Application Security
Certification & Training Guide

A Comprehensive Resource for AppSec Professionals

Document Purpose

This guide provides a practical ranking of certifications and courses most relevant to Application Security professionals, including recommended learning sequences aligned with typical AppSec responsibilities: secure SDLC, vulnerability triage, code review, CI/CD security gates, and cloud-native delivery.

Coverage Areas

- OffSec Certifications
- OWASP Frameworks
- Vendor Certifications
- SANS Courses
- Cloud-Native Security
- Learning Paths

Version 1.0

January 14, 2026

Contents

1 Executive Summary

This document provides a comprehensive guide to certifications and training programs most relevant to Application Security (AppSec) professionals. The guide is structured to help security practitioners at all levels identify the most appropriate learning path based on their current role, responsibilities, and career objectives.

1.1 Document Organization

The guide is organized into four major sections:

1. **OffSec Certifications Ranked by AppSec Relevance** — A tiered ranking of Offensive Security certifications based on their direct applicability to AppSec work, from Tier 1 (highest impact) to certifications that are typically outside AppSec scope.
2. **High-Value Alternatives Outside OffSec** — Comprehensive coverage of certifications and training programs from other providers including SANS Institute, ISC2, OWASP, PortSwigger, GIAC, CNCF, and GitHub.
3. **Recommended Learning Sequence** — A structured progression path designed for maximum AppSec return on investment with minimal detours.
4. **Role-Based Selection Guide** — Quick-reference mappings of certifications to specific AppSec roles and responsibilities.

1.2 Key Recommendations at a Glance

For AppSec professionals seeking the highest-impact certifications:

- **For Web Application Security Depth:** OSWE (WEB-300), OSWA (WEB-200), Burp Suite Certified Practitioner
- **For Secure SDLC Expertise:** ISC2 CSSLP, OWASP ASVS, OWASP SAMM
- **For DevSecOps/Cloud-Native:** SANS SEC540, CKS, GitHub Advanced Security Certification
- **For Foundational Skills:** PortSwigger Web Security Academy, OWASP Top 10

2 OffSec Certifications: Ranked by AppSec Relevance

Offensive Security (OffSec) offers a range of certifications that vary significantly in their relevance to Application Security work. This section provides a tiered ranking to help AppSec professionals prioritize their certification investments.

2.1 Tier 1: Direct AppSec Impact

Tier 1 certifications have the strongest alignment with core AppSec responsibilities including web application assessment, code review, vulnerability analysis, and exploit understanding from a source-level perspective.

2.1.1 OSWE — Offensive Security Web Expert (WEB-300)

Course Code	WEB-300
Certification	OSWE (Offensive Security Web Expert)
Primary Focus	Advanced white-box web application security assessment
Key Skills	• White-box web assessment methodology • Vulnerability root cause analysis from source code • Exploit development in source-level context • Advanced authentication bypass techniques • Server-side attack development
AppSec Alignment	**Highest** — Best alignment to advanced AppSec work. Emphasizes understanding vulnerabilities at the source code level, which directly translates to secure code review capabilities and remediation guidance.
Ideal Candidates	Senior AppSec Engineers, Security Architects, Code Review Specialists
Official Link	OffSec WEB-300 Course Page

Why OSWE is Tier 1 for AppSec:

The OSWE certification stands out as the most AppSec-aligned OffSec offering because it emphasizes white-box assessment—examining application source code to identify, understand, and exploit vulnerabilities. This approach directly mirrors the work of AppSec professionals who must review code, understand vulnerability root causes, and provide actionable remediation guidance to development teams.

Unlike black-box penetration testing certifications, OSWE teaches candidates to think like both an attacker and a defender by understanding how vulnerabilities manifest in actual code. This dual perspective is invaluable for AppSec engineers embedded with development teams who must translate security findings into specific code-level fixes.

