POUFNE · WERSJA DEMONSTRACYJNA

OCENA PODATNOŚCI

RAPORT Z TESTÓW BEZPIECZEŃSTWA

INFORMACJE O RAPORCIE	
System / Cel audytu	
Okres testowania	
Miejsce przeprowadzenia	
Główny audytor(rzy)	
Wersja raportu	
Klasyfikacja dokumentu	
Data raportu	

⚠ **WERSJA DEMONSTRACYJNA —** Niniejszy dokument opiera się na rzeczywistym audycie bezpieczeństwa. Część danych została usunięta zgodnie z przepisami o ochronie danych osobowych. Dokument przeznaczony wyłącznie do celów demonstracyjnych.

Streszczenie kierownicze

Niniejszy raport przedstawia wyniki niezależnego audytu podatności przeprowadzonego na docelowej aplikacji internetowej. Zakres oceny obejmował: rekonesans, konfigurację SSL/TLS, nagłówki bezpieczeństwa HTTP, zgodność z RODO oraz aktywne testy penetracyjne.

3	3	1	3
WYSOKI	ŚREDNI	NISKI	INFO

Następujące odkrycia wymagają natychmiastowej uwagi:

- Brak walidacji po stronie serwera (back-end) — atakujący może przesłać dowolne dane bezpośrednio do bazy danych, omijając wszystkie mechanizmy kontroli front-endu.
- Potwierdzono wystąpienie wielu podatności Cross-Site Scripting (XSS). Przechowywany XSS w systemie blogów umożliwia tworzenie kont administratora.
- Tokeny sesji nie są unieważniane po wylogowaniu, co umożliwia ponowne odtworzenie żądań i przełączanie kont.

Pełne usunięcie wszystkich odkryć o poziomie WYSOKIM i ŚREDNIM jest zdecydowanie zalecane przed wdrożeniem produkcyjnym oraz przed jakimkolwiek przeglądem regulacyjnym lub sądowym.

1. Wprowadzenie

1.1 Zakres i cel

Niniejszy raport dokumentuje wyniki oceny podatności przeprowadzonej na docelowym systemie. Metoda oceny jest dostosowana do konkretnego rodzaju projektu i wykorzystuje aktualne narzędzia oraz techniki stosowane przez rzeczywistych cyberprzestępców. Każde zlecenie jest realizowane indywidualnie, w oparciu o skumulowane doświadczenie audytorów.

1.2 Informacje organizacyjne

Pole	Szczegóły
Raport przekazano	Wyłącznie upoważnionym osobom (dane ukryte — wersja demonstracyjna)
Format raportu	PDF — chroniony hasłem
Uwaga (wersja demo)	Część wrażliwych danych została usunięta

1.3 Klasyfikacja podatności

Podatności opisane w niniejszym raporcie posiadają przypisany poziom priorytetu i, tam gdzie ma to zastosowanie, wynik CVSS 3.1. Stosowane poziomy priorytetu definiuje się następująco:

WYSOKI	Bezpośrednie zagrożenie dla działalności. Wysokie prawdopodobieństwo nieuprawnionego dostępu do danych lub przejęcia konta uprzywilejowanego.
ŚREDNI	Istotny wpływ na działalność. Ryzyko kradzieży danych lub eskalacji uprawnień występuje, lecz może wymagać dodatkowych warunków.
NISKI	Ograniczony wpływ w izolacji. Może przyczynić się do łańcucha podatności lub stwarzać ryzyko wizerunkowe.
INFO	Luka w konfiguracji lub brak elementu wzmocnienia bezpieczeństwa. Nie zidentyfikowano bezpośredniego wektora eksploatacji; rekomendowane do poprawy.

