7 CERTIFICAZIONI PROFESSIONALI

7.1 GIAC Secure Software Programmer (GSSP) Certification

GSSP Certification Exam coinvolge l'Istituto SANS, CERT CC, diverse agenzie governative statunitensi e aziende leader negli Stati Uniti, Giappone, India e Germania. SANS è il certificatore.

URL	https://www.giac.org/

Questa certificazione si concentra sulle questioni reali che stanno dietro le vulnerabilità più comuni e i problemi di sicurezza applicativi.

Gli esami riguardano le tecniche e i linguaggi specifici (Java o .NET) e molte delle domande usano esempi di codice reale. Gli esami aiutano le organizzazioni a soddisfare quattro obiettivi, che sono:

- identificare carenze nella conoscenza della sicurezza dei programmatori in-house e aiutare gli individui a colmare il divario;
- assicurarsi che i programmatori in outsourcing abbiano adeguate competenze Secure-coding;
- nominare nuovi dipendenti che non hanno bisogno di formazione correttiva in programmazione sicura;
- assicurarsi che ogni grande progetto di sviluppo abbia almeno una persona con avanzate capacità di programmazione sicura.

Dopo l'acquisizione di questa certificazione, i programmatori saranno a conoscenza dei difetti più comuni di sicurezza che si trovano in ambienti di programmazione specifici (Java o .NET), e sapranno come evitare questi problemi dovuti principalmente alla vulnerabilità delle applicazioni.

Web Applicaton Defender. La certificazione GIAC Web Application Defender consente ai candidati di acquisire le conoscenze e le competenze di sicurezza necessarie per gestire gli errori comuni delle applicazioni Web che portano alla maggior parte dei problemi di sicurezza.

La certificazione GSSP rimane valida per quattro anni.

7.2 International Council of E-Commerce Consultants (EC-Council) Certifications

L'EC-Council è un'organizzazione member-based che certifica gli individui in varie competenze e-business e di sicurezza delle informazioni.

URL	http://www.eccouncil.org
Contact Method	http://www.eccouncil.org/contact_us.aspx Email, web form, phone and address
Country of HQ location	US
Geographic Scope	International
Type	Industry

I diversi tipi di certificazione offerti dal EC-Council nelle aree SSE-correlate sono descritti nelle sezioni che seguono.

7.3 Certified Ethical Hacker (CEH)

Si tratta di una certificazione riconosciuta e accreditata in conformità ANSI 17024. Il corso si pone l'obiettivo di formare una nuova figura professionale, l'hacker etico, che si dedichi alla difesa della sicurezza informatica. Il principio didattico è di apprendere da un lato le tecniche di intrusione e violazione informatica e dall'altro lato le metodologie di difesa da queste stesse tecniche. CEH dispone di 26 moduli, di cui i seguenti sono collegati a SSE:

- Module 17: Web Application Vulnerabilities
- Module 19: SQL Injection
- Module 24: Buffer Overflows
- Module 26: Penetration Testing Methodologies

7.4 Certified Security Analyst (ECSA)

La certificazione ECSA completa la certificazione CEH (vedi sopra) esplorando la fase analitica di hacking etico. ECSA fa un ulteriore passo in avanti, rispetto a CEH, approfondendo come analizzare l'esito di questi strumenti e tecnologie. Attraverso metodi e tecniche di *penetration testing* la certificazione ECSA aiuta i candidati a effettuare le valutazioni necessarie per identificare e mitigare efficacemente i rischi per la sicurezza delle informazioni dell'infrastruttura.

ECSA ha 47 moduli, di cui i seguenti sono collegati a SSE:

- Module 10: Advanced Exploits and Tools
- Module 11: Penetration Testing Methodologies
- Module 27: Stolen Laptop, PDAs and Cellphones Penetration Testing
- Module 28: Application Penetration Testing
- Module 40: Security Patches Penetration Testing
- Module 41: Data Leakage Penetration Testing
- Module 42: Penetration Testing Deliverables and Conclusion
- Module 43: Penetration Testing Report and Documentation Writing
- Module 44: Penetration Testing Report Analysis
- Module 45: Post-Testing Actions

7.5 Certified Secure Programmer (ECSP)

La certificazione ECSP è destinata ai programmatori e agli sviluppatori software è ha allo scopo di codificare e sviluppare applicazioni sicure durante tutto il ciclo di vita del software.