2.1.2 OSWA — Offensive Security Web Assessor (WEB-200)

Course Code	WEB-200
Certification	OSWA (Offensive Security Web Assessor)
Primary Focus	Foundational web application security assessment
Key Skills	• Cross-Site Scripting (XSS) identification and exploitation • SQL Injection (SQLi) attack techniques • Server-Side Request Forgery (SSRF) • Server-Side Template Injection (SSTI) • Authentication and session management testing • Web application enumeration and reconnaissance
AppSec Alignment	**Very High** — Strong foundation for AppSec analysts and engineers who need consistent skill at finding, validating, and explaining common web vulnerabilities.
Ideal Candidates	AppSec Analysts, Junior-to-Mid AppSec Engineers, Security Testers
Official Link	OffSec WEB-200 Course Page

Why OSWA is Tier 1 for AppSec:

OSWA provides the essential foundational skills that every AppSec professional needs. The certification focuses on the most common and impactful web vulnerabilities—the same issues that AppSec teams encounter daily during vulnerability triage, security assessments, and developer coaching sessions.

The practical, hands-on nature of the OSWA exam ensures that certified professionals can not only identify vulnerabilities but also reproduce and validate them—a critical skill for effective vulnerability triage and remediation guidance.

2.2 Tier 2: AppSec-Adjacent with High Utility

Tier 2 certifications provide valuable broader attacker tradecraft knowledge that enhances AppSec effectiveness, particularly for professionals whose responsibilities extend beyond pure web application security.

2.2.1 OSCP / OSCP+ — Offensive Security Certified Professional (PEN-200)

Course Code	PEN-200
Certification	OSCP (Offensive Security Certified Professional) / OSCP+
Primary Focus	General penetration testing methodology
Key Skills	• Network penetration testing • Active Directory attacks • Privilege escalation (Linux and Windows) • Lateral movement techniques • Post-exploitation methodology • Basic web application testing
AppSec Alignment	**Moderate-High** — Less web-app-focused than OSWA/OSWE, but provides valuable exploitation intuition for severity assessment and prioritization. Particularly useful for platform-integrated AppSec roles.
Best Use Cases	• CI/CD pipeline security • Infrastructure-adjacent AppSec • Identity and access management security • Understanding lateral movement for impact assessment
Official Links	OffSec PEN-200 Course Page OSCP+ Standalone Exam

Why OSCP is Tier 2 for AppSec:

While OSCP is often considered the "gold standard" for penetration testing certifications, its relevance to pure AppSec work is more limited than OSWA or OSWE. However, for AppSec professionals whose responsibilities include CI/CD security, infrastructure security, or who need to understand how application vulnerabilities can lead to broader compromise, OSCP provides invaluable context.

The OSCP+ variant offers a maintenance pathway for professionals who want to demonstrate continued competency without retaking the full course.

2.2.2 KLCP — Kali Linux Certified Professional (PEN-103)

Course Code	PEN-103
Certification	KLCP (Kali Linux Certified Professional)
Primary Focus	Kali Linux proficiency and security tooling
AppSec Alignment	**Low-Moderate** — Useful for establishing baseline tooling fluency, but largely optional for AppSec professionals who are already productive with security testing tools.
Recommendation	Consider only if you need a structured approach to Kali Linux proficiency; otherwise, practical experience with tools like Burp Suite and OWASP ZAP is sufficient.

2.3 Tier 3: Usually Not Priority for AppSec

Tier 3 certifications are excellent for their intended purposes but typically represent overinvestment for most AppSec roles unless specific job requirements dictate otherwise.

2.3.1 Advanced Offensive Certifications

Certification	Focus Area	AppSec Relevance
OSEP	Evasion Techniques and Breaching Defenses	Red Team / Exploit Dev
OSED	Windows User Mode Exploit Development	Exploit Development
OSEE	Advanced Windows Exploitation	Expert Exploit Research

Assessment: These certifications are excellent for red team and exploit development tracks. However, for most AppSec roles, they represent significant time investment in areas that rarely translate to daily AppSec deliverables. Consider only if your role specifically involves high-end security research or internal offensive R&D.

2.3.2 Defense and Response Certifications

Certification	Focus Area	AppSec Relevance
OSDA	Security Operations and Defense Analysis	SOC / Blue Team
OSTH	Threat Hunting	Threat Intelligence
OSIR	Incident Response	IR / DFIR

Assessment: These certifications may be valuable for AppSec leaders who also own detection and response readiness. However, they are not the most efficient path for leveling up core AppSec deliverables such as secure code review, vulnerability triage, or secure SDLC implementation.

