PRZYKŁAD. Wymyślony sklep example-shop.pl, wszystkie dane są fikcyjne.

ShieldWave

Poufne

Ocena bezpieczeństwa zewnętrznej aplikacji webowej (black-box)

example-shop.pl

Raport	Data skanowania	Czas trwania
SW-C2A909-MUFGYC3J	23 września 2026, 09:14 UTC	1,4 minuty

Platforma	Serwer	Wykonane moduły
WordPress 6.8.1	nginx	20

Podsumowanie

Dla kierownictwa i DPO

Wynik ekspozycji zewnętrznej

15/100

Poziom ryzyka

Krytyczne

0-25	26-50	51-75	76-100
Krytyczne	Wysokie	Średnie	Niskie

1	5	4	6
krytyczne	wysokie	średnie	niskie

Całkowita liczba ustaleń	Krytyczne + wysokie	Łańcuchy ataków	Pokrycie
16	6	0	100%

Oceniana aplikacja uzyskała wynik ekspozycji zewnętrznej 15 na 100, co wskazuje na krytyczny poziom ryzyka. Natychmiast wymagane są działania naprawy w ciągu 24-48 godzin.

Cel przedstawia krytycznie wysoką pozycję ryzyka. Wymagana jest natychmiastowa naprawa, zanim aplikacja będzie uznana za bezpieczną do użytku produkcyjnego.

Natychmiastowe działania - pierwsze 24 godziny

1. Usuń lub ogranicz dostęp do: `.sql`
2. Wdróż brakujące nagłówki bezpieczeństwa: HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Permissions-Policy
3. Wyłącz niepotrzebne endpointy i usługi eksponowane w internecie

Natychmiast wymagane są działania naprawy. Szczegółowe ustalenia i plan naprawy znajdują się w pełnym raporcie poniżej.

Spis treści

Ten raport przedstawia wyniki zautomatyzowanej oceny bezpieczeństwa aplikacji webowej. Ocena została przeprowadzona przy użyciu silnika skanowania ShieldWave.
Ten raport został przygotowany na podstawie nieinwazyjnej, zewnętrznej oceny bezpieczeństwa przeprowadzonej w modelu black-box. Wszystkie testy zostały wykonane bez jakichkolwiek poświadczeń autentykacji, bez logowania do panelu administracyjnego i bez żadnych działań, które mogłyby zakłócić dostępność lub działanie usługi. Wyniki odzwierciedlają tylko zewnętrzną powierzchnię ataku widoczną z Internetu.

Najważniejsze ustalenia

Najważniejsze ustalenia o krytycznym i wysokim poziomie ważności z oceną exploitability.

Nr	Ważność	Ustalenie	Exploitability	Wysiłek
F-001	Krytyczne	Dostępny wrażliwy plik: /backup.sql	Potwierdzone	Niski
F-002	Wysokie	Wtyczka 'contact-form-7': 5.8.4 (najnowsza: 6.1.5)	Potwierdzone	Wysoki
F-003	Wysokie	Interfejs XML-RPC WordPress jest włączony - może być wykorzystany do ataków brute-force (próbowanie tysięcy kombinacji haseł aż do trafienia właściwego) i DDoS	Potwierdzone	Wysoki
F-004	Wysokie	Brak rekordu DMARC - brak ochrony przed phishingiem	Potwierdzone	Niski
F-005	Wysokie	Brakuje nagłówka Strict-Transport-Security - HTTPS nie jest wymuszane na poziomie przeglądarki	Potwierdzone	Niski
F-006	Wysokie	Brakuje nagłówka Content-Security-Policy - brak ograniczeń ładowania skryptów i zasobów	Potwierdzone	Niski

Szybkie wygrane

Szybkie wygrane to poprawki o małym nakładzie pracy i dużym efekcie. Ten raport zawiera 5 szybkich wygranych, w sekcji Ustalenia z oznaczeniem „Szybka wygrana".

Mocne strony bezpieczeństwa

Pozytywne wskaźniki bezpieczeństwa zaobserwowane podczas zewnętrznego skanowania black-box. Uwaga: brak wykrytych podatności nie gwarantuje ich braku, oznacza jedynie, że automatyczne testy ich nie zidentyfikowały.

- ✓ Nie znaleziono ujawnionych zasobów chmurowych

Ustalenia (16)

Krytyczne F-001 Fakt

Dostępny wrażliwy plik: /backup.sql

https://example-shop.pl/backup.sql

CWE-538 · A01:2021 - Broken Access Control

Cała baza danych lub kopia plików strony jest pobieralna z publicznego URL, kto pobierze, ma kopię wszystkich treści, użytkowników i prawdopodobnie hashe haseł.

Zaufanie	Potwierdzone, 99%
Źródło	info-leak
Wysiłek	Niski · 15 min
Wymagany specjalista	DevOps / administrator serwera / panel hostingu lub Cloudflare

Dowód

```
HTTP 200 - file accessible. Verify: curl -sI "https://example-shop.pl/backup.sql"
```

Ustalenie potwierdzone przez zautomatyzowany skaner bezpieczeństwa na podstawie analizy odpowiedzi serwera.

Co trzeba zrobić

NATYCHMIAST usunąć plik backupu z katalogu publicznego; backupy trzymać poza document root lub w prywatnym storage (S3 z ACL).

