SECURITATE & GDPR

Ghid Securitate Website 2026

SSL, parole, 2FA, malware, WordPress hardening, backup, WAF și incident response

~26 pagini · 19 min citire · PDF A4

Un site compromis costă în medie 5.000–50.000€ între downtime, date pierdute, amendă GDPR și reputație distrusă. Atacurile automate scanează milioane de site-uri zilnic — inclusiv al tău. Acest ghid acoperă protecția practică, de la SSL la plan de răspuns la incidente, pentru orice site românesc.

Cuprins

1 SSL/TLS — criptare și încredere

HTTPS nu e opțional din 2018 — Google marchează site-urile fără SSL ca nesigure, iar browserele afișează avertismente care alungă 90% din vizitatori. Certificatul SSL criptează datele în tranzit și e gratuit prin Let's Encrypt.

Sfat ValCode
Testează SSL pe ssllabs.com — ținta e nota A sau A+. Orice sub B are vulnerabilități active.

- Certificat SSL activ pe tot domeniul (inclusiv www și subdomenii)
- TLS 1.2+ obligatoriu, dezactivează TLS 1.0/1.1
- HSTS header: forțează HTTPS, previne downgrade attacks
- Redirect 301 automat HTTP → HTTPS pe toate paginile
- Mixed content: zero resurse HTTP pe pagini HTTPS
- Reînnoire automată Let's Encrypt (Certbot sau hosting managed)

2 Parole și autentificare — prima linie de apărare

80% din breșe folosesc parole slabe sau reutilizate. „admin/admin123” pe WordPress e compromis în sub 60 de secunde de boți automatizați. Politica de parole și autentificarea multi-factor elimină 99% din atacurile de tip brute force.

Sfat ValCode
Activează 2FA pe contul de hosting chiar azi — e cel mai compromis după WordPress admin.

- Parolă minim 16 caractere, random, manager parole (Bitwarden, 1Password)
- Utilizator admin non-default: nu „admin”, nu „administrator”
- 2FA obligatoriu pe: WordPress admin, hosting, domeniu, email
- Limitare încercări login: max 5, blocaj 30 min (Wordfence, Fail2Ban)
- Schimbare parole la 90 zile pentru accese critice
- Fără parole în repo Git, email sau chat — doar manager parole

3 Autentificare în doi pași (2FA) — implementare

2FA adaugă un al doilea factor pe lângă parolă: cod din app (TOTP), SMS sau hardware key. Chiar dacă parola e furată, atacatorul nu poate accesa contul. Pentru site-uri WordPress, plugin-uri ca Wordfence sau Solid Security oferă 2FA gratuit.

Sfat ValCode
Nu folosi SMS ca 2FA principal — SIM swapping e real. TOTP sau hardware key sunt superioare.

- TOTP (Google Authenticator, Authy) — preferat, fără dependență SMS
- 2FA obligatoriu pentru rol Administrator și Editor
- Backup codes: generează și stochează în siguranță 10 coduri
- Hardware key (YubiKey): maxim securitate pentru accese critice
- Dezactivează XML-RPC dacă nu e necesar — vector de brute force
- Monitorizare login: alertă email la login de pe IP nou

4 Malware — detectare, curățare și prevenție

Malware-ul pe site înseamnă redirecturi către spam, phishing pe vizitatorii tăi sau cryptomining în browser. Google blacklist-ează site-urile infectate — traficul scade la zero până la curățare. Scanarea zilnică automată e non-negociabilă.

Sfat ValCode
Dacă site-ul e pe Google Blacklist, trimite cerere de review în Search Console imediat după curățare — recuperarea durează 1–5 zile.

- Scanner zilnic: Wordfence, Sucuri, MalCare (WordPress)
- Monitorizare fișiere: alertă la modificare fișiere core WP
- Verificare Google Safe Browsing săptămânal
- Curățare profesională dacă infectat — nu doar „delete plugin”
- Analiză vector intrare post-incident: cum a intrat malware-ul
- Notificare clienți dacă date personale au fost accesate (GDPR 72h)

5 WordPress hardening — securizare specifică

WordPress alimentează 43% din web — și e ținta #1 a atacurilor. Majoritatea breșelor vin din plugin-uri neactualizate, teme piratate și wp-admin expus. Hardening-ul reduce suprafața de atac fără a afecta funcționalitatea.

