

Raport z audytu bezpieczeństwa

Sklep Przykładowy

sklep-przykladowy.example

Audyt rozszerzony sklepu WooCommerce

Zleceniodawca

Przykładowa Firma Sp. z o.o.

Wykonawca

Marcin Zagórski, Vertiso

Termin testów

14–18 września 2026

Data raportu i wersja

22 września 2026, wersja 1.0

To przykładowy raport. Firma, serwis i wyniki są wymyślone i nie dotyczą żadnego rzeczywistego klienta. Dokument pokazuje, jak wygląda raport i jak opisuję problemy. Prawdziwy raport jest poufny i przekazywany wyłącznie zleceniodawcy.

1 Podsumowanie dla właściciela

Sklep działa poprawnie, ale w jego konfiguracji wykryto **14 problemów, w tym dwa krytyczne**. Najpoważniejszy to przestarzała wtyczka formularza ze znaną podatnością: pozwala osobie nieuprawnionej wykonać własny kod na serwerze. Drugi krytyczny dotyczy modułu napisanego na zamówienie: przez niego można odczytać i zmienić dane w bazie sklepu.

Podczas testów na działającym sklepie nic nie zostało zmienione. Zalecam zacząć od czterech poprawek poniżej, najlepiej w ciągu kilku dni.

2 ● Krytyczne	4 ● Wysokie	5 ● Średnie	3 ● Niskie
-------------------------	-----------------------	-----------------------	----------------------

Od czego zacząć

1	Zaktualizować lub usunąć wtyczkę formularza VT-01 · Pozwala przejść sklep bez logowania	1 godz.
2	Usunąć kopię bazy z katalogu publicznego i przenieść kopie poza serwer VT-04 · Każdy może pobrać dane klientów	2 godz.
3	Zablokować konta administratorów dawnych współpracowników VT-05 · Zapomniane konta z pełnymi uprawnieniami	1 godz.
4	Poprawić zapytanie w module filtrowania produktów VT-02 · Wymaga pracy programisty	4 godz.

Te cztery poprawki zajmą około **8 godz.** pracy, wszystkie 14 około **23 godz.**

Co jest w porządku

- ✓ WordPress, WooCommerce i motyw działają w aktualnych wersjach.
- ✓ Certyfikat HTTPS jest poprawny, a strona wymusza połączenie szyfrowane.
- ✓ Płatności obsługuje zewnętrzna bramka, więc dane kart nie trafiają na serwer sklepu.
- ✓ W plikach i bazie nie znaleziono śladów włamania ani złośliwego kodu.

2 Zakres i metodyka

Obiekt testów	serwis sklep-przykładowy.example: WordPress, WooCommerce, wtyczki, motyw oraz moduł napisany na zamówienie
Rodzaj audytu	audyt rozszerzony: osiem obszarów, w tym przegląd kodu własnych modyfikacji i test procesu zakupowego
Perspektywy testów	anonimowy odwiedzający, klient z kontem, administrator (konto testowe)
Bezpieczeństwo testów	testy ingerujące w serwis wykonano na kopii, na działającym sklepie wyłącznie odczyty
Metodyka	OWASP Web Security Testing Guide, ocena wagi w skali CVSS v3.1

Obszary i liczba znalezionych problemów

Obszar	Liczba	Identyfikatory
Aktualność systemu	2	VT-01, VT-10
Konta i uprawnienia	3	VT-03, VT-05, VT-09
Serwer i konfiguracja	4	VT-06, VT-07, VT-12, VT-13
Kopie zapasowe	1	VT-04
Dane klientów	1	VT-14
Ślady wirusa	0	nie znaleziono problemów
Kod własnych modyfikacji	1	VT-02
Proces zakupowy	2	VT-08, VT-11

Źródła: OWASP Web Security Testing Guide (owasp.org/www-project-web-security-testing-guide); FIRST, CVSS v3.1 Specification Document (first.org/cvss/v3.1/specification-document).

3 Lista problemów

Problemy są pogrupowane według wagi. Każdy z nich opisuję w rozdziale 4.

