

Kompleksowy Raport Bezpieczeństwa i Wydajności – inwood.pl

Data testu: 01.05.2025

Narzędzia użyte:

- Qualys SSL Server Test (SSL Labs) – Rating A
- SecurityHeaders.com – ocena F
- UpGuard Security – ocena A (810/950)
- Google PageSpeed Insights – Mobile: 71; Desktop: 82

Spis treści

1. Wprowadzenie
2. SSL/TLS
3. Nagłówki bezpieczeństwa HTTP
4. DNS
5. Ochrona poczty e-mail
6. CMS i podatności
7. Wydajność strony
8. Kolejne kroki i harmonogram wdrożenia
9. Słowniczek pojęć

1. Wprowadzenie

- **Cel raportu:** Pełna ocena konfiguracji SSL/TLS, nagłówków HTTP, DNS, poczty, podatności CMS oraz wydajności strony inwood.pl.
- **Data:** 01.05.2025
- **Narzędzia:** Qualys SSL Labs, SecurityHeaders.com, UpGuard, PageSpeed Insights

2. SSL/TLS

2.1 Co działa poprawnie

- ☒ Certyfikat RSA 2048 bit (SHA-256)
- ☒ Transparency i OCSP (nieodwołany)
- ☒ Wyłączone starsze protokoły (SSL 2/3, TLS 1.0/1.1)

2.2 Usprawnienia (! priorytet wysoki)

1. Dodaj rekord DNS CAA

```
inwood.pl. CAA 0 issue "letsencrypt.org"
```

Dlaczego? Ogranicza, które CA mogą wystawiać certyfikaty dla domeny.

2. Usuń słabe szyfry (CBC, RSA key-exchange)

```
ssl_ciphers "ECDHE-ECDSA-AES128-GCM-SHA256:  
             ECDHE-RSA-AES128-GCM-SHA256:  
             ECDHE-ECDSA-CHACHA20-POLY1305:  
             ECDHE-RSA-CHACHA20-POLY1305";
```

Dlaczego? Zapobiega atakom typu Bleichenbacher, Lucky Thirteen.

3. Włącz OCSP Stapling

```
ssl_stapling on;  
ssl_stapling_verify on;
```

Dlaczego? Przyspiesza i zabezpiecza weryfikację certyfikatu.

4. Dodaj HSTS

```
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

Dlaczego? Wymusza HTTPS, chroni przed downgrade attack.



3. Nagłówki bezpieczeństwa HTTP

Nagłówek	Rekomendacja	Priorytet
Content-Security-Policy	```Content-Security-Policy:	
default-src 'self';		
script-src 'self' https://cdnjs.cloudflare.com ;		
style-src 'self' 'unsafe-inline';		
img-src 'self' data;;		
upgrade-insecure-requests;```	!	
X-Frame-Options	X-Frame-Options: SAMEORIGIN	!
X-Content-Type-Options	X-Content-Type-Options: nosniff	!
Referrer-Policy	Referrer-Policy: strict-origin-when-cross-orig in	!
Permissions-Policy	```Permissions-Policy:	
camera=(), microphone=(), geolocation=()```	!	

Dlaczego?

- **CSP** blokuje złośliwe skrypty (XSS)
- **X-Frame-Options** chroni przed clickjackingiem
- **nosniff** zapobiega MIME-sniffingowi
- **Referrer-Policy** ogranicza wyciek danych
- **Permissions-Policy** minimalizuje dostęp do API przeglądarki

4. DNS

1.  DNSSEC: **wyłączone** → **Włącz** (chroni przed fałszywymi rekordami DNS)
2.  DNS CAA: **brak** → **Dodaj**:

inwood.pl. CAA 0 issue "letsencrypt.org"

5. Ochrona poczty e-mail

Mechanizm	Stan	Rekomendacja
SPF	OK	—
DMARC	p=quarantine	Zmień na <code>p=reject; pct=100; rua=mailto:admin@inwood.pl</code>
PTR	brak (niski priorytet)	—

Dlaczego? `p=reject` blokuje fałszywe wiadomości podszywające się pod Twoją domenę.

6. CMS i podatności

- **!** **Contact Form 7 5.9.3** → **Zaktualizuj** do najnowszej wersji.
- **!** **Elementor Pro 3.21.0** → **Zaktualizuj** do najnowszej wersji.
- **✓** Brak otwartych portów (bezpiecznie).
- **✓** Poprawne przekierowanie HTTP → HTTPS.

7. Wydajność strony

7.1 Mobile (71 ⚠)

- FCP: 3,3 s
- LCP: 5,3 s
- CLS: 0,04

Rekomendacje (mobile):

1. Usuń zasoby blokujące renderowanie (↓ ~2350 ms)
2. Usuń nieużywany CSS (↓ ~118 KB)
3. Minifikuj CSS/JS (↓ ~54 KB)
4. Konwertuj obrazy do WebP/AVIF (↓ ~265 KB)
5. Serwuj obrazy o właściwych wymiarach (↓ ~203 KB)
6. Ustaw długi cache TTL
7. Lazy-load dla niekrytycznych zasobów

7.2 Desktop (82 ✓)

- FCP: 0,8 s
- LCP: 1,4 s
- CLS: 0,216

Rekomendacje (desktop):

1. Format nowej generacji dla dużych obrazów (↓ ~961 KB)
2. Optymalne rozmiary obrazów (↓ ~1325 KB)
3. Usuń render-blocking resources (↓ ~560 ms)
4. Preload kluczowych zasobów (fonty, CSS)
5. Rezerwuj wymiary obrazów (niższy CLS)

8. Kolejne kroki i harmonogram

Priorytet	Zadanie	Czas realizacji
!	Wyłączenie słabych szyfrów, wdrożenie CSP, HSTS	1–2 dni
!	Dodanie CAA, DNSSEC, OCSP Stapling	1 dzień
!	Dodanie nagłówków X-Frame-Options, nosniff, Referrer-Policy, Permissions-Policy	1 dzień
!	Zmiana DMARC na p=reject , weryfikacja SPF	½ dnia
!	Aktualizacja wtyczek WordPress	½ dnia
!	Optymalizacja mobilnej wydajności (render-blocking, obrazki, cache)	1–2 dni
✓	Testy wstępne w środowisku testowym	½ dnia
✓	Wdrożenie na produkcję i monitorowanie	1 dzień

9. Słowniczek pojęć

- **FCP (First Contentful Paint):** czas do wyświetlenia pierwszego elementu treści.
- **LCP (Largest Contentful Paint):** czas do wyświetlenia największego elementu treści.
- **CLS (Cumulative Layout Shift):** miara nieoczekiwanych przesunięć układu.
- **CSP (Content-Security-Policy):** nagłówek kontrolujący źródła zasobów.
- **HSTS (Strict-Transport-Security):** nagłówek wymuszający HTTPS.
- **DNSSEC:** mechanizm zabezpieczający integralność zapisów DNS.
- **DMARC/SPF/PTR:** mechanizmy zabezpieczające przed podszywaniem się pod pocztę.