SECURITE · WEB

Cybersecurite des applications web — menaces & bonnes p

Date de realisation : 06/05/2026

Allan Theresine — BTS SIO SLAM — Portfolio 2026

Pourquoi cette veille ?

La cybersecurite est devenue une responsabilite partagee par tous les developpeurs. En 2025-2026, les cyberattaques se multiplient et se sophistiquent, portees par l'intelligence artificielle. En tant qu'etudiant en BTS SIO SLAM, comprendre les vulnerabilites les plus courantes (OWASP), les approches modernes (Zero Trust, DevSecOps) et le cadre reglementaire (NIS2) est indispensable pour construire des applications robustes.

1. OWASP Top 10 2025 — la reference mondiale mise a jour

L'**OWASP Top 10 2025** constitue la reference mondiale pour la securite des applications web. Cette edition introduit deux nouvelles categories et se concentre sur les **causes profondes** des failles plutot que sur leurs symptomes — une approche plus pragmatique pour les developpeurs.

Les principales categories a risque en 2025 :

- **Controle d'acces defaillant** (1er) : des utilisateurs accedent a des ressources auxquelles ils ne devraient pas avoir acces — faille la plus frequente.
- **Injections SQL / NoSQL / OS** : des donnees non filtrees executees comme du code. Toujours tres presente malgre les outils modernes.
- **Composants vulnerables** : l'utilisation de librairies open source obsoletes ou compromises (packages npm, pip) est un vecteur d'attaque majeur.
- **Mauvaise configuration de securite** : headers HTTP manquants, permissions trop larges, ports ouverts inutilement.

Source : MetaCompliance — « OWASP Top 10 2025 : risques cles des applications web » (dec. 2025) — https://www.metacompliance.com/fr/blog/cyber-security-awareness/owasp-top-10-2025-securite-web

2. Menaces 2025 : ransomwares et attaques IA

En 2025, les ransomwares connaissent une progression sans precedent. Des organisations, y compris des institutions publiques francaises, font face a des demandes de rancon atteignant plusieurs millions d'euros. Les cybercriminels utilisent desormais l'**IA pour automatiser** la detection de failles en temps reel et personnaliser leurs attaques de phishing.

Des failles critiques ont touche des composants tres utilises comme **Next.js** et des packages **npm**. Les attaques sur la **chaine logistique logicielle** (supply chain) sont en forte hausse : un package malveillant publie sur npm peut compromettre des milliers de projets en cascade. La verification reguliere des dependances est devenue non-negociable.

Source 1 : Human Coders — « Les pires failles de securite de 2025 » (oct. 2025) — https://blog.humancoders.com/les-pires-failles-de-securite-de-2025/ Source 2 : Studi — « Tendances de la cybersecurite en

2025 » — https://www.studi.com/fr/blog/metiers-formations/tendances-cybersecurite-avenir-formation

3. Bonnes pratiques a adopter en tant que developpeur

• **DevSecOps** : integrer la securite des la premiere ligne de code. C'est la tendance dominante en 2025 — la securite n'est plus une etape finale.

• **Zero Trust** : ne jamais faire confiance par defaut, verifier systematiquement chaque acces et chaque appareil connecte.

• **Audit des dependances** : utiliser npm audit ou Dependabot pour scanner les packages et detecter les composants vulnerables regulierement.

• **Authentification MFA** : rendre l'authentification robuste face aux attaques ciblant le travail a distance.

• **Directive NIS2** : la reglementation europeenne impose de nouvelles obligations de securite. Connaitre ses implications est attendu des professionnels du developpement.

La France vise a doubler les emplois du secteur cybersecurite, passant de 37 000 a 75 000 postes. Le marche recrute massivement des profils alliant developpement et sensibilite securite.

Source : Coursera — « 7 cybersecurity trends a connaitre en 2026 » (dec. 2025) — https://www.coursera.org/fr-FR/articles/cybersecurity-trends

Synthese & apport personnel

La cybersecurite en 2026 n'est plus l'affaire exclusive de specialistes : c'est une responsabilite de chaque developpeur. Maitriser les bases (OWASP, Zero Trust, DevSecOps, audit de dependances) me permettra de produire des applications plus fiables en stage et en entreprise. Ce sujet completera directement ma formation BTS SIO en me preparant aux exigences concretes du marche.

Sources consultees

• *https://www.metacompliance.com/fr/blog/.../owasp-top-10-2025-securite-web (dec. 2025)*

• *https://blog.humancoders.com/les-pires-failles-de-securite-de-2025/ (oct. 2025)*

• *https://www.studi.com/fr/blog/metiers-formations/tendances-cybersecurite-avenir-formation*

• *https://www.coursera.org/fr-FR/articles/cybersecurity-trends (dec. 2025)*

• *https://www.splashtop.com/fr/blog/cybersecurity-trends-2025 (sept. 2025)*