MIDNIGHT WEBS

RESURSĂ GRATUITĂ · LISTĂ DE SECURITATE

Listă de verificare pentru securitatea lansării site-ului

Majoritatea site-urilor mici care ajung compromise nu au fost vizate de atacatori sofisticați. Rulau un plugin vechi, o parolă refolosită sau o pagină de administrare neprotejată. Lista de mai jos adună cele aproximativ 40 de verificări care închid aceste breșe înainte ca site-ul să fie public.

Actualizat în noiembrie 2026 | 12 min de citit | 48 verificări

PENTRU CINE ESTE	CE ACOPERĂ	CUM O FOLOSEȘTI
Proprietari, manageri de proiect și dezvoltatori care pregătesc o lansare	8 domenii, de la accesul în conturi la testele din ziua lansării	Dă fiecărui punct un responsabil și o dată; „!” marchează punctele care nu se omit

ÎNCEPE DE AICI

Dacă ai doar o oră, parcurge secțiunile 1, 2 și 5. Autentificarea în doi pași, un domeniu blocat și un backup testat opresc cele mai costisitoare incidente.

BIFEAZĂ CĂSUȚA CÂND AI TERMINAT · ESENȚIAL = IMPACT MAXIM

01 Conturi și acces

Parolele slabe sau refolosite rămân cea mai frecventă cale de intrare în site-urile mici, pentru că atacatorii încearcă pur și simplu parole scurse de la alte servicii. Rezolvă mai întâi accesul; este și cea mai ieftină parte a listei.

- [ ] ESENȚIAL **Activează autentificarea în doi pași peste tot unde contează**
  Găzduire, registrar de domenii, panoul CMS, email și analytics. Preferă o aplicație de autentificare sau o cheie de acces (passkey) în locul SMS-ului, care poate fi interceptat prin duplicarea cartelei SIM.

- [ ] ESENȚIAL **Folosește un manager de parole și parole generate**
  Parole aleatorii de peste 16 caractere, unice pentru fiecare serviciu. Ghidul actual NIST pune accent pe lungime și unicitate, nu pe reguli forțate de complexitate.

- [ ] **Fiecare persoană își are propriul cont**
  Conturile comune fac imposibil de aflat cine a schimbat ce sau de scos o persoană fără să încurci pe toți ceilalți.

- [ ] **Aplică principiul privilegiului minim**
  Un editor are nevoie de rolul „Editor”, nu de „Administrator”. Păstrează numărul administratorilor la cei care chiar au nevoie, ideal doi sau trei.

- [ ] **Elimină persoanele plecate și conturile nefolosite**
  Verifică găzduirea, registrarul, conturile Google/Meta, instrumentele de plată și lista de utilizatori din CMS. Colaboratorii din proiectele vechi sunt rămășițele obișnuite.

- [ ] **Notează cine deține fiecare cont**
  Domeniul, găzduirea și conturile de plată trebuie înregistrate pe firmă, nu pe emailul personal al unui colaborator. Păstrează codurile de recuperare în managerul de parole.

CUM VERIFICI

Deschide adresa de administrare într-o fereastră privată: trebuie să ceară parola și un al doilea factor. Verifică lista de utilizatori după nume pe care nu le recunoști.

02 Domeniu, DNS și HTTPS

Domeniul controlează tot restul. Dacă îl preia cineva, preia site-ul, emailul și reputația ta.

- [ ] ESENȚIAL **Blochează domeniul și protejează contul de la registrar**
  Activează blocarea la registrar (transfer lock), 2FA și reînnoirea automată. Un domeniu expirat poate fi înregistrat de oricine, inclusiv de cei care te vor imita.

- [ ] ESENȚIAL **Servește toate paginile prin HTTPS, cu reînnoire automată**
  Browserele îl cer pentru plăți și formulare. Durata certificatelor se scurtează (industria a stabilit trecerea la 200 de zile din martie 2026, apoi 100 și 47 de zile), deci reînnoirea manuală nu mai ține.

- [ ] **Redirecționează HTTP către HTTPS printr-un redirect permanent (301)**
  Și alege o singură versiune canonică a adresei, cu sau fără „www”, ca site-ul să nu existe în două locuri.

