Extended web application security

Category: Networking & Security | **Vendor:** Various

Duration: 32.00 hours (4 days) **26.0 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

Your application written in any programming language 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.

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.

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

So that nothing unexpected happens.

Nothing.

About This Course

Your application written in any programming language 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.

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.

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

So that nothing unexpected happens.

Nothing.

Who Should Attend

Web developers.

Prerequisites & Entry Requirements

General Prerequisites:

General Web development.

Learning Outcomes

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

- Getting familiar with essential cyber security concepts
- Understanding how cryptography supports security
- Understanding Web application security issues
- Detailed analysis of the OWASP Top Ten elements
- Putting Web application security in the context of any programming language
- Going beyond the low hanging fruits
- Input validation approaches and principles
- Managing vulnerabilities in third party components

Detailed Course Outline

Day 1

- Cyber security basics
- What is security?
- Threat and risk
- Cyber security threat types – the CIA triad
- Consequences of insecure software
- The OWASP Top Ten 2021
- The OWASP Top 10 2021
- A01 - Broken Access Control
- Access control basics
- Confused deputy
- File upload
- Open redirects and forwards
- Cross-site Request Forgery (CSRF)
- A02 - Cryptographic Failures
- Information exposure

- Cryptography for developers

Day 2

- A03 - Injection
- Input validation
- Injection
- SQL injection
- NoSQL injection
- Parameter manipulation
- Code injection
- Some other injection types
- 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
- 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

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
- Insufficient logging
- Case study – Plaintext passwords at Facebook
- Logging best practices
- Monitoring best practices
- Firewalls and Web Application Firewalls (WAF)
- Intrusion detection and prevention
- Case study – The Marriott Starwood data breach
- A10 - Server-side Request Forgery (SSRF)
- Server-side Request Forgery (SSRF)
- Case study – SSRF and the Capital One breach
- Web application security beyond the Top Ten
- Denial of service
- Wrap up
- Secure coding principles
- And now what?

Skills You Will Learn:

- Getting familiar with essential cyber security concepts
- Understanding how cryptography supports security
- Understanding Web application security issues
- Detailed analysis of the OWASP Top Ten elements
- Putting Web application security in the context of any programming language
- Going beyond the low hanging fruits
- Input validation approaches and principles
- Managing vulnerabilities in third party components

Frequently Asked Questions

Q: What delivery options are available for Extended web application security?

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 4-day Extended web application security course provides up to 26.0 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Extended web application security training?

The training takes place over 4 day(s), with each day lasting approximately 32.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Extended web application security?

Yes, we provide corporate training, dedicated training, and closed classes for Extended web application security. 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: Extended web application security, Web Application Security, EWASEC

Q: Why choose Nexus Human for Extended web application security?

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 Extended web application security 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)