cloud application security in Java for AWS ?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 5-day Cloud application security in Java for AWS course provides up to 32.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Cloud application security in Java for AWS training?

The training takes place over 5 day(s), with each day lasting approximately 40.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Cloud application security in Java for AWS ?

Yes, we provide corporate training, dedicated training, and closed classes for Cloud application security in Java for AWS . Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Cloud application security in Java for AWS , Cloud Application Security, CASEC-JAWS

Q: Why choose Nexus Human for Cloud application security in Java for AWS ?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Cloud application security in Java for AWS training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)