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

GWEB
Web Application Defender
giac.org/gweb

6 Day Program | 36 CPEs | Laptop Required

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**

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

Section Descriptions

SECTION 1: Web Fundamentals and Secure Configurations

The first section of the course will set the stage for the course with the fundamentals of web applications such as the HTTP protocol and the various mechanisms that make web applications work. We then transition over to the architecture of the web applications which plays a big role in securing the application.

TOPICS: Introduction to HTTP Protocol; Overview of Web Authentication Technologies; Web Application Architecture; Recent Attack Trends; Web Infrastructure Security/Web Application Firewalls; Managing Configurations for Web Apps

SECTION 2: Input-Related Defenses

Section 2 is devoted to protecting against threats arising from external input. Modern applications have to accept input from multiple sources, such as other applications, browsers, and web services. The basic mechanics of the common input related attacks are covered, followed by real-world examples and defense patterns that work in large applications. Input related flaws take up multiple places in the OWASP Top 10 list, the coverage of these input related topics forms a great defense foundations against these common risks.

TOPICS: Input-related Vulnerabilities in Web Applications; SQL Injection; Cross-site Request Forgery; Cross-site Scripting Vulnerability and Defenses; Unicode Handling Strategy; File Upload Handling; Business Logic and Concurrency

SECTION 3: Authentication and Authorization

Section 3 starts with a discussion of authentication and authorization in web applications, followed by examples of exploitation and the mitigations that can be implemented in the short and long terms. Considering the trend to move towards less reliance on passwords for authentication, we cover the modern patterns of password-less authentication and multifactor authentications.

TOPICS: 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: Web Services and Front-End Security

In this section, we start with covering the concepts of Web services and specifically SOAP based web services. Then we pivot the focus to the front end usage of JavaScript with the related security implications such as CORS (Cross Domain Requests). We will cover security issues, mitigation strategies, and general best practices for implementing AJAX based Web applications. We will also examine real-world attacks and trends to give you a better understanding of exactly what you are protecting against. We end the day with multiple client-side, header-based defense mechanisms such as Content Security Policy to help you further secure your applications. We go in-depth into how these headers can uplift the security level of an application, but we'll also look at the potential downfall of these mechanisms.

TOPICS: Web services overview; XML Security; AJAX Attack Trends and Defenses; Modern JavaScript Frameworks; Browser Features and Defenses; Browser-Based Defense such as Content Security Policy

SECTION 5: APIs and Microservices Security

The section starts off with the topic of deserialization security issue which is quickly rising to be a common attack amongst modern applications. We also cover the topic of DNS rebinding which lingers in the application world since practically the beginning of web applications. The focus then shift over to REST API and GraphQL API-based Web services and APIs where these technologies exist in every modern applications and have lots of potential security pitfalls. We then extend the discussion into microservices architecture and the security implications of this modern architecture. Across all these technology topics we cover the common attacks and the current best practices in keeping them secure. The day ends with three process centric topics of operational security, security testing, and logging.

TOPICS: Deserialization; REST Security; GraphQL Security; Microservices; Operational Security; Security Testing; Logging and Error Handling

SECTION 6: DevSecOps and Defending the Flag

We start this section by introducing the concept of DevSecOps and how to apply it to web development and operations in enterprise environment. The main activity of this section will be a lab experience that will tie together the lessons learned during the entire course and reinforce them with hands-on implementation. Students will then have to decide which vulnerabilities are real and which are false positives, then mitigate the vulnerabilities. Students will learn through these hands-on exercises how to secure the web application, starting with securing the operating system and the web server, finding configuration problems in the application language setup, and finding and fixing coding problems on the site.

TOPICS: DevSecOps

"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

GWEB
Web Application Defender
giac.org/gweb

GIAC Certified Web Application Defender

The GIAC Web Application Defender certification allows candidates to demonstrate mastery of the security knowledge and skills needed to deal with common web application errors that lead to most security problems. The successful candidate will have hands-on experience using current tools to detect and prevent input validation flaws, cross-site scripting (XSS), and SQL injection as well as an in-depth understanding of authentication, access control, and session management, their weaknesses, and how they are best defended. GIAC Certified Web Application Defenders (GWEB) have the knowledge, skills, and abilities to secure web applications and recognize and mitigate security weaknesses in existing web applications.

- Access Control, AJAX Technologies and Security Strategies, Security Testing, and Authentication
- Cross Origin Policy Attacks and Mitigation, CSRF, and Encryption and Protecting Sensitive Data
- File Upload, Response Readiness, Proactive Defense, Input Related Flaws and Input Validation
- Modern Application Framework Issues and Serialization, Session Security & Business Logic, Web
- Application and HTTP Basics, Web Architecture, Configuration, and Security