SEC522: Application Security: Securing Web Applications, APIs, and Microservices™

GWEB
Web Application Defender
giac.org/gweb

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Defend against OWASP Top 10 attacks and input-driven vulnerabilities like SQL injection, XSS, and CSRF
- Harden infrastructure, configurations, and software supply chains against modern attack campaigns
- Strengthen authentication and authorization with passkeys, multifactor authentication, OAuth, and SAML
- Protect REST and GraphQL APIs and microservices from abuse and data exposure
- Improve web security using protective HTTP headers, Content Security Policy, and cross-origin controls
- Secure AI and LLM-powered application components against prompt injection and other emerging attacks

Business Takeaways

- Comply with PCI DSS requirements and other compliance requirements
- Reduce the overall application security risks, protect company reputation
- Adopt the "shift left" mindset: Address security issues early and quickly, reducing cost
- Adopt APIs, microservices, and AI capabilities in a secure manner
- Prepare students for the GWEB certification

"Lots of good hands-on exercises using real-world examples."

—Nicolas Kravec, **Morgan Stanley**

"The exercises are a good indicator of understanding the material. They worked flawlessly for me."

—Robert Fratila, **Microsoft**

It's not a matter of "if" but "when." Be prepared for a web attack. We'll teach you how.

HTTP is no longer just about websites. It is the universal language that lets cloud services, microservices, APIs, and AI platforms talk to each other. Whether you are securing a traditional web application, protecting cloud-native services, or defending AI model endpoints, the fundamentals remain the same: HTTP-based protocols and the security implications that come with them.

SEC522 is built around this reality and provides training that goes well beyond traditional web application security. As organizations move to cloud platforms, adopt microservices, and embed AI capabilities into their products, they are all building on the same HTTP foundation. A vulnerability in any of these systems can compromise far more than a single application. It can expose entire cloud environments, API ecosystems, and AI services.

Throughout SEC522, we show how HTTP security principles apply across the whole technology stack. Traditional web applications, RESTful APIs, GraphQL endpoints, and AI model serving platforms all rely on HTTP. Students learn to recognize attack patterns that span these technologies and to implement defensive strategies that protect the entire ecosystem, including the emerging generation of LLM-powered and agentic applications.

The skills taught in SEC522 apply the moment you return to work. AI platforms expose inference endpoints over HTTP APIs, cloud services communicate through REST interfaces, and microservices orchestrate through HTTP calls, so the security principles you master here only grow in importance. You will learn to spot vulnerabilities early in development, communicate risk clearly, and implement controls that protect modern architectures.

Hands-On Cloud Application Security Training

The lab environment offers a realistic application setting where students can explore attacks and see the impact of defensive mechanisms. Structured as challenges with helpful hints, the hands-on labs provide practical experience that students can apply immediately when they return to work. 17 labs across Sections 1 to 5 culminate in an exciting, competitive Defend the Flag capstone that fills the final afternoon. This closing challenge allows participants to put their skills to the test in a dedicated, immersive exercise.

- **SECTION 1:** HTTP Basics, Inspecting HTTP/2 Traffic and Crafting Requests, Isolation, SSRF and Credential Theft
- **SECTION 2:** SQL Injection, Cross-Site Request Forgery, Cross-Site Scripting, File Upload and Java Deserialization
- **SECTION 3:** Passkeys and WebAuthn Origin Binding, Authentication Weaknesses and Session Fixation, OAuth and Authorization, JWT Algorithm Confusion and TLS Inspection
- **SECTION 4:** Cross-Origin Requests (CORS), API Discovery, API Security: BOLA, Client-Side Hardening: CSP and Clickjacking
- **SECTION 5:** AI Security: Defending an LLM Chatbot, then the Defend-the-Flag Capstone

Section Descriptions

SECTION 1: Web Foundations and Secure Configurations

The course opens with the fundamentals that make web applications work, including the HTTP protocol family, authentication, sessions, and application architecture. It then hardens every layer beneath the application: software dependencies, server configurations, and cloud environments, with hands-on defense against supply chain attacks and SSRF.

TOPICS: Introduction to HTTP, Including HTTP/2 and HTTP/3; Authentication, Sessions, and Cookies; Web Application Architecture; Dependency and Supply Chain Security; Cloud Security and SSRF Defense

SECTION 2: Input Attacks and Defenses

Every input to an application is a potential weapon. This section builds the defensive foundation against input-driven attacks: injection in its many forms, including prompt injection, cross-site request forgery, cross-site scripting, and the handling of Unicode, file uploads, and serialized data. It closes with business logic and concurrency flaws.

TOPICS: Injection Attacks, From SQL to Prompt Injection; Cross-Site Request Forgery; Cross-Site Scripting Foundations; Input Validation Strategies; File Upload, Deserialization, Business Logic, and Concurrency

SECTION 3: Authentication, Authorization, and Cryptography

Identity is the new perimeter. This section covers authentication from passwords to passkeys and multifactor, session management, and access control, then digs into the protocols behind modern identity: OAuth, OpenID Connect, JWT, and SAML. It closes with transport security and cryptography, including preparing applications for post-quantum migration.

TOPICS: Authentication Vulnerabilities and Modern Factors, Including Passkeys; Session Management and Fixation; Access Control and Authorization; OAuth, OpenID Connect, JWT, and SAML; Transport Security, Cryptography, and Post-Quantum Readiness

SECTION 4: APIs, Web Services, and Client-Side Security

This section secures every interface a modern application exposes. It moves from XML and SOAP web services to the same-origin policy and CORS, then deep into REST and GraphQL API security. The second half turns to the browser: defeating XSS with CSP and Trusted Types, protecting the client-side supply chain, and defending against clickjacking.

TOPICS: Web Services Overview; XML Security; Same-Origin Policy and CORS; REST and GraphQL API Security; XSS Defense and Client-Side Supply Chain

SECTION 5: AI Security, MLSecOps, and Microservices

The final section tackles the frontier: securing microservices and the AI applications built on them. Topics include service-to-service trust, AI gateways and Model Context Protocol integrations, prompt injection defense, the OWASP Top 10 for LLM applications, MLSecOps, and agentic threat modeling. The afternoon belongs to the Defend the Flag capstone.

TOPICS: Microservices Security Patterns; AI and LLM Application Security; MLSecOps Lifecycle; Threat Modeling AI and Agentic Systems; Incident Response for Agentic Applications

"I pentest websites and report vulnerabilities with recommendations on how to fix [them]. This course allowed me to get a better understanding of attack mechanics and vulnerabilities that enable them. Now, I will be able to provide more pointed feedback to developers that should lead to speedier resolutions."

—Alexei Gorbounov, **Cisco**

Who Should Attend

- Application developers
- Application security analysts or managers
- Application architects
- Penetration testers who are interested in learning about defensive strategies
- Security professionals who are interested in learning about web application security
- Auditors who need to understand defensive mechanisms in web applications
- Employees of PCI-compliant organizations who need to be trained to comply with those requirements

NICE Framework Work Roles

- Software Developer (OPM 621)
- Secure Software Assessor (OPM 622)
- Research & Development Specialist (OPM 661)
- Information Systems Security Developer (OPM 631)
- Systems Developer (OPM 632)

GWEB
Web Application Defender
giac.org/gweb

GIAC Certified Web Application Defender

The GIAC Web Application Defender (GWEB) certification validates a practitioner's expertise handling the common web application errors that lead to most security problems. GWEB certification holders have hands-on experience using current tools to detect and prevent input validation flaws, cross-site scripting (XSS), and SQL injection, also possessing in-depth understanding of the weaknesses and best defenses for authentication, access control, and session management.