SecureNinja
The Cybersecurity Experts

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

OWASP Top 10

In SecureNinja's OWASP Top 10 course, students will gain valuable insight into threats that are part of the OWASP Top 10 2019. This is a language-agnostic course that dives into the concepts around web application threats, vulnerabilities, and strategies to mitigate them. The course dives into each of the Top 10 items, providing easy-to-understand conceptual ideas, newsflashes demonstrating how these vulnerabilities have resulted in real exploits against organizations and recommendations for defending them.

Course Objectives

- Express the vulnerabilities and exploits facing modern web applications.
- Learn about the OWASP Top 10 2019 (updated for this year) covering all aspects including the vulnerability, why it happens, exploits, and defenses.
- See how real organizations have been affected by these exploits.

Topics covered

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Components with Known Vulnerabilities
- Unvalidated Redirects and Forwards

Course Length

- 2 Day Training

Class Formats

- Instructor-Led CBT/ Remote Training Available

Follow On Courses

- Web Application Exploiting and Defending