DOCUMENTAȚIE SECURITATE

Verificări de securitate web și protecție împotriva atacurilor

VERSIUNE DEMO

Conținut Demo

Această versiune demo prezintă **4 din 29** verificări din categoria Securitate.

Versiunea completă include toate cele **29 verificări** verificări cu:

Generat la: 28.01.2026 23:06:08

IDENTITATE FISCALĂ

PFA BODNARIU RAZVAN TRAIAN

CUI: 52188722 | **Reg. com.:** F2025026473001

Tel: +4 0775 278326 | **Email:** office@webrt.eu

Despre Securitate

Ce este Securitate?

Securitatea web reprezintă setul de măsuri tehnice și configurații care protejează un site web împotriva atacurilor malițioase, furtului de date și exploatării vulnerabilităților. O configurație de securitate corectă este esențială pentru protejarea datelor utilizatorilor și a reputației afacerii.

Beneficii

- Protecție împotriva atacurilor XSS, CSRF, clickjacking
- Criptarea datelor în tranzit prin HTTPS
- Conformitate cu GDPR și alte reglementări de protecție a datelor
- Încredere crescută din partea utilizatorilor
- Prevenirea pierderilor financiare și de reputație

Standarde și Ghiduri

Verificările din această categorie sunt bazate pe: **OWASP Top 10, Mozilla Security Guidelines**

Verificări în versiunea Demo

4 din **29** verificări

Versiunea completă include toate cele 29 verificări.

Securitate — Demo (4 din 29 verificări)

Verificare	Detalii
Allowed HTTP Methods	**Ce înseamnă:** Restricționarea metodelor HTTP la cele necesare previne atacurile care ar putea exploata funcții avansate ale serverului web. **Ce verifică:** Verifică dacă sunt permise doar metodele HTTP necesare (GET, POST, HEAD) și sunt dezactivate cele periculoase (TRACE, DELETE, PUT). **De ce e important:** Metodele HTTP periculoase pot fi exploatate pentru atacuri de tip cross-site tracing sau pentru modificarea neautorizată de conținut. **Cum se rezolvă:** Adăugați în .htaccess: <LimitExcept GET POST HEAD> Require all denied </LimitExcept> RewriteEngine On RewriteCond %{REQUEST_METHOD} ^(TRACE|DELETE|TRACK) [NC] RewriteRule .* - [F] **Documentație oficială:** • OWASP Testing for HTTP Methods • Apache Limit Module Documentation
CSP Upgrade Insecure Requests	**Ce înseamnă:** Această directivă CSP face ca toate resursele HTTP de pe site să fie automat "upgrated" la HTTPS, eliminând problemele de securitate cu conținutul mixt. **Ce verifică:** Verifică utilizarea directivei upgrade-insecure-requests în Content Security Policy. **De ce e important:** Directiva upgrade-insecure-requests forțează automat toate resursele HTTP să fie încărcate prin HTTPS, eliminând conținutul mixt. **Cum se rezolvă:** Activați upgrade-insecure-requests pentru conversie automată HTTP→HTTPS. Apache: Header always set Content-Security-Policy "upgrade-insecure-requests". Nginx: add_header Content-Security-Policy "upgrade-insecure-requests" always;. Meta tag alternativ: <meta http-equiv="Content-Security-Policy" content="upgrade-insecure-requests">. Test mode: Content-Security-Policy-Report-Only cu report-uri. Testați în DevTools Security/Console. **Documentație oficială:** • W3C Upgrade Insecure Requests • Google Mixed Content Guide
Complete Security Headers	**Ce înseamnă:** Această configurație completă de securitate pentru .htaccess oferă protecție cuprinzătoare împotriva celor mai comune atacuri web. **Ce verifică:** Verifică dacă toate header-urile de securitate esențiale sunt configurate corect. **De ce e important:** Un set complet de header-uri de securitate oferă protecție în profunzime împotriva diverselor tipuri de atacuri web. **Cum se rezolvă:** Configurați .htaccess complet: HTTPS redirect (RewriteCond %{HTTPS} off), Security headers (X-Frame-Options SAMEORIGIN, X-Content-Type-Options nosniff, X-XSS-Protection, HSTS, CSP), Hide server (Header unset Server), Secure cookies (HttpOnly;Secure), File protection (FilesMatch .env|.htaccess|.ini), Directory protection (Options -Indexes), HTTP methods restriction (LimitExcept GET POST HEAD), Disable TRACE. Verificați: securityheaders.com. **Documentație oficială:** • OWASP Secure Headers Project • Mozilla Security Guidelines • Apache Security Configuration

Verificare	Detalii
Content Security Policy	**Ce înseamnă:** Content Security Policy controlează ce resurse (JavaScript, CSS, imagini) poate încărca site-ul dvs., prevenind atacurile malițioase. **Ce verifică:** Verifică dacă site-ul are configurat Content Security Policy (CSP) pentru a preveni atacurile XSS și injection. **De ce e important:** CSP este o barieră de apărare puternică împotriva atacurilor XSS, clickjacking și altor atacuri de injecție. **Cum se rezolvă:** Adăugați în .htaccess: Header always set Content-Security-Policy "default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; img-src 'self' data:;" **Documentație oficială:** • CSP Quick Reference Guide • Google CSP Evaluator Tool

□□ Disponibile în versiunea completă

Categoria conține încă **Securitate 25 verificări suplimentare** în versiunea completă.

Verificări disponibile în versiunea completă:

- Content Security Policy Enhanced
- Cookie Flags
- Cookie Secure
- Cross Origin Headers
- DNS Info
- Directory Browsing
- Expect Ct
- HSTS Preload
- HTTPS Redirect
- Hpkp Header
- Mixed Content
- Permissions Policy
- Referrer Policy
- SSL Certificate
- Security Headers
- Sensitive Files Exposed
- Server Signature
- Set Cookie
- Strict Transport Security
- TLS Version
- Trace Method
- XContent Type Options
- XFrame Options
- XPermitted Policies
- XXss Protection

Fiecare verificare include: explicații detaliate, impact asupra afacerii,
recomandări tehnice, exemple de implementare și link-uri către documentația oficială.

Contactați-ne pentru versiunea completă: office@webrt.eu