ID	Problem	CVSS	Waga
VT-01	Przestarzała wtyczka formularza ze znaną podatnością	9,8	● Krytyczne
VT-02	Wstrzyknięcie SQL w module filtrowania produktów	9,1	● Krytyczne
VT-03	Panel logowania bez limitu prób	7,5	● Wysokie
VT-04	Kopia zapasowa bazy danych dostępna z internetu	7,5	● Wysokie
VT-05	Konta byłych współpracowników z pełnymi uprawnieniami	8,1	● Wysokie
VT-06	Wgranie pliku wykonywalnego przez formularz opinii	8,8	● Wysokie
VT-07	Ujawnianie wersji oprogramowania	5,3	● Średnie
VT-08	Ciasteczko sesji koszyka bez zabezpieczających flag	4,2	● Średnie
VT-09	Loginy użytkowników widoczne dla każdego	5,3	● Średnie
VT-10	Nieużywane wtyczki i motywy zostawione na serwerze	5,6	● Średnie
VT-11	Brak limitu prób przy kodach rabatowych	6,5	● Średnie
VT-12	Brak części nagłówków bezpieczeństwa	3,7	● Niskie
VT-13	Włączone przestarzałe wersje protokołu TLS	3,7	● Niskie
VT-14	Brak wymagań co do siły haseł klientów	3,1	● Niskie

Skala wag (CVSS v3.1): krytyczne 9,0–10,0, wysokie 7,0–8,9, średnie 4,0–6,9, niskie 0,1–3,9. Ocena opisuje wagę techniczną problemu, a nie jego wpływ na Twój biznes, dlatego o kolejności napraw (rozdział 5) decyduje też łatwość wykorzystania błędu i nakład na poprawkę.

4 Opis problemów

VT-01 ● Krytyczne

CVSS 9,8

Przestarzała wtyczka formularza ze znaną podatnością

Co znaleziono	Zainstalowana wersja wtyczki do formularzy jest o kilka wydań starsza od bieżącej i zawiera podatność opisaną przez producenta w informacji o wydaniu. Błąd można wykorzystać bez logowania.
Czym grozi	Możliwość wykonania dowolnego kodu na serwerze, przejęcia sklepu i dostępu do danych klientów.
Jak naprawić	Zaktualizować wtyczkę do wersji z poprawką albo ją usunąć. Po zmianie sprawdzić działanie formularzy i zamówień.

Gdzie: wtyczka formularzy kontaktowych, zainstalowana wersja 4.3.1, aktualna 4.6.2 Nakład: 1 godz.
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

VT-02 ● Krytyczne

CVSS 9,1

Wstrzyknięcie SQL w module filtrowania produktów

Co znaleziono	Moduł wstawia wartość parametru sortowania z adresu strony wprost do zapytania do bazy danych, bez zabezpieczenia. Test na kopii sklepu potwierdził, że w ten sposób da się odczytać dane z innych tabel.
Czym grozi	Odczyt i zmiana danych w bazie sklepu bez logowania, w tym zamówień, danych klientów i skrótów haseł.
Jak naprawić	Przepisać zapytanie na zapytanie z parametrami i dopuścić tylko z góry znane wartości sortowania. Sprawdzić pozostałe miejsca modułu, które budują zapytania z danych od użytkownika.

Gdzie: moduł napisany na zamówienie, parametr sortowania w adresie listy produktów Nakład: 4 godz.
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

VT-03 ● Wysokie

CVSS 7,5

Panel logowania bez limitu prób

Co znaleziono	Formularz logowania do panelu administracyjnego nie ogranicza liczby nieudanych prób ani nie wymaga drugiego składnika.
Czym grozi	Automat może zgadywać hasła do skutku, a przejęte konto daje dostęp do zamówień i danych klientów.
Jak naprawić	Włączyć limit prób i logowanie dwuskładnikowe dla administratorów oraz ograniczyć dostęp do panelu do znanych adresów.

Gdzie: formularz logowania do panelu administracyjnego Nakład: 2 godz.
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Kopia zapasowa bazy danych dostępna z internetu

Co znaleziono	W katalogu dostępnym z internetu leży archiwum z kopią bazy danych sprzed kilku tygodni. Plik można pobrać bez logowania, a jego nazwa jest przewidywalna.
Czym grozi	Każdy, kto pobierze plik, zdobywa zamówienia, dane kontaktowe klientów i skróty haseł. Wyciek takich danych może wymagać zgłoszenia naruszenia do UODO (RODO, art. 33).
Jak naprawić	Usunąć plik i zablokować dostęp do katalogu. Przenieść kopie zapasowe poza serwer sklepu, w miejsce niedostępne z internetu. Sprawdzić w dziennikach serwera, czy plik był pobierany.

