# Raport bezpieczeństwa – Nagłówki HTTP

Strona: porolex.pl | Źródło: SecurityHeaders.com

Poniższy raport zawiera analizę konfiguracji nagłówków HTTP bezpieczeństwa dla strony porolex.pl. Brak wdrożenia podstawowych nagłówków skutkuje oceną F w narzędziu SecurityHeaders.com. Zaleca się wprowadzenie poniższych zmian w konfiguracji serwera lub poprzez system zarządzania treścią (CMS), aby zwiększyć poziom bezpieczeństwa strony.

## Strict-Transport-Security

Zapewnia, że przeglądarka używa wyłącznie HTTPS.

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

## Content-Security-Policy

Chroni przed XSS – pozwala zdefiniować bezpieczne źródła treści.

```
Content-Security-Policy: default-src 'self'; img-src *; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'
```

## X-Frame-Options

Zapobiega osadzaniu strony w ramkach (clickjacking).

```
X-Frame-Options: SAMEORIGIN
```

## X-Content-Type-Options

Blokuje sniffowanie MIME przez przeglądarkę.

```
X-Content-Type-Options: nosniff
```

## Referrer-Policy

Ogranicza informacje o stronie źródłowej wysyłane dalej.

```
Referrer-Policy: strict-origin-when-cross-origin
```

## Permissions-Policy

Ogranicza dostęp do funkcji przeglądarki (kamera, mikrofon itp.).

```
Permissions-Policy: geolocation=(), microphone=()
```

## X-Powered-By / Server

Ukrywa informacje o technologii serwera (np. PHP/8.3.6).

```
Usuń nagłówek X-Powered-By oraz ustaw server_tokens off w nginx.
```

## Instrukcja wdrożenia – nginx

Dodaj poniższe linie do konfiguracji nginx (np. /etc/nginx/sites-available/porolex):

```
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
add_header X-Frame-Options "SAMEORIGIN" always;
add_header X-Content-Type-Options "nosniff" always;
add_header Referrer-Policy "strict-origin-when-cross-origin" always;
add_header Permissions-Policy "geolocation=(), microphone=()" always;
add_header Content-Security-Policy "default-src 'self'; img-src *; script-src 'self' 'unsafe-inline'; style-src 'self'
```

```
'unsafe-inline'" always;
server_tokens off;
```

Po zapisaniu konfiguracji uruchom:

```
sudo nginx -t
sudo systemctl reload nginx
```

## Alternatywa – WordPress

Jeśli nie masz dostępu do konfiguracji serwera, możesz użyć jednej z poniższych wtyczek:

```
- HTTP Headers
- iThemes Security
- Wordfence
- WPS Hide Login
```