Wysokie F-002 Fakt

Wtyczka 'contact-form-7': 5.8.4 (najnowsza: 6.1.5)

https://example-shop.pl/wp-content/plugins/contact-form-7/

Wtyczka jest stara, autor wypuścił aktualizację (często łatającą bezpieczeństwo), ale strona wciąż używa wersji podatnej.

Zaufanie	Potwierdzone, 95%
Źródło	wp-analyzer
Wysiłek	Wysoki · 30 min
Wymagany specjalista	admin WordPress / ktokolwiek z dostępem do FTP

Dowód

Wersja oprogramowania zidentyfikowana na podstawie sygnatur kodu źródłowego, meta tagów lub nagłówków HTTP.

Co trzeba zrobić

Wykonać backup, zaktualizować wtyczki w Kokpit → Wtyczki; jeśli wtyczka jest porzucona (brak aktualizacji 12+ msc), zastąpić alternatywą.

Wysokie F-003 Fakt

Interfejs XML-RPC WordPress jest włączony - może być wykorzystany do ataków brute-force i DDoS

`https://example-shop.pl/xmlrpc.php`

CWE-749 · A01:2021 - Broken Access Control

XML-RPC (stary interfejs WordPressa do zdalnego dostępu, często wykorzystywany przez atakujących do prób zgadywania hasła) pozwala na masowe próbowanie haseł setkami na sekundę w jednym żądaniu, jest jednym z głównych wektorów ataków brute-force na WP.

Zaufanie	Potwierdzone, 95%
Źródło	cms-deep
Wysiłek	Wysoki · 30 min
Wymagany specjalista	admin WordPress / ktokolwiek z dostępem do FTP

Dowód

```
POST /xmlrpc.php system.listMethods returned HTTP 200
```

Endpoint XML-RPC odpowiedział z HTTP 200 i Content-Type: text/xml.

Co trzeba zrobić

Wyłączyć XML-RPC w functions.php (`add_filter xmlrpc_enabled __return_false`) lub wtyczką Disable XML-RPC, albo blokadą w .htaccess/Nginx.

Wysokie F-004 Fakt

Brak rekordu DMARC - brak ochrony przed phishingiem

`https://example-shop.pl`

CWE-290 · A07:2021 - Identification and Authentication Failures

Bez DMARC (polityka mówiąca serwerom pocztowym, co zrobić z mailami podszywającymi się pod Twoją domenę) ochrony Gmail/Outlook nie wiedzą, co zrobić z mailem podszywającym się pod Twoją domenę, często trafia do skrzynki odbiorcy jak legalny.

Zaufanie	Potwierdzone, 95%
Źródło	subdomain-deep
Wysiłek	Niski · 30 min
Wymagany specjalista	DevOps / administrator serwera / panel hostingu lub Cloudflare

Dowód

```
No TXT record at _dmarc.example-shop.pl
```

Weryfikacja rekordu DNS nie znalazła wymaganego rekordu bezpieczeństwa poczty elektronicznej.

Co trzeba zrobić

Dodać rekord TXT na hoście _dmarc.twojadomena.pl: `v=DMARC1; p=none; rua=mailto:dmarc@twojadomena.pl; fo=1`. UWAGA: p=none to wyłącznie monitoring i nie chroni jeszcze przed podszywaniem. Po 4-8 tygodniach analizy raportów przejść na p=quarantine, docelowo p=reject (adkim=s; aspf=s), bo dopiero te polityki realnie blokują phishing. DMARC wymaga działającego SPF i/lub DKIM.

Wysokie F-005 Szybka wygrana Fakt

Brakuje nagłówka Strict-Transport-Security - HTTPS nie jest wymuszane na poziomie przeglądarki

`https://example-shop.pl` CWE-319 · A02:2021 - Cryptographic Failures

Przeglądarka odwiedzającego nie ma instrukcji, żeby ZAWSZE używać HTTPS, w publicznym Wi-Fi (kawiarnia, lotnisko) ktoś może podsłuchać dane logujących się klientów.

Zaufanie	Potwierdzone, 99%
Źródło	headers-deep
Wysiłek	Niski · 30 min
Wymagany specjalista	DevOps / administrator serwera / panel hostingu lub Cloudflare

Dowód

Nagłówek bezpieczeństwa nie został wykryty w odpowiedzi HTTP.
Zweryfikowane przez analizę nagłówka odpowiedzi.

Co trzeba zrobić

Dodać nagłówek `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload` w konfiguracji serwera (Nginx/Apache) lub w panelu Cloudflare.

Wysokie F-006 Szybka wygrana Fakt

Brakuje nagłówka Content-Security-Policy - brak ograniczeń ładowania skryptów i zasobów

https://example-shop.pl CWE-1021 · A05:2021 - Security Misconfiguration

Strona nie ma listy dozwolonych źródeł skryptów (CSP, reguły mówiące przeglądarce, jakie skrypty wolno ładować; chronią przed wstrzyknięciem złośliwego kodu na Twoją stronę), jeśli ktoś wstrzyknie złośliwy kod np. przez komentarz lub formularz, przeglądarki go uruchomią bez ograniczeń.