Gdzie: archiwum w katalogu wtyczki do kopii zapasowych Nakład: 2 godz.

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Konta byłych współpracowników z pełnymi uprawnieniami

Co znaleziono	Wśród administratorów są konta dwóch osób, które nie współpracują już przy sklepie. Ostatnie logowanie na tych kontach było ponad rok temu, a same konta mają pełne uprawnienia i nie mają drugiego składnika.
Czym grozi	Przejęcie zapomnianego konta daje pełną kontrolę nad sklepem i może długo pozostać niezauważone.
Jak naprawić	Usunąć lub zablokować konta, które nie są potrzebne. Pozostałym nadać najniższe potrzebne uprawnienia i co kwartał przeglądać listę.

Gdzie: lista użytkowników z rolą administratora Nakład: 1 godz.

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Wgranie pliku wykonywalnego przez formularz opinii

Co znaleziono	Formularz opinii przyjmuje zdjęcia, ale sprawdza tylko rozszerzenie nazwy pliku, a nie jego zawartość. W teście na kopii udało się wgrać plik PHP, który serwer następnie uruchomił.
Czym grozi	Zalogowany klient, a nawet ktoś, kto dopiero założy konto, może uruchomić własny kod na serwerze i przejąć sklep.
Jak naprawić	Sprawdzać typ i zawartość przesyłanych plików, zmieniać ich nazwy i zablokować uruchamianie skryptów w katalogu przesłanych plików.

Gdzie: formularz opinii o produkcie, katalog przesłanych plików Nakład: 3 godz.

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Ujawnianie wersji oprogramowania

Co znaleziono	Odpowiedzi serwera i kod strony zdradzają dokładne wersje systemu i wtyczek.
Czym grozi	Ułatwia atakującemu dobór ataku do znanych podatności konkretnych wersji.
Jak naprawić	Ukryć numery wersji w nagłówkach i kodzie strony. To zalecenie uzupełniające, nie zastępuje aktualizacji. Gdzie: nagłówki odpowiedzi serwera i kod źródłowy strony Nakład: 1 godz. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Ciasteczko sesji koszyka bez zabezpieczających flag

Co znaleziono	Ciasteczko sesji koszyka, ustawiane przez moduł własny, nie ma flag Secure, HttpOnly i SameSite.
Czym grozi	Skrypt wykonany na stronie, na przykład po wykorzystaniu innego błędu, może odczytać ciasteczko i przejąć sesję klienta.
Jak naprawić	Dodać flagi Secure, HttpOnly i SameSite do ciasteczka w kodzie modułu. Gdzie: ciasteczko sesji koszyka ustawiane przez moduł własny Nakład: 1 godz. CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N

Loginy użytkowników widoczne dla każdego

Co znaleziono	Interfejs API systemu wypisuje loginy autorów i administratorów bez logowania.
Czym grozi	Atakujący zna prawdziwe loginy, więc zgadywanie haseł jest łatwiejsze (patrz VT-03).
Jak naprawić	Ograniczyć listę użytkowników w API do osób zalogowanych i ujednolicić komunikaty przy błędnym logowaniu. Gdzie: publiczny interfejs API systemu Nakład: 1 godz. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Nie używane wtyczki i motywy zostawione na serwerze

Co znaleziono	Na serwerze leżą wyłączone wtyczki i nie używane motywy, które nie są aktualizowane.
Czym grozi	Pliki wyłączonej wtyczki nadal da się wywołać z internetu, więc znana w nich podatność może być wykorzystana mimo wyłączenia.
Jak naprawić	Usunąć wtyczki i motywy, z których sklep nie korzysta. Gdzie: trzy wyłączone wtyczki i dwa nie używane motywy Nakład: 1 godz. CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L

Brak limitu prób przy kodach rabatowych

Co znaleziono	Pole kodu rabatowego nie ogranicza liczby prób. W teście na kopii automat sprawdził kilkaset kodów w kilka minut.
Czym grozi	Można odgadnąć aktywne kody rabatowe i użyć ich bez uprawnień, co obniża marżę i obciąża serwer.
Jak naprawić	Ograniczyć liczbę prób z jednego adresu, wydłużyć kody i blokować po serii błędnych prób. Gdzie: pole kodu rabatowego w koszyku Nakład: 3 godz. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L