2.4 Not AppSec-Focused (Deprioritize)

Certification	Focus Area	Recommendation
OSWP	Wireless Security Assessment	Skip unless product environment requires wireless security expertise

3 High-Value Certifications and Training Outside OffSec

Beyond OffSec, numerous high-quality certifications and training programs offer significant value for AppSec professionals. This section organizes alternatives by focus area and provides detailed assessments of each option.

3.1 Web Application and API Security Depth

These certifications focus on practical, hands-on web application security skills that directly translate to AppSec work.

3.1.1 PortSwigger Web Security Academy

Provider	PortSwigger
Format	Free online learning platform with structured learning paths
Key Features	• Comprehensive coverage of web vulnerabilities • Interactive labs with real vulnerability exploitation • Progressive difficulty from apprentice to expert • Regular content updates reflecting current threats • Mystery lab challenges for advanced practice
AppSec Value	**Excellent** — Pairs exceptionally well with any AppSec role that involves validating findings, reviewing fixes, or coaching developers on secure coding practices.
Cost	Free
Official Link	Web Security Academy Learning Paths

3.1.2 Burp Suite Certified Practitioner (BSCP)

Provider	PortSwigger
Certification	BSCP (Burp Suite Certified Practitioner)
Exam Format	Practical examination requiring exploitation of real vulnerabilities
Key Skills Validated	• Real-world web exploitation workflow • Burp Suite proficiency across all major features • Vulnerability chaining and complex attack scenarios • Time-pressured security assessment
AppSec Value	**Very High** — Provides practical validation of web security skills and tool proficiency. Highly respected credential that demonstrates hands-on capability.
Official Link	Burp Suite Certified Practitioner

3.1.3 SANS SEC522: Securing Web Applications, APIs, and Microservices

Provider	SANS Institute
Course Code	SEC522
Duration	6 days
Primary Focus	Defensive web application security for modern architectures
Key Topics	• HTTP protocol security • API security patterns and anti-patterns • Microservices security architecture • Cloud workload protection • Authentication and authorization frameworks • Security testing integration
AppSec Value	**Excellent** — Highly aligned with modern AppSec responsibilities. Provides both offensive understanding and defensive implementation guidance.
Official Link	SANS SEC522 Course Page

3.1.4 SANS SEC542: Web App Penetration Testing and Ethical Hacking

Provider	SANS Institute
Course Code	SEC542
Duration	6 days
Primary Focus	Offensive web application penetration testing
Key Skills	• Web application penetration testing methodology • Vulnerability reproduction and validation • Professional security assessment reporting • Tool proficiency (Burp Suite, OWASP ZAP, etc.)
AppSec Value	**High** — More pentest-oriented than SEC522, but highly useful for AppSec staff who need to reproduce, validate, and precisely explain security issues to developers.
Official Link	SANS SEC542 Course Page

3.2 Secure SDLC and AppSec Program Design

These certifications and frameworks focus on the programmatic aspects of application security—building mature programs, defining requirements, and integrating security throughout the software development lifecycle.

3.2.1 ISC2 CSSLP: Certified Secure Software Lifecycle Professional

Provider	ISC2
Certification	CSSLP
Prerequisites	4 years cumulative work experience in software development lifecycle
Domains Covered	• Secure Software Concepts • Secure Software Requirements • Secure Software Architecture and Design • Secure Software Implementation • Secure Software Testing • Secure Software Deployment, Operations, and Maintenance • Secure Software Supply Chain • Secure Software Lifecycle Management
AppSec Value	**Excellent** — One of the clearest "secure software lifecycle" credentials available. Ideal for AppSec engineers, architects, and program owners who need to demonstrate comprehensive SDLC security knowledge.
Official Link	ISC2 CSSLP Certification Page

3.2.2 OWASP Application Security Verification Standard (ASVS)

Provider	OWASP Foundation
Type	Security Standard / Framework (not a certification)
Current Version	ASVS 4.0
Purpose	Provides a basis for testing web application security controls and establishing verifiable security requirements
Verification Levels	• **Level 1:** Low assurance — opportunistic vulnerabilities • **Level 2:** Standard assurance — most applications • **Level 3:** High assurance — critical applications
Key Use Cases	• Defining security requirements for applications • Creating security testing checklists • Establishing vendor security requirements • Measuring security maturity
AppSec Value	**Essential** — The best practical standard for translating security into verifiable requirements for applications and APIs. Every AppSec professional should be familiar with ASVS.
Official Link	OWASP ASVS Project Page