1.4 Punktacja CVSS 3.1

Większość odkryć posiada wynik CVSS 3.1 zapewniający obiektywną, niezależną od dostawcy miarę krytyczności. Wyniki mieszczą się w przedziale od 0,0 (brak) do 10,0 (krytyczny). Stosowane metryki:

Metryka	Opis	Wartości
Attack Complexity (AC)	Warunki poza kontrolą atakującego wymagane do eksploatacji	Low / High
Privileges Required (PR)	Poziom uprawnień, które atakujący musi posiadać przed eksploatacją	None / Low / High
User Interaction (UI)	Czy wymagany jest udział użytkownika innego niż atakujący	None / Required
Scope (S)	Czy eksploatacja może wpłynąć na komponenty poza podatnym zakresem	Unchanged / Changed
Confidentiality (C)	Wpływ na poufność informacji	None / Low / High
Integrity (I)	Wpływ na integralność i wiarygodność informacji	None / Low / High
Availability (A)	Wpływ na dostępność komponentu lub systemu	None / Low / High

2. Faza I — Rekonesans

Faza I obejmuje pasywne i półpasywne zbieranie informacji: analizę domeny, wykrywanie zapory aplikacji internetowej (WAF), konfigurację SSL/TLS, mapowanie aplikacji internetowej, nagłówki bezpieczeństwa HTTP oraz ocenę zgodności z RODO.

2.1 Analiza domeny

Zebrano ogólne informacje o domenie, w tym dane rejestracyjne, serwery nazw (nameservers) oraz adresy IP.

Pole	Wartość
Domena	[Usunięto — wersja demonstracyjna]
Adres(y) IP	[Usunięto — wersja demonstracyjna]
Rejestrator / Data wygaśnięcia	[Usunięto — wersja demonstracyjna]
Serwery nazw (Nameservers)	[Usunięto — wersja demonstracyjna]

2.2 Web Application Firewall (WAF)

STATUS	[Treść usunięta — ochrona danych]

2.3 Konfiguracja SSL/TLS

Konfigurację SSL/TLS przeanalizowano za pomocą zautomatyzowanych narzędzi na wszystkich endpointów HTTPS.

2.3.1 Obsługiwane protokoły

STATUS	BRAK KRYTYCZNYCH PODATNOŚCI — WYMAGANE DZIAŁANIE (TLS 1.3 wyłączony)

protokół	Status
TLS 1.3	**Wyłączony**
TLS 1.2	**Włączony**
TLS 1.0	Wyłączony ✓
SSL 3	Wyłączony ✓
SSL 2	Wyłączony ✓

2.3.2 Zestawy szyfrów (Cipher Suites) — TLS 1.2

STATUS	BRAK KRYTYCZNYCH PODATNOŚCI — obecne słabe szyfry (patrz niżej)

Zestaw szyfrów (kolejność preferowana przez serwer)	Bity klucza
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) FS ⚠ SŁABY	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) FS ⚠ SŁABY	256

Zestaw szyfrów (kolejność preferowana przez serwer)	Bity klucza
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) FS ⚠ SŁABY	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) FS ⚠ SŁABY	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) ⚠ SŁABY	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) ⚠ SŁABY	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) ⚠ SŁABY	256

2.3.3 Dodatkowe testy SSL/TLS

STATUS	BRAK PODATNOŚCI

Test	Wynik
TLS Fallback SCSV	Serwer obsługuje TLS Fallback SCSV
Renegocjacja TLS	Renegocjacja sesji nieobsługiwana
Kompresja TLS	Kompresja wyłączona
Heartbleed (TLSv1.2)	Brak podatności
Algorytm podpisu	sha256WithRSAEncryption
Siła klucza RSA	2048 bitów

2.3.4 Wynik SSL/TLS

95 / 100

Ogólna ocena SSL/TLS

2.4 Mapowanie aplikacji internetowej

STATUS	BRAK PODATNOŚCI

[Treść wrażliwa – usunięta.]

2.5 Nagłówki bezpieczeństwa (Security Headers)

STATUS	WYMAGANE DZIAŁANIE — brak 5 z 6 zalecanych nagłówków

Nagłówek bezpieczeństwa	Status
Strict-Transport-Security	Obecny ✓
Content-Security-Policy	Brak ✗
X-Frame-Options	Brak ✗
X-Content-Type-Options	Brak ✗
Referrer-Policy	Brak ✗
Permissions-Policy	Brak ✗

Brakujące nagłówki — zalecenia

Content-Security-Policy Zapobiega atakom XSS poprzez białolistowanie zatwierdzonych źródeł treści. Bez CSP przeglądarki ładują dowolne zasoby. Dokumentacja: OWASP CSP Cheat Sheet.

