Frameworks Worth Knowing

CYBERSECURITY
&
SECURE PROGRAMMING

The day the names nearly stopped

15 April 2025 — the CVE funding cliff

- MITRE wrote to the CVE Board: the US government did not intend to renew the contract.
- Funding was due to expire the next day, 16 April 2025.
- Why this mattered.
  - CVE IDs are how every patch advisory, scanner and policy refers to a specific bug.
  - Without them, two engineers cannot be sure they are discussing the same vulnerability.
- How it was rescued.
  - CISA exercised an eleven-month extension on its $57.8m contract within hours.
  - The CVE Foundation was launched the same week for long-term independence.
  - By February 2026 CISA confirmed CVE is now a priority line-item — no funding gap in March 2026.

The three families — one map of the territory

Family	Audience	Question it answers	Headliners
OWASP	Developers	What to fix in the code	Top 10, ASVS, Cheat Sheets, SAMM
MITRE	Defenders	How attackers think	CVE, CWE, CAPEC, ATT&CK, D3FEND
NIST / ISO / EU	Governance	What management system to run	CSF 2.0, ISO 27001, NIS2, DORA, CE+, PCI DSS, SOC 2

The OWASP family

OWASP Top 10:2025 — the awareness layer

- Released as a release candidate at Global AppSec USA, 6 November 2025; finalised December 2025.
- Three changes worth flagging.
  - A02 — Security Misconfiguration jumped from #5 to #2 (cloud-native estates).
  - A03 — Software Supply Chain Failures (broadened from 'Vulnerable and Outdated Components').
  - A10 — Mishandling of Exceptional Conditions (new; 24 underlying CWEs on error handling and 'fail open').
- Broken Access Control is still A01, as it has been since 2021.
- Data-informed but not blindly data-driven — eight of ten from quantitative analysis, two from a community survey.

Beyond the Top 10 — the rest of OWASP, in one slide

- Other Top 10 lists worth knowing by name.
  - OWASP API Security Top 10 (2023) — drops Injection entirely; three of top five are authorisation failures.
  - OWASP Mobile Top 10 (2024) — first refresh in eight years; pair with MASVS.
  - OWASP Top 10 for LLM Applications (2025) — Prompt Injection #1; we cover it in Chapter 34.
- ASVS 5.0 — ~350 testable requirements across 17 chapters; L1/L2/L3 levels. 'ASVS L2' is increasingly common contract language.
- SAMM v2 — 'is this organisation set up to produce secure applications repeatedly?' — five business functions, three maturity levels.
- Cheat Sheet Series — ~90 short opinionated 'how to do this correctly' pages; bookmark before reading further.

CYBERSECURITY
&
SECURE PROGRAMMING

DISCUSSION

Open https://owasp.org/Top10/A02_2021-Cryptographic_Failures/ and look at the top of the page. How many CWEs feed into this single OWASP category?

The MITRE family

CVE vs CWE — the distinction that matters

CVE names the bug. CWE names the kind of bug.

A CVE is a single, named vulnerability instance — 'Apache Log4j 2.0–2.14.1 contains CVE-2021-44228, a JNDI lookup that allows remote code execution.' A CWE is the underlying kind of flaw — CVE-2021-44228 maps to CWE-502 (Deserialisation of Untrusted Data) and CWE-20 (Improper Input Validation). One CWE can be referenced by tens of thousands of CVEs; one CVE can map to one or more CWEs.

CVE answers 'which bug?'. CWE answers 'what kind of bug?'.

— MITRE CVE Programme and Common Weakness Enumeration

ATT&CK — what attackers actually do

- Adversarial Tactics, Techniques and Common Knowledge — a curated knowledge base of behaviour, not bugs.
- Enterprise matrix v18.1 (released 28 October 2025).
  - 14 tactics (columns), 216 techniques, 475 sub-techniques.
  - 172 named Groups, 784 Software entries, 52 Campaigns, 44 Mitigations.
  - v19 publishing today, 28 April 2026 — technique IDs in our worked example are stable.
- Big change in v18: per-technique 'Detections' replaced by structured Detection Strategies and Analytics — pull a machine-readable analytic into your SIEM.
- Used as a shared coordinate system: ATT&CK Navigator paints coverage layers; Sigma rules tag the techniques they detect.
- ATT&CK is a threat library, not a methodology. It feeds STRIDE; it does not replace it.