3.2.3 OWASP Software Assurance Maturity Model (SAMM)

Provider	OWASP Foundation
Type	Maturity Model / Framework (not a certification)
Purpose	Framework for building and maturing an AppSec program with measurable activities and outcomes
Business Functions	• **Governance:** Strategy, policy, compliance, education • **Design:** Threat modeling, security requirements, security architecture • **Implementation:** Secure build, secure deployment, defect management • **Verification:** Architecture assessment, requirements testing, security testing • **Operations:** Incident management, environment management, operational management
AppSec Value	**Excellent** — Essential for building or maturing an AppSec program. Provides metrics, maturity levels, and roadmap guidance for program development.
Official Link	OWASP SAMM Project Page

3.2.4 OWASP Top 10

Provider	OWASP Foundation
Type	Awareness Document / Risk Framework
Current Version	OWASP Top 10:2021 (2025 update pending)
Purpose	Standard awareness document for developers and web application security, representing broad consensus about the most critical security risks
Current Categories	• A01: Broken Access Control • A02: Cryptographic Failures • A03: Injection • A04: Insecure Design • A05: Security Misconfiguration • A06: Vulnerable and Outdated Components • A07: Identification and Authentication Failures • A08: Software and Data Integrity Failures • A09: Security Logging and Monitoring Failures • A10: Server-Side Request Forgery (SSRF)
AppSec Value	**Foundational** — Current top-level risk framing essential for developer education, policy development, and vulnerability prioritization.
Official Link	OWASP Top Ten Project Page

3.3 CI/CD, Cloud-Native, and Platform Security

For AppSec professionals working in DevSecOps environments, these certifications address security in modern delivery pipelines and cloud-native architectures.

3.3.1 SANS SEC540: Cloud Native Security and DevSecOps Automation

Provider	SANS Institute
Course Code	SEC540
Duration	5 days
Primary Focus	Security automation in cloud-native and DevSecOps environments
Key Topics	• CI/CD pipeline security • Kubernetes security • Infrastructure as Code (IaC) security • Container security • Cloud-native security controls • Security automation and tooling • Supply chain security
AppSec Value	**Excellent** — Directly relevant if your AppSec responsibilities include CI/CD gates, Kubernetes environments, cloud-native delivery, and security controls in pipelines.
Official Link	SANS SEC540 Course Page

3.3.2 CKS: Certified Kubernetes Security Specialist

Provider	Cloud Native Computing Foundation (CNCF)
Certification	CKS
Prerequisites	Must hold valid CKA (Certified Kubernetes Administrator)
Exam Format	Performance-based exam in live Kubernetes environment
Domains Covered	• Cluster Setup (10%) • Cluster Hardening (15%) • System Hardening (15%) • Minimize Microservice Vulnerabilities (20%) • Supply Chain Security (20%) • Monitoring, Logging, and Runtime Security (20%)
AppSec Value	**High** — Essential for AppSec professionals operating in Kubernetes environments. Focuses on securing container-based applications across build, deploy, and runtime phases.
Official Link	CNCF CKS Certification Page

3.4 Toolchain-Specialized Certifications

3.4.1 GitHub Advanced Security Certification

Provider	GitHub / Microsoft
Certification	GitHub Advanced Security
Primary Focus	Implementation and administration of GitHub Advanced Security (GHAS) features
Key Topics	• Code scanning configuration and management • Secret scanning setup and response • Dependency security (Dependabot) • Security policies and PR checks • Enterprise-scale GHAS deployment • Security alert triage and remediation workflows
AppSec Value	**High (Conditional)** — Directly aligned if you are implementing or managing GHAS at scale. High ROI for organizations using GitHub as their primary development platform.
Official Link	Microsoft Learn: GitHub Advanced Security

