AUDAX CYBERSECURITY
OFFENSIVE SECURITY · CTEM

Web Application & API Security — Checklist (OWASP-aligned)

Οι web εφαρμογές & τα APIs είναι από τα πιο εκτεθειμένα assets σας. Χρησιμοποιήστε το checklist (ευθυγραμμισμένο με OWASP Top 10 & API Top 10) για να εντοπίσετε τα κρίσιμα κενά — και πώς η Audax τα **αποδεικνύει τεχνικά** μέσα από web, API & mobile penetration testing.

AUTHENTICATION & SESSION

- [ ] **Ισχυρό authentication + MFA· προστασία από brute-force / credential stuffing**
- [ ] **Ασφαλής διαχείριση session (secure/httponly cookies, rotation, logout, timeout)**

ACCESS CONTROL (AUTHORIZATION)

- [ ] **Καμία IDOR / BOLA — έλεγχος ιδιοκτησίας σε κάθε object reference** — πώς: **Audax: web/API pentest**
- [ ] **Function-level authorization (BFLA)· least privilege· καμία privilege escalation**

INPUT VALIDATION & INJECTION

- [ ] **SQL/NoSQL injection, XSS, command injection, SSRF, insecure deserialization**
- [ ] **Server-side validation & output encoding — όχι εμπιστοσύνη στον client**

API SECURITY

- [ ] **Auth σε ΚΑΘΕ endpoint· rate limiting· προστασία από mass assignment** — πώς: **Audax: API pentest**
- [ ] **Ελαχιστοποίηση data exposure· versioning· documentation χωρίς secrets**

DATA PROTECTION & CONFIGURATION

- [ ] **TLS παντού· security headers (CSP, HSTS)· secrets σε vault, όχι στον κώδικα**
- [ ] **Security misconfiguration· error handling χωρίς stack traces· hardened defaults**

BUSINESS LOGIC, DEPS & TESTING

- [ ] **Έλεγχος business-logic flaws & abuse cases (όχι μόνο scanner findings)**
- [ ] **Vulnerable & outdated components (supply chain)· τακτικό penetration testing & retest** — πώς: **Audax: pentest & retest**

Αντέχουν οι εφαρμογές σας σε πραγματικό αντίπαλο;

Ζητήστε web/API penetration test από την Audax — χειροκίνητος έλεγχος πέρα από scanners, proof-of-concept exploitation, τεκμηρίωση για developers & διοίκηση, retest.

✉ info@audax.gr · ☎ +30 210 9839367 · 🌐 www.audax.gr/services/offensive-security-services/web-api-mobile-penetration-testing/