Zaufanie	Potwierdzone, 99%
Źródło	headers-deep
Wysiłek	Niski · 30 min
Wymagany specjalista	programista WordPress / PHP (mid+)

Dowód

Nagłówek bezpieczeństwa nie został wykryty w odpowiedzi HTTP.
Zweryfikowane przez analizę nagłówka odpowiedzi.

Co trzeba zrobić

Dodać nagłówek Content-Security-Policy w konfiguracji serwera; zacząć od raportowania (Report-Only) i stopniowo zaostrzać.

Średnie F-007 Fakt

Certyfikat SSL wygasa za 19 dni

https://example-shop.pl CWE-295 · A02:2021 - Cryptographic Failures

Zaufanie	Potwierdzone, 95%
Źródło	ssl-deep

Średnie F-008 Szybka wygrana Fakt

Brakuje nagłówka X-Frame-Options - strona może być podatna na clickjacking

https://example-shop.pl CWE-1021 · A05:2021 - Security Misconfiguration

Ktoś może wczytać Twoją stronę w ukrytej ramce na fałszywej stronie i podstępem nakłonić użytkownika do kliknięcia czegoś, czego nie chciał kliknąć (clickjacking: technika nakłaniająca użytkownika do kliknięcia w coś innego niż widzi).

Zaufanie	Silny sygnał, 84%
Źródło	headers-deep
Wymagany specjalista	DevOps / administrator serwera / panel hostingu lub Cloudflare

Co trzeba zrobić

Dodać nagłówek `X-Frame-Options: DENY` (lub odpowiedni `frame-ancestors` w CSP) w konfiguracji serwera.

Średnie F-009 Szybka wygrana Fakt

Brakuje nagłówka X-Content-Type-Options - wykrywanie typów MIME nie jest blokowane

`https://example-shop.pl` CWE-16 · A05:2021 - Security Misconfiguration

Bez wyraźnej instrukcji przeglądarki same zgadują typ pliku, wgrany plik z fałszywym rozszerzeniem może zostać uruchomiony jako skrypt.

Zaufanie	Potwierdzone, 99%
Źródło	headers-deep
Wymagany specjalista	DevOps / administrator serwera / panel hostingu lub Cloudflare

Co trzeba zrobić

Dodać nagłówek `X-Content-Type-Options: nosniff` w konfiguracji serwera.

Średnie F-010 Fakt

Wersja PHP ujawniona przez nagłówek X-Powered-By: PHP/8.1.29, ułatwia ukierunkowane ataki

`https://example-shop.pl` CWE-200 · A01:2021 - Broken Access Control

Nagłówek X-Powered-By: PHP/x.y.z pokazuje dokładną wersję PHP, jeśli wersja jest po EOL (np. 7.4), atak jest wstępnie przygotowany pod tę wersję.

Zaufanie	Potwierdzone, 95%
Źródło	wp-hardening
Wymagany specjalista	DevOps / administrator serwera / panel hostingu lub Cloudflare

Co trzeba zrobić

W php.ini ustawić `expose_php = Off`; zaktualizować PHP do wspieranej wersji (8.2+).

Niskie F-011 Fakt

Wersja WordPress 6.8.1 jest ujawniana w tagu meta generator, ułatwia ukierunkowane ataki

https://example-shop.pl CWE-200 · A01:2021 - Broken Access Control

Wersja WP widoczna w meta tagu HTML, RSS i nagłówkach, jeśli jest stara, każdy automatyczny skaner od razu wie, którą podatność spróbować.

Zaufanie	Potwierdzone, 95%
Źródło	wp-hardening
Wymagany specjalista	admin WordPress / ktokolwiek z dostępem do FTP

Co trzeba zrobić

Dodać kod usuwający tag generator (`remove_action wp_head, the_generator`); rozważyć wtyczkę hardening (Wordfence, iThemes Security).

Niskie F-012 Fakt

Plik readme.txt wtyczki "woocommerce" jest dostępny (wersja 9.9.5), ujawnia wersję ułatwiając ukierunkowane ataki

https://example-shop.pl/wp-content/plugins/woocommerce/readme.txt
CWE-200 · A01:2021 - Broken Access Control

Zaufanie	Potwierdzone, 95%
Źródło	wp-deep

Niskie F-013 Fakt

Nie wykryto uwierzytelniania dwuskładnikowego ani wtyczki bezpieczeństwa logowania na stronie logowania

https://example-shop.pl/wp-login.php
CWE-308 · A07:2021 - Identification and Authentication Failures

Jedynym zabezpieczeniem konta admin jest hasło, jeśli wycieknie (phishing, reused password z innego serwisu), nic nie blokuje wejścia.

Zaufanie	Potwierdzone, 95%
Źródło	wp-deep
Wymagany specjalista	admin WordPress / ktokolwiek z dostępem do FTP

Co trzeba zrobić

Włączyć 2FA wtyczką (Wordfence Login Security, WP 2FA, miniOrange) dla wszystkich kont z rolą wyższą niż Subscriber.

Niskie F-014 Szybka wygrana Fakt

Brakuje nagłówka Permissions-Policy - funkcje przeglądarki nie są jawnie ograniczone

https://example-shop.pl CWE-16 · A05:2021 - Security Misconfiguration

Złośliwy skrypt wstrzyknięty na stronę mógłby teoretycznie poprosić o dostęp do kamery lub lokalizacji odwiedzającego, podszywając się pod Twoją domenę.