- [ ] **Publică SPF, DKIM și DMARC pentru emailul firmei**
  Fără ele, infractorii pot trimite mesaje care par să vină de la domeniul tău, iar Gmail și Yahoo îți pot muta emailurile reale la spam. Pornește DMARC cu `p=none` și rapoarte, apoi treci la quarantine sau reject când rapoartele arată curat.

- [ ] **Șterge înregistrările DNS pe care nu le mai folosești**
  Înregistrările vechi, care arată spre servicii anulate, pot fi revendicate de atacatori (subdomain takeover). Verifică una câte una înregistrările A, CNAME și MX.

- [ ] **Adaugă HSTS după ce totul funcționează prin HTTPS**
  Începe cu un max-age scurt, de exemplu 300 de secunde, testează toate subdomeniile, apoi crește-l la un an. Adaugă „preload” doar dacă ești sigur că toate subdomeniile rămân pe HTTPS.

CUM VERIFICI

Rulează domeniul prin SSL Labs (ssllabs.com/ssltest) pentru certificat și folosește `dig TXT yourdomain.com` și `dig TXT _dmarc.yourdomain.com` ca să confirmi că înregistrările de email există.

03 Platformă, software și setări de server

Atacatorii scanează internetul după vulnerabilități cunoscute în software vechi. Majoritatea atacurilor reușite folosesc o breșă care avea deja un remediu public.

- [ ] ESENȚIAL **Actualizează CMS-ul, temele, pluginurile și pachetele de server înainte de lansare**
  Apoi programează actualizările, cel puțin săptămânal pentru pluginuri. Activează actualizările automate de securitate acolo unde platforma le permite.

- [ ] **Șterge tot ce nu folosești**
  Pluginurile și temele dezactivate pot fi totuși exploatate. Mai puține componente înseamnă mai puține actualizări și o suprafață de atac mai mică.

- [ ] **Elimină conținutul demo, utilizatorii de test și conturile implicite**
  Un utilizator numit „admin” sau „test” cu parolă slabă este primul lucru încercat de scripturile automate.

- [ ] ESENȚIAL **Asigură-te că fișierele private nu sunt publice**
  Încearcă yourdomain.com `/.env`, `/.git/config`, `/backup.zip` și `/phpinfo.php`. Toate trebuie să dea 404 sau 403, niciodată conținut. Ține secretele, cheile API și copiile bazei de date în afara directorului public.

- [ ] **Oprește listarea directoarelor și editarea fișierelor din panou**
  În WordPress adaugă `define('DISALLOW_FILE_EDIT', true);` în wp-config.php, ca un cont de administrator furat să nu poată modifica direct codul.

- [ ] **Adaugă antetele standard de securitate**
  `X-Content-Type-Options: nosniff`, un `Referrer-Policy`, protecție împotriva clickjacking-ului (frame-ancestors sau X-Frame-Options) și, când ești gata să o testezi, un Content-Security-Policy. Verifică rezultatul pe securityheaders.com sau Mozilla Observatory.

CUM VERIFICI

Fă lista tuturor pluginurilor și temelor cu versiunea lor și compar-o cu ultima versiune a producătorului. Orice a fost abandonat de peste un an trebuie înlocuit.

04 Formulare, autentificare și plăți

Fiecare câmp în care poate scrie un vizitator este o poartă de intrare. Consideră orice input ostil până când serverul l-a verificat.

- [ ] ESENȚIAL **Validează și curăță datele pe server**
  Verificările din browser sunt doar pentru confort; oricine le poate ocoli. Folosește interogări parametrizate împotriva SQL injection și escapează ieșirea împotriva injecției de scripturi.

- [ ] ESENȚIAL **Protejează formularele publice de spam și abuz**
  Folosește o alternativă la CAPTCHA precum Cloudflare Turnstile, un câmp-capcană (honeypot) și limitarea ratei, ca boții să nu-ți inunde căsuța sau cota de email.

- [ ] **Adaugă protecție CSRF și cookie-uri sigure**
  Cookie-urile de sesiune trebuie să fie Secure, `HttpOnly` și `SameSite=Lax` (sau Strict). Așa alte site-uri nu pot trimite pe ascuns acțiuni în numele unui utilizator autentificat.

