

		Short Link	Prerequisite	
eLearning Module to Course Mapping and Prerequisites			None	Programming Skills Basics of Web Apps
Awareness Modules				
100. Introduction to Application Security		http://AspectSecurity.com/elearning/100	✓	
101. Introduction to Verification		http://AspectSecurity.com/elearning/101	✓	
102. Introduction to the Secure Development Lifecycle		http://AspectSecurity.com/elearning/102	✓	
103. Introduction to Managing Software Security		http://AspectSecurity.com/elearning/103	✓	
110. Validating User Input		http://AspectSecurity.com/elearning/110	✓	
120. Enforcing Access Control		http://AspectSecurity.com/elearning/120	✓	
130. Authenticating Users		http://AspectSecurity.com/elearning/130	✓	
140. Error Handling and Security Logging		http://AspectSecurity.com/elearning/140	✓	
150. Protecting Sensitive Data		http://AspectSecurity.com/elearning/150	✓	
160. Securing Communications		http://AspectSecurity.com/elearning/160	✓	
170. Hardening Application Platforms and Frameworks		http://AspectSecurity.com/elearning/170	✓	
Technical Training, Advanced Verification, and Advanced Defense Modules				
Validating User Input				
211. Input Validation Strategy (minimize, on server, whitelist, global, business)		http://AspectSecurity.com/elearning/211	✓	
212. Preventing Injection Attacks (parameterized interfaces, encoding, validation)		http://AspectSecurity.com/elearning/212	✓	
213. Preventing XSS Vulnerabilities (reflected, stored, DOM)		http://AspectSecurity.com/elearning/213	✓	
214. Using Canonicalization and Encoding (incl. character sets and content-type)		http://AspectSecurity.com/elearning/214	✓	
215. Performing Secure File Upload and Download (filenames/paths, size, content, injection)		http://AspectSecurity.com/elearning/215	✓	
216. Preventing Header Injection (response splitting, download injection, defenses)		http://AspectSecurity.com/elearning/216	✓	
Enforcing Access Control				
221. Access Control Strategy (access control matrix, multiple layers)		http://AspectSecurity.com/elearning/221	✓	
222. Using Access Control in the Presentation Layer (forced browsing, single/multi-role)		http://AspectSecurity.com/elearning/222	✓	
223. Implementing URL Access Control (centralized, verb-based)		http://AspectSecurity.com/elearning/223	✓	
224. Implementing Business Function Access Control (single/multi-role)		http://AspectSecurity.com/elearning/224	✓	
225. Implementing Data Layer Access Control (ownership, access reference map)		http://AspectSecurity.com/elearning/225	✓	
226. Unsafe Redirects and Forwards		http://AspectSecurity.com/elearning/226	✓	
227. Clickjacking		http://AspectSecurity.com/elearning/227	✓	
Authenticating Users				
231. Authentication Strategy (repository, verification, identity)		http://AspectSecurity.com/elearning/231	✓	
232. Understanding HTTP Authentication Schemes (basic, forms, sessions, cookies)		http://AspectSecurity.com/elearning/232	✓	
233. Secure Session Management (logout, change password, forgot password, remember me)		http://AspectSecurity.com/elearning/233	✓	
234. Protecting Credentials (SSL, logout, harvesting, hashing, html, cookies)		http://AspectSecurity.com/elearning/234	✓	
235. Managing Identity within an Application (session, user object, backend)		http://AspectSecurity.com/elearning/235	✓	
236. Preventing Forged Requests (CSRF) (vectors, testing, tokens)		http://AspectSecurity.com/elearning/236	✓	
Error Handling and Security Logging				
241. Handling Security Errors and Detecting Attacks (exceptions, hiding implementation details,		http://AspectSecurity.com/elearning/241	✓	
242. Effective Security Logging (what to log, accountability, forensics)		http://AspectSecurity.com/elearning/242	✓	
Protecting Sensitive Data				
251. Introduction to Cryptography		http://AspectSecurity.com/elearning/251	✓	
252. Using Cryptography Securely		http://AspectSecurity.com/elearning/252	✓	
Securing Communications				
261. Using SSL (server certificate, client certificates, proxies, linking)		http://AspectSecurity.com/elearning/261	✓	
262. Securing Cookie Use (paths, domains, expiration, caching, secure, httponly)		http://AspectSecurity.com/elearning/262	✓	
263. Using Services Securely (SSL, authentication, authorization, validation, data protection)		http://AspectSecurity.com/elearning/263	✓	
Hardening Application Platforms and Frameworks				
271. Hardening Web Servers (fingerprinting, default files, attack surface, extension mapping)		http://AspectSecurity.com/elearning/271	✓	
272. Hardening Application Servers (default apps, extension mapping, SSL, timeouts, errors)		http://AspectSecurity.com/elearning/272	✓	
Language and Platform Specific Modules				
281. Introduction to Secure Coding for Rich Internet Applications		http://AspectSecurity.com/elearning/281	✓	✓
282. Introduction to Secure Coding for Ajax Applications		http://AspectSecurity.com/elearning/282	✓	✓
283. Introduction to Secure Coding for Java EE Applications		http://AspectSecurity.com/elearning/283	✓	✓
284. Introduction to Secure Coding for .NET Applications		http://AspectSecurity.com/elearning/284	✓	✓
Security Specialist Modules				
Application Security Verification				
410. Security Verification Methodology (Risk profiling, Security Architecture Review, Code Review, Pen		http://AspectSecurity.com/elearning/410	✓	
411. Effective Security Testing ((Manual and Tools) Browser, Proxy and Scanner)		http://AspectSecurity.com/elearning/411	✓	
412. Effective Security Code Review (Manual and Tools) IDE (Eclipse), Grep, Static Analysis		http://AspectSecurity.com/elearning/412	✓	✓
420. Threat Modeling and Security Architecture Review		http://AspectSecurity.com/elearning/420	✓	
Managing Application Security				
450. Integrating Security into Waterfall Projects		http://AspectSecurity.com/elearning/450	✓	
460. Integrating Security into Agile Projects		http://AspectSecurity.com/elearning/460	✓	