Zaufanie	Potwierdzone, 99%
Źródło	headers-deep
Wymagany specjalista	DevOps / administrator serwera / panel hostingu lub Cloudflare

Co trzeba zrobić

Dodać nagłówek Permissions-Policy z explicite zablokowanymi funkcjami (`camera=(), microphone=(), geolocation=()`).

Niskie F-015 Sygnał

DNSSEC nie jest włączone, odpowiedzi DNS nie są podpisane kryptograficznie, co zwiększa ryzyko fałszowania DNS

https://example-shop.pl

CWE-350 · A07:2021 - Identification and Authentication Failures

Ktoś atakujący sieć (np. publiczne Wi-Fi w hotelu) może zafałszować odpowiedź DNS i przekierować Twoich klientów na fałszywą stronę z Twoją domeną w pasku (DNSSEC: mechanizm cyfrowo podpisujący odpowiedzi DNS, bez niego atakujący może przekierować klientów na fałszywą stronę).

Zaufanie	Heurystyka, 60%
Źródło	subdomain-deep
Wymagany specjalista	DevOps / administrator serwera / panel hostingu lub Cloudflare

Co trzeba zrobić

W panelu rejestratora domeny (lub Cloudflare) włączyć DNSSEC, dodać rekord DS u rejestratora, proces zajmuje do 48h propagacji.

Niskie F-016 Sygnał

Brak rekordów CAA, dowolny urząd certyfikacji może wydać certyfikaty SSL dla tej domeny

https://example-shop.pl CWE-295 · A02:2021 - Cryptographic Failures

Bez CAA (rekord mówiący, kto może wystawiać certyfikaty SSL dla Twojej domeny, utrudnia atakującym wystawienie fałszywego certyfikatu) dowolna instytucja certyfikująca (CA) może wystawić ważny certyfikat HTTPS dla Twojej domeny, jeśli któraś zostanie zhakowana, ktoś może podszyć się pod Twoją stronę.

Zaufanie	Heurystyka, 60%
Źródło	subdomain-deep
Wymagany specjalista	DevOps / administrator serwera / panel hostingu lub Cloudflare

Co trzeba zrobić

Dodać rekord CAA w DNS: `0 issue "letsencrypt.org"` (lub Twój CA), ograniczy wystawianie certów tylko do listy zaufanych.

Łańcuchy ataków (0)

Nie zidentyfikowano wieloetapowych łańcuchów ataków na podstawie kombinacji wykrytych ustaleń.

Analiza powierzchni ataku

Analiza powierzchni ataku oparta na AI nie była dostępna dla tego skanu. Wykryte ustalenia i ich dowody znajdziesz w pozostałych sekcjach raportu.

Plan naprawy

Priorytetowy plan naprawy oparty na ważności, możliwości eksploatacji i wpływie na biznes.

0-24h
Natychmiastowe

F-001 Dostępny wrażliwy plik: /backup.sql

1-7 dni
Krótkoterminowe

F-002 Wtyczka 'contact-form-7': 5.8.4 (najnowsza: 6.1.5)

F-003 Interfejs XML-RPC WordPress jest włączony - może być wykorzystany do ataków brute-force i DDoS

F-004 Brak rekordu DMARC - brak ochrony przed phishingiem

F-005 Brakuje nagłówka Strict-Transport-Security - HTTPS nie jest wymuszane na poziomie przeglądarki

F-006 Brakuje nagłówka Content-Security-Policy - brak ograniczeń ładowania skryptów i zasobów

---

1-3 miesiące
Średnioterminowe

F-007 Certyfikat SSL wygasa za 19 dni

F-008 Brakuje nagłówka X-Frame-Options - strona może być podatna na clickjacking

F-009 Brakuje nagłówka X-Content-Type-Options - wykrywanie typów MIME nie jest blokowane

F-010 Wersja PHP ujawniona przez nagłówek X-Powered-By: PHP/8.1.29, ułatwia ukierunkowane ataki

---

ciągłe
Strategiczne

F-011 Wersja WordPress 6.8.1 jest ujawniana w tagu meta generator, ułatwia ukierunkowane ataki

F-012 Plik readme.txt wtyczki "woocommerce" jest dostępny (wersja 9.9.5), ujawnia wersję ułatwiając ukierunkowane ataki

F-013 Nie wykryto uwierzytelniania dwuskładnikowego ani wtyczki bezpieczeństwa logowania na stronie logowania

F-014 Brakuje nagłówka Permissions-Policy - funkcje przeglądarki nie są jawnie ograniczone

F-015 DNSSEC nie jest włączone, odpowiedzi DNS nie są podpisane kryptograficznie, co zwiększa ryzyko fałszowania DNS

F-016 Brak rekordów CAA, dowolny urząd certyfikacji może wydać certyfikaty SSL dla tej domeny