- [ ] **Restricționează încărcarea de fișiere**
  Permite doar tipurile necesare, verifică tipul real și dimensiunea, redenumește fișierele și stochează-le în afara directorului public, unde se poate.

- [ ] **Colectează doar ce ai nevoie**
  Fiecare câmp în plus este o dată pe care trebuie s-o protejezi și s-o ștergi la cerere conform GDPR. Dacă nu folosești numărul de telefon, nu-l cere.

- [ ] **Lasă furnizorul de plăți să gestioneze datele cardului**
  Folosește checkout găzduit sau câmpuri găzduite (Stripe, PayPal, gateway-ul băncii tale), ca numerele de card să nu ajungă niciodată pe serverul tău. Astfel obligațiile PCI rămân la nivelul cel mai redus.

CUM VERIFICI

Trimite fiecare formular cu un șir foarte lung, cu un apostrof și cu `<b>bold</b>`. Trebuie acceptat sau respins curat, iar formatarea nu trebuie să apară niciodată randată în pagină.

05 Backup-uri și recuperare

Backup-urile te protejează de hackeri, dar și de actualizări eșuate, ștergeri accidentale și probleme la găzduire. Un backup pe care nu l-ai restaurat niciodată este doar o speranță.

- [ ] ESENȚIAL **Automatizează backup-urile zilnice ale fișierelor și bazei de date**
  Păstrează 14–30 de zile de istoric, ca să poți reveni la momentul de dinaintea problemei, nu doar la seara trecută.

- [ ] ESENȚIAL **Păstrează o copie în altă parte**
  Regula 3-2-1: trei copii, pe două tipuri de stocare, una în afara locației. Un backup din același cont de găzduire dispare odată cu el.

- [ ] **Criptează backup-urile care conțin date personale**
  Datele clienților dintr-un backup rămân date ale clienților conform GDPR.

- [ ] **Restaurează un backup într-un mediu de test înainte de lansare**
  Cronometrează cât durează. Acesta este timpul tău real de recuperare; majoritatea proprietarilor îl află abia în timpul unei urgențe.

- [ ] **Scrie o notă de recuperare de o pagină**
  Cine poate restaura, unde sunt stocate backup-urile, cum te autentifici și pe cine suni la furnizorul de găzduire. Ține o copie care nu depinde de site.

CUM VERIFICI

Alege backup-ul de ieri, restaurează-l pe o copie de test și verifică dacă apar paginile, imaginile și mesajele din formulare.

06 Monitorizare și reacție la incidente

Site-urile compromise rulează adesea nesesizate săptămâni întregi. Monitorizarea reduce acest timp la minute.

- [ ] ESENȚIAL **Configurează monitorizarea disponibilității cu alerte**
  Instrumente gratuite precum UptimeRobot sau Better Stack verifică la 1–5 minute și te anunță când site-ul nu mai răspunde.

- [ ] **Urmărește expirarea certificatului și a domeniului**
  Setează alerte cu 30 și cu 7 zile înainte de expirare, trimise la două persoane.

- [ ] **Adaugă Google Search Console și verifică „Probleme de securitate”**
  Google îți spune dacă găsește malware sau conținut piratat, adesea înaintea vizitatorilor tăi.

- [ ] **Înregistrează autentificările eșuate și modificările din administrare**
  Verifică-le după lansare și alertează la eșecuri repetate de la aceeași adresă.

- [ ] **Trimite alertele către o căsuță pe care cineva o citește**
  O notificare de securitate care ajunge la un fost angajat nu este monitorizare.

- [ ] **Pregătește un plan scurt de incident**
  Pe cine contactezi, cum pui site-ul în mentenanță, cum resetezi toate parolele și cine informează clienții. Conform GDPR, o încălcare a securității datelor personale trebuie raportată autorității în 72 de ore de la momentul în care ai aflat.

CUM VERIFICI

Oprește scurt site-ul în mediul de test sau îndreaptă monitorul spre o adresă greșită. Confirmă că alerta ajunge și cine o primește.