FIN7 (G0046) through the ATT&CK lens

- Financially-motivated criminal group active since 2013; originally retail/hospitality POS, now ransomware affiliation.
- Initial Access.
  - T1566.001 — Spearphishing Attachment (Word/RTF, often LNK or DDE-execution).
- Execution.
  - T1059.001 — PowerShell. Also T1059.003 (cmd) and T1047 (WMI).
- Persistence.
  - T1547.001 — Registry Run Keys. Or T1053.005 (Scheduled Task), T1543.003 (Service).
- Lateral Movement.
  - T1021.001 — RDP, often combined with T1078 (Valid Accounts).
- Impact.
  - T1486 — Data Encrypted for Impact; data staged to MEGA for double-extortion.

CYBERSECURITY
&
SECURE PROGRAMMING

DISCUSSION

Open https://attack.mitre.org/groups/G0046/ — scroll to Techniques Used. If you were defending against FIN7, which technique would you instrument first?

Governance — the whistle-stop tour

CYBERSECURITY & SECURE PROGRAMMING

Governance frameworks at a glance

Framework	What it is	Status
NIST CSF 2.0	Voluntary outcomes framework — Govern/Identify/Protect/Detect/Respond /Recover	Internal scaffolding; not certifiable
ISO/IEC 27001:2022	Certifiable ISMS standard; Annex A has 93 controls in 4 themes	The certificate vendor websites cite
CIS Controls v8.1	18 controls / 153 Safeguards; IG1 / IG2 / IG3 tiers for SMEs	Prescriptive; pairs with CSF
NIS2 (EU 2022/2555)	EU cybersecurity law; essential vs important entities	Ireland late; NCSB Bill expected 2026
DORA (EU 2022/2554)	Financial-services operational resilience regulation	Fully applicable since 17 January 2025
Cyber Essentials v3.3	UK self-assessment + CE+ technical audit; five control areas	Effective from today, 28 April 2026
PCI DSS v4.0.1	Card-payment contractual standard	Future-dated requirements mandatory since 31 March 2025
SOC 2 (Type I / II)	AICPA attestation report on Trust Services Criteria	Lingua franca of B2B SaaS assurance

Cyber Essentials v3.3 — effective today, 28 April 2026

- Cheapest credible certification in the British Isles; mandatory for many UK central-government supplier contracts since 2014.
- Two flavours: Cyber Essentials (self-assessment, verified) and Cyber Essentials Plus (adds external technical audit).
- Three v3.3 tightenings worth knowing.
  - MFA mandatory for all cloud services where supported — automatic-fail if missing.
  - 14-day patching window for high/critical updates (CVSS v3 base 7.0+) — automatic-fail if missed.
  - Cloud services can no longer be excluded from scope — formal definition added.
- Self-assessment fees: GBP 320–600 + VAT depending on size. CE+ from ~GBP 1,500 to GBP 4,000+ for complex environments.

An opinionated picking guide

A small Irish SaaS — pick in this order

1. Cyber Essentials Plus first. Cheapest credible cert by an order of magnitude (~GBP 1,500–4,000); v3.3 controls are forcing-function basics.
2. SOC 2 Type II within twelve months. Lingua franca of B2B SaaS sales; Security TSC only is a defensible scope. Budget USD 20k–50k for the first audit fee.
3. ISO 27001 only when a customer asks for it by name. For under ~100 staff without a regulated customer pulling, ISO-first is over-engineered and slow.
4. NIST CSF 2.0 is internal scaffolding, not a customer artefact. Pair with CIS Controls v8.1 IG1 or IG2 as the prescriptive Safeguards.
5. NIS2 / DORA / CRA / AI Act are obligations, not choices. If they apply, you comply — beside the certification programme, not instead of it.

The map is not the territory.

Frameworks are coordinate axes, not menus from which you choose one.

What's next

- Practical (W2 P): Threat modelling on OWASP Juice Shop — STRIDE on a real DFD, in the lab.
- W3 L1: Cryptography fundamentals — symmetric, asymmetric, hashing, where each goes wrong.
- Reading: Chapter 5 in the book; bookmark owasp.org/Top10/, attack.mitre.org, and the IASME Cyber Essentials page.
- Stretch task: open ATT&CK Navigator and paint a coverage layer for a sector that interests you. Hour well spent.