Sfat ValCode
Instalează maximum 15 plugin-uri active — fiecare e o potențială ușă de intrare. Calitate peste cantitate.

- Update imediat: core WP, plugin-uri, teme — automatizare cu backup pre-update
- Elimină plugin-uri neutilizate — nu doar dezactivează, șterge
- wp-admin: restricționare IP sau mutare URL (ex: /dashboard-secret)
- Dezactivează editor fișiere WP: DISALLOW_FILE_EDIT în wp-config
- Permisiuni fișiere: 644 fișiere, 755 directoare, 440 wp-config.php
- Fără teme/plugin-uri piratate (nulled) — backdoor garantat

6 Backup — strategia 3-2-1

Backup-ul fără test de restore e iluzie de securitate. Regula 3-2-1: 3 copii, 2 medii diferite, 1 offsite. Backup zilnic automat cu retenție 30 zile minim. Testează restore-ul trimestrial — nu aștepta incidentul real.

Sfat ValCode
Un restore care durează 4 ore în test va dura 8 ore în criză — optimizează acum, nu în incident.

- Backup zilnic automat: fișiere + bază de date
- Stocare offsite: AWS S3, Google Cloud, Backblaze — nu pe același server
- Retenție: 30 zile daily, 12 luni monthly
- Test restore trimestrial: mută pe staging, verifică funcționalitate
- Backup pre-update: automat înainte de orice update WP
- Backup criptat: AES-256 pentru copii offsite

7 WAF și protecție perimetru — Cloudflare, Wordfence

Web Application Firewall blochează atacuri înainte să ajungă la server: SQL injection, XSS, DDoS. Cloudflare Free oferă WAF de bază și CDN global. Pentru WordPress, Wordfence Premium adaugă firewall la nivel de aplicație.

Sfat ValCode
Activează Cloudflare „Under Attack Mode” doar în incident DDoS — afectează UX normal. Folosește doar când e necesar.

- Cloudflare: DNS proxy, WAF free, DDoS protection, cache global
- Reguli WAF: blocare țări fără trafic legitim (opțional)
- Rate limiting: max 100 request/min per IP pe wp-login
- Bot fight mode: blochează boți rău intenționați automat
- Wordfence firewall: reguli specifice WordPress, block IP
- Monitorizare uptime: UptimeRobot gratuit, alertă SMS/email

8 Răspuns la incidente — plan în 6 pași

Când se întâmplă — și se va întâmpla — reacția în primele 60 de minute decide impactul total. Un plan documentat evită panica, pierderea de dovezi și extinderea breșei. Pregătește planul acum, nu în mijlocul atacului.

Sfat ValCode
Păstrează un document „Incident Response” cu telefoane hosting, acces backup, contact ANSPDCP — accesibil offline.

- Pas 1: Izolare — pune site în maintenance, deconectează DB dacă e necesar
- Pas 2: Evaluare — ce e compromis? Date clienți? Cât timp e activ?
- Pas 3: Notificare — echipa, hosting, ANSPDCP dacă date personale (72h)
- Pas 4: Curățare — restore din backup curat sau curățare profesională
- Pas 5: Patch — închide vectorul: update, schimbare parole, 2FA
- Pas 6: Post-mortem — documentează, îmbunătățește, testează din nou

Întrebări frecvente

Cât costă securizarea unui site WordPress?
0–50€/lună cu Cloudflare Free + Wordfence Free + backup UpdraftPlus. Pentru site-uri cu trafic sau date sensibile: 100–300€/lună (Wordfence Premium, backup managed, monitorizare). ValCode.dev include hardening în mentenanță.

Site-ul meu e mic — sunt țintă pentru hackeri?
Da. Atacurile sunt automate și nu discriminează după mărime. Boții scanează tot internetul. Un site nesecurizat e compromis în medie în 30–45 zile de la expunere.

Implementare completă

Site + SEO + Google Ads + Mentenanță
Audit gratuit · Demo site gratuit · Răspuns în 24h

valcode.dev/contact

+40 750 205 515 · contact@valcode.dev