ECSP dispone di 33 moduli, di cui i seguenti sono collegati a SSE:

- Module 01: Introduction to Secure Coding
- Module 02: Designing Secure Architecture
- Module 03: Cryptography
- Module 04: Buffer Overflows
- Module 05: Secure C and C++ Programming
- Module 06: Secure Java and JSP Programming
- Module 07: Secure Java Script and VBScript Programming
- Module 08: Secure Microsoft.NET Programming

- Module 09: Secure PHP Programming
- Module 10: Securing Applications from Bots
- Module 11: Secure SQL Server Programming
- Module 12: SQL Rootkits
- Module 13: Secure Application Testing
- Module 14: VMware Remote Recording and Debugging
- Module 15: Writing Secure Documentation and Error Messages
- Module 16: Secure ASP Programming
- Module 17: Secure PERL Programming
- Module 18: Secure XML, Web Services and AJAX Programming
- Module 19: Secure RPC, ActiveX and DCOM Programming
- Module 20: Secure Linux Programming
- Module 21: Secure Linux Kernel Programming
- Module 22: Secure Xcode Programming
- Module 23: Secure Oracle PL/SQL Programming
- Module 24: Secure Network Programming
- Module 25: Windows Socket Programming
- Module 26: Writing Shellcodes
- Module 27: Writing Exploits
- Module 28: Programming Port Scanners and Hacking Tools
- Module 29: Secure Mobile Phone and PDA Programming
- Module 30: Secure Game Designing
- Module 31: Securing E-Commerce Applications
- Module 32: Software Activation, Piracy Blocking and Automatic Updates
- Module 33: PCI Compliance and Secure Programming

7.6 Certified Software Security Lifecycle Professional (CSSLP) and Certified Information Systems Security Professional (CISSP)

Il CSSLP ha lo scopo di convalidare le conoscenze di sviluppo software sicuro e di buone pratiche. Il CSSLP è un codice in lingua neutrale e applicabile a chiunque sia coinvolto nel SDLC.

La certificazione è rilasciata dal Consorzio di Certificazione Internazionale Information Systems Security, (ISC)², un'organizzazione globale no-profit specializzata nella formazione e certificazione di professionisti della sicurezza informatica. Esso fornisce prodotti di formazione vendor-neutral.

URL	https://www.isc2.org/csslp/default.aspx
Contact Method	CSSLP Contact [https://www.isc2.org/csslp/default.aspx] Web form CISSP Contact [https://www.isc2.org/cissp/default.aspx] Web form General Contact [https://www.isc2.org/contactus/default.aspx] Web form, phone and address
Country of HQ location	US
Geographic Scope	International
Type	Industry (no profit)

In accordo al (ISC)², il CSSLP è progettato per:

- Stabilire le migliori pratiche, al fine di limitare la proliferazione delle vulnerabilità di sicurezza che derivano da processi di sviluppo insufficienti
- attestare la capacità professionista di mitigare i problemi di sicurezza e dei rischi che circondano lo sviluppo di applicazioni in tutto il SDLC, dalla specifica e progettazione alla realizzazione e manutenzione

I seguenti domini compongono il CSSLP Common Body of Knowledge (CBK), che si concentra sulla necessità di integrare la sicurezza nel SDLC:

- Secure Software Concepts: implicazioni di sicurezza nello sviluppo di software.
- Secure Software Requirements: catturare i requisiti di sicurezza nei raccolta dei requisiti di fase
- Secure Software Design: tradurre i requisiti di sicurezza in elementi di design di applicazioni
- Secure Software Implementation/Coding: unit testing per la funzionalità sicurezza e la resilienza contro gli attacchi, e lo sviluppo di codice sicuro e sfruttare la mitigazione
- Secure Software Testing: test integrati di quality assurance per la funzionalità sicurezza e la resilienza contro gli attacchi
- Software Acceptance: implicazioni per la sicurezza in fase di accettazione del software
- Software Deployment, Operations, Maintenance and Disposal: problemi di sicurezza intorno operazioni di steady-state e la gestione del software.