07 Confidențialitate și aspecte legale

Colectarea de date creează obligații. Un site care colectează mai puțin și explică clar este mai sigur și mai ușor de apărat.

- [ ] ESENȚIAL **Publică o politică de confidențialitate care corespunde realității**
  Enumeră ce colectezi, de ce, cine primește datele (analytics, furnizor de email, procesator de plăți) și cât timp le păstrezi.

- [ ] ESENȚIAL **Cere consimțământul pentru cookie-uri înainte de cele neesențiale**
  Analytics, publicitatea și pixelii de urmărire nu trebuie să se încarce până când vizitatorul acceptă, dacă ai vizitatori din UE sau din Regatul Unit. Cookie-urile esențiale (autentificare, coș) nu cer consimțământ.

- [ ] **Semnează acorduri de prelucrare a datelor cu furnizorii**
  Instrumentele de email, analytics și găzduirea care prelucrează date personale ale rezidenților UE au nevoie de un DPA; majoritatea furnizorilor oferă unul de acceptat online.

- [ ] **Leagă politicile de locurile unde se colectează datele**
  Lângă formulare, la abonarea la newsletter și în checkout.

- [ ] **Verifică datele firmei și informațiile de contact**
  Denumirea legală, numărul de înregistrare, adresa și codul de TVA, acolo unde este cazul. În multe țări sunt obligatorii pe site-urile comerciale.

CUM VERIFICI

Deschide site-ul într-o fereastră privată curată și verifică în instrumentele de dezvoltator (fila Network) ce se încarcă înainte să apeși „Accept”.

08 Teste în ziua lansării

Ultima trecere dovedește că site-ul funcționează pe dispozitive reale, cu date reale și cu servere de email reale.

- [ ] ESENȚIAL **Testează fiecare formular și confirmă că mesajul ajunge**
  Verifică și folderul de spam. Adresele de expeditor și reply-to trebuie să folosească propriul domeniu.

- [ ] ESENȚIAL **Testează checkout-ul de la cap la coadă**
  O plată reală mică, emailul de confirmare și o rambursare. Șterge apoi comenzile de test.

- [ ] ESENȚIAL **Elimină „`noindex`” și parolele de pe mediul de test**
  O etichetă `noindex` uitată ține un site nou în afara Google. Verifică ca `robots.txt` să nu conțină „`Disallow: /`”.

- [ ] **Adaugă redirecturi 301 de la toate adresele vechi**
  Dacă ai înlocuit un site existent, asociază paginile vechi cu cele noi, ca pozițiile, marcajele și linkurile să continue să funcționeze.

- [ ] **Verifică paginile 404, linkurile rupte și imaginile**
  Parcurge site-ul cu un instrument gratuit precum Screaming Frog (până la 500 de adrese gratuit) și corectează fiecare eroare.

- [ ] **Trimite sitemap-ul**
  În Google Search Console și în Bing Webmaster Tools.

- [ ] **Testează pe un telefon real și pe o conexiune lentă**
  Folosește date mobile, nu Wi-Fi-ul din birou.

- [ ] **Fă un ultim backup și notează ora lansării**
  Dacă ceva nu merge, poți reveni la o stare cunoscută ca bună.

CUM VERIFICI

Roagă pe cineva care nu a mai văzut site-ul să facă sarcina principală (să te contacteze, să cumpere ceva) pe propriul telefon, în timp ce te uiți.

Surse și lecturi suplimentare

OWASP Cheat Sheet Series
https://cheatsheetseries.owasp.org/

NIST SP 800-63B: ghid pentru identitate digitală (parole)
https://pages.nist.gov/800-63-4/sp800-63b.html

Mozilla Observatory (testarea antetelor de securitate)
https://developer.mozilla.org/en-US/observatory

Google: cerințe pentru expeditorii de email (SPF, DKIM, DMARC)
https://support.google.com/a/answer/81126

Ai nevoie de ajutor?

Midnight Webs proiectează, securizează și întreține site-uri pentru afaceri mici. Spune-ne ce ai nevoie și stabilim împreună pașii.

midnightwebs.com/ro/estimate

Citește online: midnightwebs.com/ro/resources/website-launch-security-checklist