SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

SEC522: Defending Web Applications Security Essentials

GWEB
Web Application Defender
giac.org/gweb

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Understand the major risks and common vulnerabilities related to web applications through real-world examples
- Mitigate common security vulnerabilities in web applications using proper coding techniques, software components, configurations, and defensive architecture
- Understand the best practices in various domains of web application security such as authentication, access control, and input validation
- Fulfill the training requirement as stated in PCI DSS 6.5
- Deploy and consume web services (SOAP and REST) in a more secure fashion
- Proactively deploy cutting-edge defensive mechanisms such as the defensive HTTP response headers and Content Security Policy to improve the security of web applications
- Strategically roll out a web application security program in a large environment
- Incorporate advanced web technologies such as HTML5 and AJAX cross-domain requests into applications in a safe and secure manner
- Develop strategies to assess the security posture of multiple web applications

> **"Brilliant! The combination of hands-on exercises and Q&A streamlines learning like nothing else."**
>
> — McKell Gomm, **Henry Schein**

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

The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure them. Traditional network defenses, such as firewalls, fail to secure web applications. DEV522 covers the OWASP Top 10 Risks and will help you better understand web application vulnerabilities, thus enabling you to properly defend your organization's web assets.

Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world applications that have been proven to work. The testing aspect of vulnerabilities will also be covered so that you can ensure your application is tested for the vulnerabilities discussed in class.

To maximize the benefit for a wider range of audiences, the discussions in this course will be programming language agnostic. Focus will be maintained on security strategies rather than coding-level implementation.

DEV522 is intended for anyone tasked with implementing, managing, or protecting web applications. It is particularly well suited to application security analysts, developers, application architects, pen testers, auditors who are interested in recommending proper mitigations for web security issues, and infrastructure security professionals who have an interest in better defending their web applications.

The course will also cover additional issues the authors have found to be important in their day-to-day web application development practices. The topics that will be covered include:

- Infrastructure security
- Server configuration
- Authentication mechanisms
- Application language configuration
- Application coding errors like SQL injection and cross-site scripting
- Cross-site request forging
- Authentication bypass
- Web services and related flaws
- Web 2.0 and its use of web services
- XPATH and XQUERY languages and injection
- Business logic flaws
- Protective HTTP headers

SEC522 features full-day lab with hands-on exercises on how to secure a web application, starting with securing the operating system and web server, finding configuration problems in the application language setup, and finding and fixing coding problems in the site.The course makes heavy use of hands-on exercises and will conclude with a large defensive exercise that reinforces the lessons learned throughout the week.

Section Descriptions

SECTION 1: Web Fundamentals and Security Configurations

You cannot win the battle if you do not understand what you are trying to defend. Day one starts with an overview of recent web application attack and security trends, followed by an examination of the essential technologies that are at play in web applications. We arm you with the right information so you can understand how web applications work and the security concepts related to them.

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: Defense Against Input-Related Threats

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. Web application attacks during the past few years have reminded us that these attack patterns are employed frequently.

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: Web Application Authentication and Authorization

Section 3 starts with a discussion of authentication 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. We complete the discussion by providing information on how to discover and test for vulnerabilities.

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

We'll start section 4 by focusing on proactive defense mechanisms so that we can be ahead of the bad guys in the game of hack-and-defend. We will cover such topics as handling file uploads, intrusion detection, and the use of deception. The material is designed to give you the extra edge in defending your application.

TOPICS: Honeytoken; Web Services Overview; Security in Parsing of XML; XML Security; AJAX Technologies Overview; AJAX Attack Trends and Common Attacks; REST Security; Browser-based Defense such as Content Security Policy

SECTION 5: Cutting-Edge Web Security

Section 5 focuses on cutting-edge web application technologies and current research in this area. Topics such as serialization security, clickjacking, and DNS rebinding are covered. These vulnerabilities have emerged and changed in recent years, and we are refining our defense strategies against them. We cover recent developments on these topics and the latest defensive tactics to protect against these attacks.

TOPICS: Serialization Security; Clickjacking; DNS Rebinding; HTML5 Security; Logging Collection and Analysis for Web Apps; Security Testing; IPv6 Impact on Web Security

SECTION 6: Capture-and-Defend-the-Flag Exercise

Section 6 starts by introducing the secure software development life cycle and how to apply it to web development. The main activity will be a large lab that will tie together the lessons learned during the week and reinforce them with hands-on applications. Students will be provided with a virtual machine to implement a complete database-driven dynamic website. In addition, they will use a custom tool to enumerate security vulnerabilities and simulate a vulnerability assessment of the website. Students will then have to decide which vulnerabilities are real and which are false positives, then mitigate the vulnerabilities. The scanner will score the student as vulnerabilities are eliminated or checked off as false positives. Advanced students will be able to extend this exercise and find vulnerabilities not presented by the scanner. 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: Mitigating Server Configuration Errors; Discovering and Mitigating Coding Problems; Testing Business Logic Issues and Fixing Problems; Testing Web Services and Mitigating Security Problems; Reinforcing Key Topics Discussed Throughout the Course through Comprehensive Exercises

> **"I'm responsible for the web application security for my company, but have never been a developer. I feel I now have the knowledge needed to sit with my developers, understand, and discuss in greater depth the security of our web applications!"**
>
> — James Baker, **Pass Key**

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