La qualificazione CSSLP è valida per tre anni, dopo di che deve essere rinnovata. Può essere rinnovata rifacendo l'esame o, più comune, con l'acquisizione di crediti formativi professionali (CPE).

Il CISSP, un altro programma di certificazione da (ISC)² con regole simili, è destinato ai professionisti che sviluppano politiche e procedure in materia di sicurezza delle informazioni.

7.7 Certificazioni ISACA (CISA, CISM, CRISC)

Le certificazioni ISACA sono accettate e riconosciute a livello globale e sono destinate al management IT per rafforzare le loro competenze negli ambiti: audit IT, sicurezza, governance e gestione dei rischi. Nel dettaglio:

- Certified Information Systems Auditor (CISA). Certifica le competenze necessarie ad amministrare e controllare l'IT dell'azienda e a compiere un effettivo audit sulla sicurezza dell'organizzazione. La certificazione CISA ha per oggetto le seguenti aree: Processo di audit dei sistemi informatici; IT Governance e Management; Acquisizione, sviluppo e implementazione dei sistemi informatici; Operazioni, mantenimento e supporto dei servizi informatici; Protezione delle risorse informatiche.
- Certified in Risk and Information Systems Control (CRISC), prepara e abilita i professionisti IT alle sfide IT e alla gestione dei rischi aziendali. La certificazione CRISC ha per oggetto le seguenti aree della gestione degli IT Risk: Identificazione, e Valutazione dei Rischi; Risposta ai Rischi; Monitoraggio dei rischi; Impostazione e implementazione dei controlli IT; Monitoraggio e manutenzione dei controlli IT.
- Certified Information Security Manager (CISM). La certificazione CISM ha per oggetto le seguenti aree: Governance della sicurezza delle informazioni; Gestione dei rischi e Conformità; Sviluppo e Gestione dei programmi di Sicurezza delle Informazioni; Capacità di reagire agli incidenti di sicurezza.

La sicurezza IT è indirizzata nella gran parte di queste certificazioni, ma non viene data molta enfasi all'Ingegneria Secure Software.

URL	https://www.isaca.org/CERTIFICATION/Pages/default.aspx
Contact Method	General Contact: [http://www.isaca.org/About-ISACA/Contact-Us/Pages/default.aspx] Web form, phone and address
Country of HQ location	US
Geographic Scope	International
Type	Industry (no profit)

7.8 International Secure Software Engineering Council (ISSECO)

ISSECO promuove corsi di formazione sul SSE per ingegneri del software in modo che possano ottenere uno standard di certificazione (ISSECO Certified Professional for Secure Software Engineering). La certificazione è fornita dall'Istituto Internazionale Software Quality (iSQI)[29].

Secondo questa iniziativa, l'attenzione di ISSECO è sulla produzione di software sicuro e il suo obiettivo è quello di creare un ambiente informatico sicuro per tutti. Non è focalizzata su specifici linguaggi di programmazione.

URL	http://www.isseco.org/index.php?p=content
Contact Method	ISSECO Contact: http://www.isseco.org/index.php?p=contact ISQUI Contact: https://www.isqi.org/ Email, phone and address
Country of HQ location	Germany
Geographic Scope	National
Type	Industry (not for profit)

I temi principali della certificazione sono:

- Viewpoints of attackers and customers
- Trust and threat models
- Methodologies
- Requirements engineering with respect to security
- Secure design
- Secure coding
- Security testing
- Secure deployment
- Security response
- Security metrics
- Code and resource protection

[29] https://www.isqi.org/

Le attività di questa iniziativa sono supportati da partner diversi:

- Supporters (financial aid)
- Training providers (training material and classes)
- Certifiers (certification and certificate quality)