SEC522: Application Security: Securing Web Apps, APIs, and Microservices

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

During the course, we demonstrate the risks of web applications and the extent of sensitive data that can be exposed or compromised. From there, we offer real world solutions on how to mitigate these risks and effectively evaluate and communicate residual risks.

After attending the class, students will be able to apply what they learned quickly and bring back techniques to not only better secure their applications, but also do so efficiently by adding security early in the software development life cycle, shifting left security decisions and testing, thus saving time, money, and resources for the organization.

Business Takeaways

- Comply with PCI DSS 6.5 requirements
- Reduce the overall application security risks, protect company reputation
- Adopt the Shifting left mindset where security issues addressed early and quickly. This avoids the costly rework.
- Ability to adopt modern apps with API and microservices in a secure manner
- This course prepares students for the GWEB certification

Hands-on Training

The provided VM lab environment contains realistic application environment to explore the attacks and the effects of the defensive mechanisms. The exercise is structured in a challenge format with hints available along the way. The practical hands-on exercises help students gain experience to hit the ground running back at the office. There are 20 labs in section 1 to section 5 of the class and in the last section, there is a capstone exercise called Defending the Flag where there is 3–4 hours of dedicated competitive exercise time.

- **SECTION 1:** HTTP Basics, HTTP/2 traffic inspection and spoofing, Environment isolation, SSRF and credential-stealing
- **SECTION 2:** SQL Injection, Cross Site Request Forgery, Cross Site Scripting, Unicode and File Upload
- **SECTION 3:** Authentication vulnerabilities and defense, Multifactor authentication, Session vulnerabilities and testing, Authorization vulnerabilities and defense, SSL vulnerabilities and testing, Proper encryption use in web application
- **SECTION 4:** WSDL enumerations, Cross Domain AJAX, Front End Features and CSP (Content Security Policy), Clickjacking
- **SECTION 5:** Deserialization and DNS rebinding, GraphQL, API gateways and JSON, SRI and Log review
- **SECTION 6:** Defending the Flag capstone exercise

You Will Be Able To

- Defend against the attacks specified in OWASP Top 10
- Infrastructure security and configuration management
- Securely integrating cloud components into a web application
- Authentication and authorization mechanisms, including single sign-on patterns
- Cross-domain web request security
- Protective HTTP headers
- Defending SOAP, REST and GraphQL APIs
- Securely implement Microservice architecture
- Defending against input related flaws such as SQL injection, XSS and CSRF

“Labs were fun and challenging.”
—Linh Sithihao, Dignity Health

“[Labs are] thought out and easy to follow with good practical knowledge learned.”
—Barbara Boone, CDC

“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
“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