---

Właściciele i terminy

Nr	Ważność	Ustalenie	Wysiłek · szacunek czasu	Priorytet · data docelowa	Status
F-001	Krytyczne	Dostępny wrażliwy plik: /backup.sql	Niski 15 min	Wysoki 24h	Otwarty
F-002	Wysokie	Wtyczka 'contact-form-7': 5.8.4 (najnowsza: 6.1.5)	Wysoki 30 min	Wysoki 7 dni	Otwarty
F-003	Wysokie	Interfejs XML-RPC WordPress jest włączony - może być wykorzystany do ataków brute-force i DDoS	Wysoki 30 min	Wysoki 7 dni	Otwarty
F-004	Wysokie	Brak rekordu DMARC - brak ochrony przed phishingiem	Niski 30 min	Wysoki 7 dni	Otwarty
F-005	Wysokie	Brakuje nagłówka Strict-Transport-Security - HTTPS nie jest wymuszane na poziomie przeglądarki	Niski 30 min	Wysoki 7 dni	Otwarty
F-006	Wysokie	Brakuje nagłówka Content-Security-Policy - brak ograniczeń ładowania skryptów i zasobów	Niski 30 min	Wysoki 7 dni	Otwarty

Brief dla wykonawcy

Gotowa wiadomość do osoby, która wprowadzi poprawki. Skopiuj tekst i wyślij razem z tym raportem.

Dzień dobry,

przesyłam wyniki zewnętrznego skanu bezpieczeństwa strony example-shop.pl z 23 września 2026. Proszę o wycenę i termin realizacji poniższych poprawek.

Natychmiastowe (0-24h):
1. Dostępny wrażliwy plik: /backup.sql

Krótkoterminowe (1-7 dni):
2. Wtyczka 'contact-form-7': 5.8.4 (najnowsza: 6.1.5)
3. Interfejs XML-RPC WordPress jest włączony - może być wykorzystany do ataków brute-force i DDoS
4. Brak rekordu DMARC - brak ochrony przed phishingiem
5. Brakuje nagłówka Strict-Transport-Security - HTTPS nie jest wymuszane na poziomie przeglądarki
6. Brakuje nagłówka Content-Security-Policy - brak ograniczeń ładowania skryptów i zasobów

Średnioterminowe (1-3 miesiące):
7. Certyfikat SSL wygasa za 19 dni
8. Brakuje nagłówka X-Frame-Options - strona może być podatna na clickjacking

9. Brakuje nagłówka X-Content-Type-Options - wykrywanie typów MIME nie jest blokowane
10. Wersja PHP ujawniona przez nagłówek X-Powered-By: PHP/8.1.29, ułatwia ukierunkowane ataki

Strategiczne (ciągłe):
11. Wersja WordPress 6.8.1 jest ujawniana w tagu meta generator, ułatwia ukierunkowane ataki
12. Plik readme.txt wtyczki "woocommerce" jest dostępny (wersja 9.9.5), ujawnia wersję ułatwiając ukierunkowane ataki
13. Nie wykryto uwierzytelniania dwuskładnikowego ani wtyczki bezpieczeństwa logowania na stronie logowania
14. Brakuje nagłówka Permissions-Policy - funkcje przeglądarki nie są jawnie ograniczone
15. DNSSEC nie jest włączone, odpowiedzi DNS nie są podpisane kryptograficznie, co zwiększa ryzyko fałszowania DNS

...oraz 1 pozostała poprawka opisana w raporcie.

Pełny raport z dowodami (adresy URL, odpowiedzi serwera) jest w załączniku.
Po wdrożeniu zmian proszę o krótką informację, co zostało zrobione. Ponowny skan potwierdzi naprawę.

Pozdrawiam,
[Imię i nazwisko]

Plan retestowania i walidacji

Planowane działania walidacyjne w celu potwierdzenia skuteczności naprawy.

Nr	Ważność	Ustalenie	Zakres retestowania	Kryteria sukcesu
F-001	Krytyczne	Dostępny wrażliwy plik: /backup.sql	Weryfikacja dostępu do pliku	Zwrócono HTTP 403/404
F-002	Wysokie	Wtyczka 'contact-form-7': 5.8.4 (najnowsza: 6.1.5)	Weryfikacja wersji	Najnowsza wersja potwierdzona
F-003	Wysokie	Interfejs XML-RPC WordPress jest włączony - może być wykorzystany do ataków brute-force i DDoS	Weryfikacja wersji	Najnowsza wersja potwierdzona
F-004	Wysokie	Brak rekordu DMARC - brak ochrony przed phishingiem	Pełne ponowne skanowanie	Nie wykryto problemu
F-005	Wysokie	Brakuje nagłówka Strict-Transport-Security - HTTPS nie jest wymuszane na poziomie przeglądarki	Weryfikacja nagłówka	Nagłówek obecny w odpowiedzi
F-006	Wysokie	Brakuje nagłówka Content-Security-Policy - brak ograniczeń ładowania skryptów i zasobów	Weryfikacja nagłówka	Nagłówek obecny w odpowiedzi

Ryzyko pozostałe i akceptacja ryzyka

Pozostałe ryzyko po naprawie i obszary wymagające decyzji biznesowej.