3.5 GIAC Web Security Certifications

3.5.1 GWEB: GIAC Certified Web Application Defender

Provider	GIAC
Certification	GWEB
Focus	Defensive web application security
Key Areas	Securing web applications, identifying vulnerabilities, implementing defensive measures
AppSec Value	**High** — Defensive web AppSec credential that validates understanding of secure web application development and deployment.
Official Link	GIAC GWEB Certification Page

3.5.2 GWAPT: GIAC Web Application Penetration Tester

Provider	GIAC
Certification	GWAPT
Focus	Offensive web application testing
Key Areas	Web application penetration testing methodology and techniques
AppSec Value	**Moderate-High** — More offensive/testing oriented, but relevant for AppSec professionals who need strong validation and methodology skills.
Official Link	GIAC GWAPT Certification Page

4 Recommended Learning Sequence for AppSec

This section presents an optimized learning sequence designed for maximum AppSec return on investment with minimal detours. The sequence is structured in progressive phases, allowing professionals to build foundational skills before advancing to specialized areas.

4.1 Phase 1: Foundation and Skill Development

Order	Resource	Objective
1a	OWASP Top 10:2021	Establish baseline understanding of critical web application risks
1b	PortSwigger Web Security Academy	Build hands-on skills through structured practice; complete relevant learning paths

Rationale: This combination provides zero-cost foundational knowledge. The OWASP Top 10 frames the risk landscape while PortSwigger Academy provides the practical skill development through interactive labs. Together, they prepare candidates for more advanced certifications.

Time Investment: 2–4 months depending on prior experience

4.2 Phase 2: Web Assessment Certification

Order	Certification	Objective
2	OSWA (WEB-200)	Solidify web assessment fundamentals with hands-on certification validation

Rationale: OSWA builds on the foundation from Phase 1 and provides formal certification in web application security assessment. The practical exam format ensures skills are truly internalized, not just theoretical.

Time Investment: 2–3 months

4.3 Phase 3: Defensive Architecture

Order	Course	Objective
3	SANS SEC522	Add web, API, and microservices defense perspective; understand security from the builder's viewpoint

Rationale: After building offensive understanding through Phases 1 and 2, SEC522 adds the defensive lens needed for effective AppSec work. This course bridges the gap between finding vulnerabilities and architecting secure solutions.

Time Investment: 1 week intensive + study time

4.4 Phase 4: Advanced Specialization

Choose one path based on role focus:

Path	Certification	Best For
4A	OSWE (WEB-300)	Deep white-box AppSec; code review specialists
4B	BSCP	Practical Burp-centric validation; testing-focused roles

Rationale: Both options provide “proof of depth.” OSWE is ideal for roles emphasizing source code review and secure architecture, while BSCP validates practical testing proficiency.

Time Investment: 3–6 months depending on path

4.5 Phase 5: Program and Process Maturity

Order	Resource	Objective
5a	OWASP ASVS	Formalize security requirements for applications
5b	OWASP SAMM	Build program maturity model and metrics
5c	ISC2 CSSLP	Obtain SDLC-oriented credential (optional based on role)

Rationale: These resources transition focus from individual technical skills to program-level effectiveness. ASVS and SAMM are practical frameworks, while CSSLP provides formal certification recognition.

Time Investment: 2–4 months

4.6 Phase 6: Cloud-Native and DevSecOps (Conditional)

Pursue if your environment is cloud-native, Kubernetes-based, or heavily automated.

