SEC101 – OWASP TOP 10 2021

Course Learning Objectives

Discover the top 10 most important web application vulnerabilities in the OWASP 2021 list, the most recent list in this standard. Covers all top 10 items, describing each vulnerability, why it happens from a business risk perspective, how hackers exploit it, and how best to defend against these issues.

Description

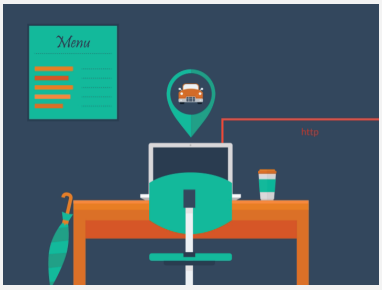
Students will learn the Top 10 threats as part of the OWASP Top 10 2021. This language agnostic course dives into concepts for web application threats, vulnerabilities and strategies to defend them. The OWASP top 10 list is an industry recognized list of vulnerabilities as dictated by the community, most recently in 2021.
The course engages students in learning about each of the Top 10 items, providing easy to understand business risks, concepts, news articles demonstrating how vulnerabilities have impacted organizations and best practices to defending against each of them.

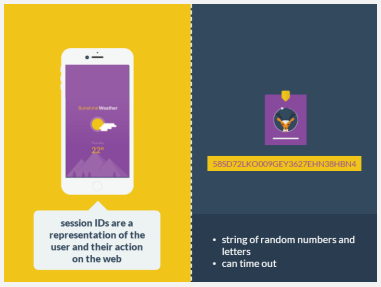
Audience

General Staff / Developers

Time Required

Tailored learning - 140 minutes total





SEC101 – OWASP TOP 10 2021

Course Outline

1. Broken Access Control

- About
- Authentication vs. Authorization
- About authorization
- Server-side checks
- Privilege escalation
- Insecure direct object reference
- Server-side session variables
- Missing functional level access control
- Page-level authorization
- Server-side request forgery (SSRF)
- Internal services authentication
- Cross-site request forgery (CSRF)
- Analyze your application for CSRF
- Defend against CSRF
- Risk of page-level authorization
- Programmed authorization

2. Cryptographic Failures

- About
- Exposed passwords
- Sensitive data exposure
- Strong cryptography
- Data sensitivity
- Clear-text communication
- Transport layer security
- Insecure storage
- Hashing for confidentiality
- Challenges to hashing
- Salts

3. Injection

- SQL injection
- Database errors
- Blind SQL
- Other forms of injection
- Unrestricted file upload
- Mad Libs analogy
- Query with bind parameters
- Defense in action
- Other defenses

4. Insecure Design

- About
- Poorly constructed threat model
- Strong threat modeling
- Methods
- Missing or ineffective business logic
- Adapt to SAST, DAST, and SCA
- SAST
- DAST
- SCA

5. Security Misconfiguration

- About misconfiguration
- Misconfiguration problems
- Newsflash
- Configuration activities
- Hardening
- Standardizing builds
- Verbose error messages
- Attack scenarios
- Generic error messages
- Patch management and audits
- Maintenance

6. Vulnerable and Outdated Components

- Using components with known vulnerabilities
- Newsflash
- Common vulnerabilities
- Catalogue dependencies
- Approval of external components
- Patch management process

SecurityCompass

SEC101 – OWASP TOP 10 2021

Course Outline

7. Identification and Authentication Failures

- About
- Factors of authentication and risks
- Weak password change control
- Strengthen forgotten password controls
- Brute-forcing and credential stuffing attacks
- Proper password strength control
- About HTTP and cookies
- Insecure session management
- Session hijacking
- Session timeout
- Network encryption
- Session fixation
- Newsflash
- Use multiple factors of authentication
- Account lockout

8. Software and Data Integrity Failures

- Software and data integrity failures
- Attack scenarios
- Mitigation against integrity failures
- How to mitigate

9. Security Logging and Monitoring Failures

- About
- Unlogged events
- Unmonitored activities and unprotected logs
- Detection
- Monitoring
- Establish an incident response and recovery plan

10. Server-Side Request Forgery (SSRF)

- About
- Common attack scenarios
- Best practices
- Best practices - Network layer
- Best practices - Application layer
- Mitigate SSRF attacks

SecurityCompass