Ryzyko pozostałe	Ważność	Jeśli pozostanie nierozwiązane	Wymagana akceptacja
Dostępny wrażliwy plik: /backup.sql	Krytyczne	Exploitability: Potwierdzone	CTO/CISO
Wtyczka 'contact-form-7': 5.8.4 (najnowsza: 6.1.5)	Wysokie	Exploitability: Potwierdzone	IT Admin
Interfejs XML-RPC WordPress jest włączony - może być wykorzystany do ataków brute-force i DDoS	Wysokie	Exploitability: Potwierdzone	IT Admin

Wnioski końcowe

Krytyczne

Poziom ryzyka ekspozycji zewnętrznej dla example-shop.pl jest oceniany jako krytyczny z wynikiem ekspozycji 15/100. 1 ustalenie krytyczne wymaga natychmiastowej uwagi w ciągu 24 godzin. 5 ustaleń o wysokiej ważności powinno być rozwiązanych w ciągu 7 dni.

Wymagane kluczowe decyzje

Natychmiast	Zablokuj dostęp do wrażliwych plików i zbadaj alerty bezpieczeństwa
Krótkoterminowo	Zastosuj wszystkie zalecane poprawki i konfiguracje
Strategicznie	Ustanów ciągły proces monitorowania bezpieczeństwa i naprawy z określonymi SLA

Rekomendacje dla dalszych działań

Na podstawie wyników oceny rekomendowane są następujące dodatkowe działania.

Test penetracyjny ręczny	Skaner automatyczny wykrył 1 krytyczne i 5 wysokich ustaleń, które wymagają ręcznej weryfikacji i głębszych testów eksploatacji przez wykwalifikowanego specjalistę bezpieczeństwa.

Okresowe skanowania bezpieczeństwa	Zaplanuj regularne zautomatyzowane skanowania (tygodniowo lub miesięcznie), aby wykryć nowe luki wprowadzone przez aktualizacje lub zmiany konfiguracji.
Monitorowanie bezpieczeństwa ciągłe	Wdróż monitorowanie w czasie rzeczywistym: nieautoryzowane próby dostępu, zmiany integralności plików i zgodność nagłówków bezpieczeństwa.

Co dalej? 4 ścieżki działania

Mam swojego informatyka

Wyślij mu ten raport razem z gotową wiadomością z sekcji Brief dla wykonawcy. Wszystkie potrzebne informacje techniczne (URL-e, CWE, dowody) znajdzie w sekcjach Ustalenia i Dodatek dowodów.

Szukam wykonawcy

Skopiuj brief i wyślij do 2-3 deweloperów webowych lub firm IT. Sugerowane platformy: Useme, LinkedIn, lokalne grupy IT. Porównaj wyceny.

Zlecam naprawę ShieldWave

Zrealizujemy wszystkie naprawy z raportu. Szacowany czas: 4-8h pracy + ponowny audyt weryfikacyjny.

Zamów wycenę

Pytania o RODO

Ten raport opisuje stan techniczny strony i nie jest oceną zgodności z RODO. Jeśli jej potrzebujesz, przekaż wyniki swojemu inspektorowi ochrony danych (IOD) lub prawnikowi.

Pytania? Napisz: security@shieldwave.io

Ryzyka prawne i reputacyjne

Ryzyka prawne wynikające z ustaleń bezpieczeństwa technicznego. Sekcja ta nie stanowi porady prawnej.

RODO / ochrona danych	Ujawnione pliki konfiguracyjne lub diagnostyczne mogą stanowić naruszenie art. 32 RODO (brak odpowiednich środków technicznych ochrony danych osobowych). Zakres obowiązków i ocenę prawną ustali Twój inspektor ochrony danych lub prawnik.
Ujawnienie danych uwierzytelniających	Publicznie dostępne pliki konfiguracyjne lub dzienniki debugowania mogą zawierać dane uwierzytelniające, klucze API lub szczegóły infrastruktury wewnętrznej.

Nieautoryzowany dostęp	Słabe mechanizmy uwierzytelniania (widoczna strona logowania, XML-RPC, enumeracja użytkowników) zwiększają ryzyko przejęcia konta i nieuprawnionego dostępu do danych.

Wpływ na prywatność i GDPR

Ocena ryzyk ochrony danych zgodnie z GDPR i obowiązującymi przepisami o ochronie prywatności.

Szczegółowa analiza wpływu na RODO nie była dostępna dla tego skanu. Ustalenia techniczne z tego raportu możesz przekazać swojemu inspektorowi ochrony danych lub prawnikowi.

Ocena wpływu na biznes

Ocena biznesowych, brandowych i operacyjnych ryzyk wynikających z ustaleń bezpieczeństwa.

- Wykryto 1 krytyczne ustalenie, które może prowadzić do pełnego przejęcia systemu, naruszenia danych lub zakłócenia usług.
- 5 problemów wysokiego priorytetu, które można wykorzystać przy umiarkowanym wysiłku, wymagających natychmiastowej uwagi.
- Ujawnione pliki konfiguracyjne i diagnostyczne mogą potencjalnie zawierać dane uwierzytelniające lub informacje o infrastrukturze, co zwiększa powierzchnię ataku.
- Koncentracja wielu ustaleń o podwyższonym ryzyku zwiększa prawdopodobieństwo, że poszczególne podatności mogą być łączone w bardziej złożone scenariusze.