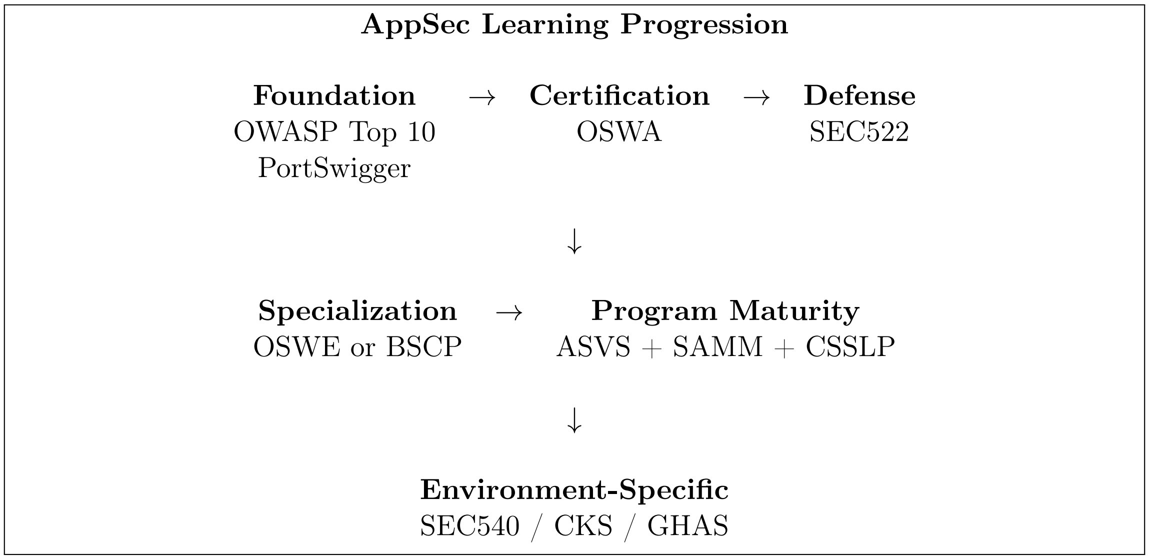
Order	Certification	Objective
6a	SANS SEC540	Cloud-native security and DevSecOps automation
6b	CKS	Kubernetes-specific security (requires CKA prerequisite)

4.7 Phase 7: Toolchain Certification (Conditional)

Pursue if GitHub Advanced Security is central in your toolchain.

Order	Certification	Objective
7	GitHub Advanced Security	GHAS implementation and administration at scale

4.8 Visual Learning Path



AppSec Learning Progression

Foundation → **Certification** → **Defense**

OWASP Top 10 OSWA SEC522

PortSwigger

↓

Specialization → **Program Maturity**

OSWE or BSCP ASVS + SAMM + CSSLP

↓

Environment-Specific

SEC540 / CKS / GHAS

5 Role-Based Certification Selection Guide

This section provides quick-reference certification recommendations based on specific AppSec roles and responsibilities.

5.1 AppSec Engineer (Embedded with Development Teams)

Primary Responsibilities	Secure design, code reviews, security standards, developer coaching, threat modeling
Priority Certifications	• OSWE (WEB-300) — White-box assessment and code review • SEC522 — Defensive architecture for modern apps • CSSLP — SDLC security credential
Essential Frameworks	ASVS (security requirements), SAMM (program maturity)
Time to Competency	12–18 months for full track

5.2 AppSec Analyst (Triage and Validation Focus)

Primary Responsibilities	Vulnerability triage, finding validation, remediation coaching, tool administration
Priority Certifications	• OSWA (WEB-200) — Web assessment fundamentals • BSCP — Practical validation skills • GitHub Advanced Security — If running GHAS workflows
Essential Training	PortSwigger Web Security Academy (complete all relevant learning paths)
Time to Competency	8–12 months for full track

5.3 DevSecOps / Platform AppSec

Primary Responsibilities	CI/CD security gates, Kubernetes security, supply chain security, pipeline automation
Priority Certifications	• SEC540 — Cloud-native and DevSecOps • CKS — Kubernetes security (if K8s environment) • GitHub Advanced Security — Pipeline integration
Optional Addition	OSCP/OSCP+ — Broader attacker context for impact assessment
Time to Competency	10–14 months for full track

5.4 AppSec Program Owner / Manager

Primary Responsibilities	Program strategy, metrics and reporting, vendor management, policy development, team leadership
Priority Certifications	• CSSLP — SDLC leadership credential • SEC522 — Technical foundation for leadership
Essential Frameworks	• OWASP SAMM — Program maturity model • OWASP ASVS — Requirements framework • OWASP Top 10 — Risk communication
Time to Competency	6–10 months for framework mastery

