LEAGUE OF CODERS
www.leagueofcoders.com.sg

WEB APPLICATION & API SECURITY HARDENING EXPRT

Duration: 5 Days

COURSE OVERVIEW

The Web Application and API Security Hardening Expert course is a comprehensive training program designed to help professionals build expertise in web application and API security. The course covers a wide range of topics related to web application and API security including:

- The course covers various security threats facing web applications and APIs, such as cross-site scripting (XSS), cross-site request forgery (CSRF), SQL injection, and other common web application vulnerabilities.
- The course covers secure development practices, such as threat modeling, secure coding, and input validation, to help students develop secure and robust web applications and APIs.
- The course covers various security topics related to web applications and APIs, including authentication, authorization, encryption, and how to harden web servers and application frameworks.
- The course covers how to perform security assessments of web applications and APIs, including how to use security tools such as Burp Suite, and how to identify and remediate security vulnerabilities.
- The course covers the regulations and standards that apply to web application and API security, such as OWASP Top 10 and OWASP API Security Top 10, and how to ensure compliance with these regulations.
- The course covers how to build secure development processes, including how to incorporate security into the software development lifecycle, and how to perform regular security testing and vulnerability assessments.

Overall, this course comes with plenty of vulnerable code samples and how to harden it. And with plenty of hands-on labs, participants would be able to identify what makes an application or API vulnerable

WHAT YOU WILL ACCOMPLISH

- ✓ Understanding Secure Software Development Lifecycle and Threat Modeling
- ✓ Identifying Web Application SQL Injections Vulnerability and Hardening
- ✓ Identifying Web Application Broken Authentication and Session Management Vulnerability and Hardening
- ✓ Identifying Web Application Sensitive Data Exposure Vulnerability and Hardening
- ✓ Identifying Web Application XML External Entities (XXE) Vulnerability and Hardening
- ✓ Identifying Web Application Improper Input Validation Vulnerability and Hardening
- ✓ Identifying Web Application Security Misconfiguration Vulnerability and Hardening
- ✓ Identifying Web Application Cross-Site Scripting Vulnerability and Hardening
- ✓ Identifying Web Application Cross-Site Forgery Vulnerability and Hardening
- ✓ Identifying Web Application Insecure Deserialisation Vulnerability and Hardening
- ✓ Identifying Web Application Known Vulnerable Components Vulnerability and Hardening
- ✓ Identifying Web Application Security Through Obscurity Vulnerability
- ✓ Identifying Web Application Unvalidated Redirects and Forwards Vulnerability and Hardening

WHAT YOU WILL ACCOMPLISH

- ✓ Identifying Web Application Broken Access Control Vulnerability and Hardening
- ✓ Identifying Web Application Insufficient Anti-automation Vulnerability and Hardening
- ✓ Identifying Web Application Cryptographic Issues Vulnerability and Hardening
- ✓ Identifying Web Application Rest API Top 10 Vulnerability and Hardening
- ✓ Web Application Penetration Testing using Burp Suite

WHY THIS COURSE

- To Understand Web Application and API Security Threats: To gain a deep understanding of the security threats facing web applications and APIs and the impact that these threats can have on an organization and also provides employees with the skills and knowledge needed to identify and remediate security risks in web applications and APIs, resulting in a stronger security posture and reduced risk of security breaches and vulnerabilities.

- To Comply With Regulations and Standards: To understand the regulations and standards that apply to web application and API security that must be met with regards to data security, such as OWASP Top 10 and OWASP API Security Top 10, and by training employees in web application and API security, organizations can ensure that they are in compliance with these regulations and standards.

- To Better Manage of Security Risks: The course covers a comprehensive range of security topics, from threat modeling to secure coding practices. This allows employees to understand the full spectrum of security risks associated with web applications and APIs, and to effectively manage these risks.

- To Be More Efficient In Development Processes: By learning about secure coding practices and best practices for web application and API security, employees can develop applications and APIs in a secure and efficient manner, reducing the risk of security vulnerabilities and increasing the reliability of the applications.

- Relying on SAST tools to detect application vulnerabilities is not enough as SAST tools can detect dangerous code patterns only in libraries and functions they are familiar with. An example: If your code uses less common or customized libraries for HTML rendering, there's a good chance the tool won't be able to identify XSS vulnerabilities.

WHY THIS COURSE

- Too many false positives is the main reason why security engineers struggle with SAST tools. Having a deep understanding og the best practices in secure coding helps.
- To Applying Secure Development Practices: To learn secure development practices, such as threat modeling, secure coding, and input validation, and apply these practices to real-world web application and API development scenarios.
- To Securing Web Applications and APIs: To learn how to secure web applications and APIs, including how to implement authentication, authorization, and encryption, and how to harden web applications and APIs.
- To Performing Security Assessments: To learn how to perform security assessments of web applications and APIs, including how to use security tools, such as Burp Suite, and how to identify and remediate security vulnerabilities.
- To Building Secure Development Processes: To learn how to build secure development processes, including how to incorporate security into the software development lifecycle, and how to perform regular security testing and vulnerability assessments.

WHO SHOULD ATTEND

- Web developers who want to improve their understanding of web application and API security and develop more secure applications.
- Security professionals who want to gain expertise in web application and API security and develop their skills in identifying and remedying security risks.
- IT managers who want to improve the security posture of their organization and ensure that their web applications and APIs are secure.
- DevOps engineers who want to understand the security considerations involved in web application and API development and ensure that their development processes are secure.
- Network administrators who need to understand how web applications fit into the overall security picture.
- Penetration testers who want to expand their skills and knowledge in web application and API security and perform more comprehensive security assessments.
- Compliance officers who want to understand the regulations and standards that apply to web application and API security and ensure that their organization is in compliance with these regulations.
- Project managers who need to understand how security affects project outcomes.

COURSE PREREQUISITE

- Participants should have a basic understanding of web development, including experience with HTML, CSS, JavaScript, and other web development technologies.
- Participants should have a basic understanding of networking and security concepts, such as IP addresses, ports, and firewalls.
- Knowledge of at least one programming language is recommended.
- Knowledge of at least one database is recommended