Zakres

Typ skanowania	Smart Scan (zautomatyzowany, nieinwazyjny)
Silnik	SmartScanEngine v1.0

20 stron przeskanowanych · 4 formularze · 6 endpointów API

Przegląd zaangażowania

Parametry oceny, zasady zaangażowania i zakres testowania.

Typ oceny	Ocena Bezpieczeństwa Zewnętrznej Aplikacji Webowej
Podejście testowania	Black-box, bez autentykacji, nieinwazyjne (tylko do odczytu)
Okno testowania	23 września 2026, 09:14 UTC
Autoryzacja	Skanowanie zautomatyzowane autoryzowane przez właściciela konta
Poza zakresem	Testowanie DDoS, credential stuffing, destrukcyjne payloads, sieć wewnętrzna, konta e-mail
Ograniczenia	Brak eksploatacji. Wszystkie testy tylko do odczytu. Liczba zapytań jest ograniczona, aby nie zakłócić działania usługi.

Macierz pokrycia testów

Obszar testowania	Metoda	Status	Powód
Nagłówki bezpieczeństwa HTTP	Zautomatyzowane	Testowano	
Konfiguracja TLS / SSL	Zautomatyzowane	Testowano	
Bezpieczeństwo platformy (WordPress)	Zautomatyzowane	Testowano	
Zależności i komponenty	Zautomatyzowane	Nie w zakresie skanowania	Nie dotyczy wykrytej platformy
Ekspozycja wrażliwych plików	Zautomatyzowane	Testowano	
Walidacja formularzy i danych	Zautomatyzowane	Testowano	
Podatności JavaScript	Zautomatyzowane	Testowano	
Bezpieczeństwo API	Zautomatyzowane	Nie w zakresie skanowania	Nie dotyczy wykrytej platformy
Bezpieczeństwo ciasteczek	Zautomatyzowane	Testowano	
Identyfikacja technologii	Zautomatyzowane	Testowano	
Enumeracja subdomen	Zautomatyzowane	Testowano	
SQL Injection	Zautomatyzowane	Testowano	
SSRF	Zautomatyzowane	Nie w zakresie skanowania	Nie dotyczy wykrytej platformy
Path Traversal	Zautomatyzowane	Testowano	
Wykrywanie malware	Zautomatyzowane	Testowano	

Obszar testowania	Metoda	Status	Powód
Ekspozycja chmury	Zautomatyzowane	Testowano	
Skanowanie portów	Zautomatyzowane	Nie w zakresie skanowania	Nie dotyczy wykrytej platformy
Wydajność i cache	Zautomatyzowane	Testowano	

Poza zakresem zautomatyzowanego skanowania: Ta zautomatyzowana ocena działa wyłącznie z zewnętrznej perspektywy (black-box), analizując tylko dane dostępne bez autentykacji. W związku z tym dostarcza weryfikowalnych spostrzeżeń na temat zewnętrznej powierzchni ataku, ale nie może ocenić wewnętrznych kontroli bezpieczeństwa, funkcjonalności uwierzytelnionej lub logiki biznesowej.

Co ta ocena może i nie może udowodnić

Ta ocena potwierdza

- ✓ Obecność lub brak nagłówków bezpieczeństwa HTTP
- ✓ Publiczna dostępność wrażliwych plików i katalogów
- ✓ Wersje oprogramowania i znane luki (CVE)
- ✓ Konfiguracja SSL/TLS i certyfikatu
- ✓ Zewnętrzna powierzchnia ataku widoczna z Internetu

Wymaga dodatkowej analizy

- – Obszary wymagające autentykacji (panele administracyjne, interfejsy API oparte na tokenach)
- – Logika biznesowa i procesy transakcji
- – Infrastruktura wewnętrzna i sieć
- – Pełna exploitability wykrytych luk (testowanie nieniszczące)

Ta ocena obejmuje tylko zewnętrzną powierzchnię ataku. Brak wykrycia w danym obszarze nie gwarantuje braku luk.

Model oceny ryzyka

Metodologia używana do obliczania wyników bezpieczeństwa, poziomów ważności i ocen zaufania.

Ważność	Zakres wyniku	Opis	Priorytet naprawy
Krytyczne	0-25	Aktywnie exploitable luki z bezpośrednim wpływem na biznes	Natychmiast (0-24h)
Wysokie	26-50	Znaczące luki wymagające szybkiej uwagi	Pilnie (1-7 dni)
Średnie	51-75	Umiarkowane ryzyka z ograniczoną exploitability	Zaplanowane (7-30 dni)
Niskie	76-100	Ustalenia informacyjne i rekomendacje hartowania	Doradztwo (30-90 dni)

Zaufanie	Wyniki zaufania (0-100%) odzwierciedlają niezawodność skanera, walidację krzyżową między modułami i szczegółowość dowodów. Ustalenia poniżej 50% zaufania wskazują na detekcję opartą na wzorcach, która wymaga ręcznej weryfikacji.
Exploitability	Exploitability oceniana jest jako Potwierdzona (zweryfikowana przez wiele sygnałów), Teoretyczna (pojedynczy sygnał) lub Mało Prawdopodobna (dopasowanie wzorca o niskim poziomie zaufania).

Ekspozycja zasobów i danych

Mapowanie ekspozycji zasobów na kategorie danych biznesowych i wpływ.