6 Comprehensive Reference Tables

6.1 Complete Certification Comparison Matrix

Certification	Provider	Focus	AppSec Tier	Best For
OSWE	OffSec	White-box Web	Tier 1	Code review, secure architecture
OSWA	OffSec	Web Assessment	Tier 1	Vulnerability validation, triage
OSCP/OSCP+	OffSec	General Pentest	Tier 2	Platform security, broader context
BSCP	PortSwigger	Web Testing	Tier 1	Practical validation skills
SEC522	SANS	Web Defense	Tier 1	Secure architecture, APIs
SEC540	SANS	DevSecOps	Tier 1*	CI/CD, cloud-native environments
SEC542	SANS	Web Pentest	Tier 2	Testing methodology
CSSLP	ISC2	SDLC	Tier 1	Program ownership, architecture
GWEB	GIAC	Web Defense	Tier 2	Defensive web security
GWAPT	GIAC	Web Pentest	Tier 2	Testing validation
CKS	CNCF	Kubernetes	Tier 1*	K8s environments only
GHAS Cert	GitHub	Toolchain	Tier 1*	GHAS implementations only

** Tier 1 conditional on environment/toolchain alignment*

6.2 Official Resource Links

Resource	Official URL
OffSec WEB-300 (OSWE)	https://www.offsec.com/courses/web-300/
OffSec WEB-200 (OSWA)	https://www.offsec.com/courses/web-200/
OffSec PEN-200 (OSCP)	https://www.offsec.com/courses/pen-200/
OffSec OSCP+	https://www.offsec.com/products/oscp-plus
PortSwigger Academy	https://portswigger.net/web-security/learning-paths

Resource	**Official URL**
BSCP Certification	https://portswigger.net/web-security/certification
SANS SEC522	https://www.sans.org/cyber-security-courses/application-security-securing-web-apps-api-microservices
SANS SEC540	https://www.sans.org/cyber-security-courses/cloud-native-security-devsecops-automation
SANS SEC542	https://www.sans.org/cyber-security-courses/web-app-penetration-testing-ethical-hacking
ISC2 CSSLP	https://www.isc2.org/certifications/csslp
OWASP ASVS	https://owasp.org/www-project-application-security-verification-st
OWASP SAMM	https://owasp.org/www-project-samm/
OWASP Top 10	https://owasp.org/www-project-top-ten/
CNCF CKS	https://www.cncf.io/training/certification/cks/
GitHub Advanced Security	https://learn.microsoft.com/en-us/credentials/certifications/github-advanced-security/
GIAC GWEB	https://www.giac.org/certification/certified-web-application-defender-gweb
GIAC GWAPT	https://www.giac.org/certification/web-application-penetration-tester-gwapt

A Appendix: Acronym Reference

Acronym	Full Name
AppSec	Application Security
ASVS	Application Security Verification Standard
BSCP	Burp Suite Certified Practitioner
CI/CD	Continuous Integration / Continuous Deployment
CKA	Certified Kubernetes Administrator
CKS	Certified Kubernetes Security Specialist
CNCF	Cloud Native Computing Foundation
CSSLP	Certified Secure Software Lifecycle Professional
DFIR	Digital Forensics and Incident Response
DevSecOps	Development, Security, and Operations
GHAS	GitHub Advanced Security
GIAC	Global Information Assurance Certification
GWAPT	GIAC Web Application Penetration Tester
GWEB	GIAC Certified Web Application Defender
IaC	Infrastructure as Code
IR	Incident Response
ISC2	International Information System Security Certification Consortium
K8s	Kubernetes
KLCP	Kali Linux Certified Professional
OSCP	Offensive Security Certified Professional
OSDA	Offensive Security Defense Analyst
OSED	Offensive Security Exploit Developer
OSEE	Offensive Security Exploitation Expert
OSEP	Offensive Security Experienced Penetration Tester
OSIR	Offensive Security Incident Responder
OSTH	Offensive Security Threat Hunter
OSWA	Offensive Security Web Assessor
OSWE	Offensive Security Web Expert
OSWP	Offensive Security Wireless Professional
OWASP	Open Worldwide Application Security Project
R&D	Research and Development
ROI	Return on Investment
SAMM	Software Assurance Maturity Model
SANS	SysAdmin, Audit, Network, and Security
SDLC	Software Development Lifecycle
SOC	Security Operations Center
SQLi	SQL Injection
SSRF	Server-Side Request Forgery
SSTI	Server-Side Template Injection
XSS	Cross-Site Scripting