Brak części nagłówków bezpieczeństwa

Co znaleziono	Serwer nie wysyła kilku zalecanych nagłówków, które utrudniają niektóre ataki przeprowadzane przez przeglądarkę.
Czym grozi	Niewielkie zwiększenie podatności na ataki w przeglądarce odwiedzającego.
Jak naprawić	Dodać brakujące nagłówki w konfiguracji serwera i przetestować, czy nie zakłócają działania strony. Gdzie: konfiguracja serwera WWW Nakład: 1 godz. CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N

Włączone przestarzałe wersje protokołu TLS

Co znaleziono	Serwer nadal akceptuje połączenia szyfrowane protokołem TLS 1.0 i 1.1.
Czym grozi	Teoretycznie umożliwia atak na szyfrowanie z bardzo starymi przeglądarkami. W praktyce ryzyko jest niewielkie.
Jak naprawić	Wyłączyć TLS 1.0 i 1.1, zostawić 1.2 i 1.3. Sprawdzić, czy sklep nie obsługuje klientów na bardzo starych urządzeniach. Gdzie: konfiguracja szyfrowania połączeń (HTTPS) Nakład: 1 godz. CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

Brak wymagań co do siły haseł klientów

Co znaleziono	Konto klienta można założyć z hasłem krótkim i prostym. Miernik siły hasła tylko podpowiada, niczego nie wymusza.
Czym grozi	Słabe hasła ułatwiają przejęcie kont klientów, a w nich adresów i historii zamówień.
Jak naprawić	Włączyć wymaganie minimalnej siły hasła przy zakładaniu konta i przy jego zmianie. Gdzie: zakładanie konta klienta i zmiana hasła Nakład: 1 godz. CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

5 Plan napraw

Kolejność uwzględnia wagę problemu, łatwość jego wykorzystania i nakład potrzebny na poprawkę. Dlatego VT-04 i VT-05, choć mają ocenę „wysokie”, są w pierwszym etapie: da się je wykorzystać bez specjalistycznej wiedzy, a naprawia się je w godzinę lub dwie.

Natychmiast do 3 dni	VT-01	Przestarzała wtyczka formularza ze znaną podatnością	8 godz.
	VT-04	Kopia zapasowa bazy danych dostępna z internetu	
	VT-05	Konta byłych współpracowników z pełnymi uprawnieniami	
	VT-02	Wstrzyknięcie SQL w module filtrowania produktów	
W pierwszej kolejności po tym do 2 tygodni	VT-03	Panel logowania bez limitu prób	5 godz.
	VT-06	Wgranie pliku wykonywalnego przez formularz opinii	
Porządki w konfiguracji do miesiąca	VT-07	Ujawnianie wersji oprogramowania	7 godz.
	VT-08	Ciasteczko sesji koszyka bez zabezpieczających flag	
	VT-09	Loginy użytkowników widoczne dla każdego	
	VT-10	Nieużywane wtyczki i motywy zostawione na serwerze	
	VT-11	Brak limitu prób przy kodach rabatowych	
Przy okazji bez terminu	VT-12	Brak części nagłówek bezpieczeństwa	3 godz.
	VT-13	Włączone przestarzałe wersje protokołu TLS	
	VT-14	Brak wymagań co do siły haseł klientów	

Razem około **23 godz.** pracy. Nakład jest szacunkowy i dotyczy samych poprawek, bez testów po stronie sklepu.

6 Co dalej

1 Omówienie wyników

Na rozmowie przechodzimy przez raport punkt po punkcie i uzgadniamy kolejność.

2 Poprawki

Wdroży je Twój zespół, Twoja agencja albo Vertiso, jak wolisz.

3 Ponowne sprawdzenie

Po wdrożeniu poprawek sprawdzam, czy problemy zostały usunięte.

Ograniczenia

Raport opisuje stan zabezpieczeń w uzgodnionym zakresie i w dniach testów. Nie gwarantuje ochrony przed każdym przyszłym atakiem. Ocena CVSS opisuje wagę techniczną podatności, a o kolejności napraw decyduje także wpływ na działanie serwisu i dane klientów.

Vertiso.pl

Pytania do raportu lub chęć zamówienia audytu własnej strony?

kontakt@vertiso.pl

+48 600 100 200

Dokument przykładowy. Dane w nim zawarte zostały wymyślone na potrzeby prezentacji i nie dotyczą żadnego rzeczywistego serwisu.