Ustalenie	Ważność	Źródło
Dostępny wrażliwy plik: /backup.sql	Krytyczne	info-leak
Plik readme.txt wtyczki "woocommerce" jest dostępny (wersja 9.9.5), ujawnia wersję ułatwiając ukierunkowane ataki	Niskie	wp-deep

Kontekst regulacyjny (Polska)

Główne prawo ochrony danych	RODO (Rozporządzenie Ogólne o Ochronie Danych Osobowych) [RODO]
Krajowa ustawa wdrażająca	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych
Prawo cyberbezpieczeństwa	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
Prawo cookies / ePrivacy	Ustawa z dnia 12 lipca 2024 r., Prawo komunikacji elektronicznej
Organ nadzorczy	Urząd Ochrony Danych Osobowych (UODO)
Termin zgłoszenia naruszenia	72 godziny od stwierdzenia naruszenia (Art. 33 RODO)
Maksymalna kara finansowa	w kontekście art. 32 RODO (obowiązek odpowiednich środków technicznych i organizacyjnych)

Zastrzeżenie

Niniejszy raport stanowi zewnętrzną ocenę bezpieczeństwa aplikacji webowej metodą black-box. Nie zastępuje audytu zgodności z RODO przeprowadzonego przez wykwalifikowanego IOD lub audytora. Ustalenia opierają się na publicznie dostępnych informacjach (odpowiedzi HTTP, nagłówki, DNS) i mogą nie odzwierciedlać pełnego stanu zabezpieczeń wewnętrznych. Rekomendacje powinny być skonsultowane z IOD przed wdrożeniem.

Metodologia i zakres oceny

Ten raport został przygotowany w oparciu o nieinwazyjną metodę **black-box**, czyli z perspektywy potencjalnego atakującego, bez logowania do panelu i bez dostępu do serwera. To ta sama perspektywa, z której Twoją witrynę widzą tysiące automatycznych narzędzi skanujących internet w poszukiwaniu celów.

Zakres tej oceny	wykryte i udokumentowane podatności w warstwie sieciowej i aplikacyjnej, obejmujące ekspozycję plików, nagłówki bezpieczeństwa HTTP, konfigurację TLS/SSL, wersje oprogramowania (CMS, wtyczki), uwierzytelnianie e-mail (SPF (rekord mówiący, jakie serwery mogą wysyłać maile w imieniu Twojej domeny, zapobiega podszywaniu się pod Twój adres), DKIM (cyfrowy podpis maili wysyłanych z Twojej domeny, odbiorca może zweryfikować, że mail naprawdę pochodzi od Ciebie), DMARC), rekordy DNS oraz wskaźniki kompromitacji. Wykryte podatności są udokumentowane dowodami technicznymi, zebranymi w sekcji Pełny rejestr dowodów, i sklasyfikowane według CWE i OWASP Top 10.
Poza zakresem tego raportu	ocena zgodności z RODO, czyli rejestr czynności przetwarzania, umowy powierzenia, polityki bezpieczeństwa i procedury. Jeśli jej potrzebujesz, przekaż wyniki swojemu inspektorowi ochrony danych (IOD) lub prawnikowi.
Obszary uzupełniające (poza zakresem tego audytu)	ręczny test penetracyjny z aktywnym wykorzystaniem podatności, audyt kodu źródłowego aplikacji oraz ocena bezpieczeństwa procesów wewnętrznych (uprawnienia, kopie zapasowe, plan reagowania na incydenty). Dla witryn o wysokim profilu ryzyka rekomendujemy uzupełnienie skanu zewnętrznego o powyższe elementy realizowane przez wyspecjalizowane firmy pentesterskie.
Rekomendacja	dla witryn przetwarzających dane osobowe klientów lub realizujących płatności online warto powtarzać taką ocenę co 6-12 miesięcy oraz po każdej większej zmianie na stronie.

To skanowanie zostało automatycznie dodane do Historii skanowania i listy Moje witryny w Twoim panelu ShieldWave.

Dodatek dowodów

Dowody techniczne wspierające kluczowe ustalenia: adresy URL, nagłówki, dane odpowiedzi.

Nr	Ważność	Ustalenie	Dowód	Źródło
F-001	Krytyczne	Dostępny wrażliwy plik: /backup.sql	`HTTP 200 - file accessible. Verify: curl -sI "https://example-shop.pl/backup.sql"`	info-leak zaufanie 99%
F-003	Wysokie	Interfejs XML-RPC WordPress jest włączony - może być wykorzystany do ataków brute-force i DDoS	`POST /xmlrpc.php system.listMethods returned HTTP 200`	cms-deep zaufanie 95%
F-004	Wysokie	Brak rekordu DMARC - brak ochrony przed phishingiem	`No TXT record at _dmarc.example-shop.pl`	subdomain-deep zaufanie 95%

ShieldWave

Zewnętrzny audyt bezpieczeństwa stron internetowych

Raport przygotowany przez
ShieldWave Zespół Bezpieczeństwa
security@shieldwave.io

Raport
SW-C2A909-MUFGYC3J

Data
23 września 2026

Witryna
shieldwave.io

Wsparcie
support@shieldwave.io

Zlecenia i wycena
security@shieldwave.io