DEVELOPER 522

Hands On | Six Days | Laptop Required | 36 CPEs | GIAC Cert: GWEB

DEV522: Defending Web Applications Security Essentials

This is the course to take if you have to defend web applications!

Traditional network defenses, such as firewalls, fail to secure web applications. The quantity and importance of data entrusted to web applications is growing, and defenders need to learn how to secure them. DEV522 covers the OWASP Top 10 and will help you to 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 implementations that really work. The testing aspect of vulnerabilities will also be covered so 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: Defending Web Applications Security Essentials 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, and auditors who are interested in recommending proper mitigations to web security issues, and to infrastructure security professionals who have an interest in better defending their web applications.

The course will cover the topics outlined by OWASP's Top 10 risks document as well as additional issues the authors found of importance in their day-to-day web application development practice.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

The course will make heavy use of hands-on exercises. It will conclude with a large defensive exercise, reinforcing the lessons learned throughout the week.

"As the world moves everything online, DEV522 is a necessity."
-Chris Spinder, B/E Aerospace, Inc.

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 PCI requirements

"This course really proved to me that ignorance is bliss. I learned a lot that I could immediately take back to the office."
-Shawn Shirley, Ferrum College

giac.org

sans.edu

Course Day Descriptions

522.1 HANDS ON: Web Basics and Authentication Security

We begin day one with an overview of the recent web application attack trends and and security. We follow that up with an overview of the essential technologies that are at play in web applications. You can't win the battle if you don't understand what you are trying to defend. We arm you with the right information so you can understand how web applications work and the security concepts related to them.

Topics: HTTP Basics; Overview of Web Technologies; Web Application Architecture; Recent Attack Trends; Authentication Vulnerabilities and Defense; Authorization Vulnerabilities and Defense

522.2 HANDS ON: Web Application Common Vulnerabilities and Mitigations

Since the Internet does not guarantee secrecy of information being transferred, encryption is commonly used to protect the integrity and secrecy of information on the web. We cover the security of data in transit or on disk and how encryption can help with securing that information in the context of web application security.

Topics: SSL Vulnerabilities and Testing; Proper Encryption Use in Web Application; Session Vulnerabilities and Testing; Cross-Site Request Forgery; Business Logic Flaws; Concurrency; Input Related Flaws and Related Defense; SQL Injection Vulnerabilities, Testing and Defense

522.3 HANDS ON: Proactive Defense and Operation Security

Day three begins with a detailed discussion on Cross-Site Scripting, related mitigation, and testing strategy, as well as HTTP response splitting. The code in an application may be totally locked down; however, if the server setting is insecure, the server running the application can be easily compromised. Locking down the Web environment is an essential topic for discussion, so this basic concept of defending the platform and host is covered. To enable any detection of intrusion, logging, and error handling must be done correctly. We will discuss the correct approach to handling incidents and handling logs. We even dive further to cover the intrusion detection aspect of web application security. In the afternoon we turn our focus to the proactive defense mechanism so that we are ahead of the bad guys in the game of hack and defend.

Topics: Cross-Site Scripting Vulnerability and Defenses; Web Environment Configuration Security; Intrusion Detection in Web Application Incident Handling; Honeytoken

DEV522 Training Formats

(subject to change)

Live Training
sans.org/security-training/by-location/all

Summit
sans.org/summit

Community SANS
sans.org/community

Mentor Program
sans.org/mentor

OnSite
sans.org/onsite

OnDemand
sans.org/ondemand

SelStudy
sans.org/selfstudy

522.4 HANDS ON: AJAX and Web Services Security

Day four of the course is dedicated to AJAX and web services security. Asynchronous JavaScript and XML (AJAX) and web services are currently the most active areas in web application development. Security issues continue to arise as organizations are diving head first into insecurely implementing new web technologies without first understanding them.

Topics: Web Services Overview; Security in Parsing of XML; XML Security; AJAX Technologies Overview; AJAX Attack Trends and Common Attacks; AJAX Defense

522.5 HANDS ON: Cutting-Edge Web Security

Day five has a strong focus of cutting-edge web application technologies and current research area. Topics such as Clickjacking and DNS rebinding are covered. These vulnerabilities are difficult to defend against and require multiple defense strategies to be successful. Another topic of discussion is the new generation of single sign on solutions such as OpenID. We cover the implication of using these authentication systems and the common gotchas to avoid.

Topics: Clickjacking; DNS Rebinding; Flash Security; Java Applet Security; Single Signon Solution and Security; IPv6 Impact on Web Security

522.6 HANDS ON: Capture and Defend the Flag Exercise

Day six starts with an introduction to the secure software development life cycle and how to apply it to web development. But the major focus of day six is a large lab. This lab will tie the lessons learned during the week together and reinforce the lessons by practicing them hands on. The student is provided with a virtual machine implementing a complete database-driven dynamic website. In addition, a custom tool is used to enumerate security vulnerabilities and simulate a vulnerability assessment of the website. It will be up to the student to decide which vulnerabilities are real and which are false positives. The student is then asked to 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.

Topics: Mitigation of Server Configuration Errors; Discovering and Mitigating Coding Problems; Testing Business Logic Issues and Fixing Problems; Web Services Testing and Security Problem Mitigation