X-Frame-Options Zapobiega atakom clickjacking przez blokowanie osadzania strony w ramkach (iframe). Zalecana wartość: SAMEORIGIN.

X-Content-Type-Options Zapobiega sniffingowi typów MIME. Jedyna poprawna wartość: nosniff.

Referrer-Policy Kontroluje informacje o źródle odsyłacza (referer) wysyłane podczas nawigacji. Powinien być ustawiony na wszystkich stronach.

Permissions-Policy Ogranicza dostęp do interfejsów API przeglądarki. Zmniejsza powierzchnię ataku.

Pełna dokumentacja: https://owasp.org/www-project-secure-headers/

2.6 Zgodność z RODO

STATUS	BRAK NARUSZEŃ

Aplikacja spełnia wymagania RODO. Dane są przechowywane za pośrednictwem Firebase, które posiada następujące certyfikaty zgodności:

Usługa Firebase	Certyfikaty
Cloud Firestore	ISO 27001, 27017, 27018 · SOC 1, 2, 3
Cloud Functions	ISO 27001, 27017, 27018 · SOC 1, 2, 3
Cloud Storage	ISO 27001, 27017, 27018 · SOC 1, 2, 3
Firebase A/B Testing	ISO 27001 · SOC 1, 2, 3
Firebase App Distribution	SOC 2
Firebase Authentication	ISO 27001, 27017, 27018 · SOC 1, 2, 3
Firebase Cloud Messaging	ISO 27001 · SOC 1, 2, 3
Firebase Crashlytics	SOC 2
Firebase Dynamic Links	ISO 27001 · SOC 1, 2, 3
Firebase Hosting	ISO 27001 · SOC 1, 2, 3
Firebase In-App Messaging	ISO 27001 · SOC 1, 2, 3
Firebase ML	ISO 27001 · SOC 1, 2, 3
Firebase Performance Monitoring	ISO 27001 · SOC 1, 2, 3
Firebase Platform	ISO 27001 · SOC 1, 2, 3
Firebase Predictions	ISO 27001 · SOC 1, 2, 3

Usługa Firebase	Certyfikaty
Firebase Realtime Database	ISO 27001 · SOC 1, 2, 3
Firebase Remote Config	ISO 27001 · SOC 1, 2, 3
Firebase Test Lab	ISO 27001, 27017, 27018 · SOC 1, 2, 3
Google Analytics for Firebase	ISO 27001 · SOC 1, 2, 3

Dokumentacja: https://firebase.google.com/support/privacy

Uwaga: Jeśli w przyszłości zostanie wprowadzona analityka zachowań użytkowników (np. Google Analytics), przed rozpoczęciem profilowania wymagana jest wyraźna zgoda użytkownika, np. poprzez baner cookies.

Regulamin usługi: [Treść usunięta — ochrona danych]

Lista osób z dostępem do środowiska produkcyjnego: [Treść usunięta — ochrona danych]

3. Faza II — Wykryte podatności

3.1 Zestawienie zbiorcze

Poniżej znajduje się lista wszystkich podatności wykrytych podczas aktywnych testów, posortowana według wyniku CVSS. Szczegółowa analiza i zalecenia dla każdej podatności zawarte są w sekcji 3.2.

#	Podatność	CVSS 3.1	Poziom
1	Brak walidacji backendowej	8,1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	WYSOKI
2	Cross-Site Scripting (XSS) — wiele lokalizacji	7,5 AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H	WYSOKI
3	Dane osobowe (e-mail) ujawnione w adresie URL	7,0 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L	WYSOKI
4	Ujawnienie informacji przez konsolę sieciową	6,5 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L	ŚREDNI
5	Możliwość wysyłania żądań po wylogowaniu	6,5 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	ŚREDNI
6	Brak weryfikacji uprawnień do pobierania plików	6,5 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	ŚREDNI
7	Możliwość usunięcia konta przy posiadaniu ID	5,0 AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L	NISKI
8	Słaba polityka haseł (min. 6 znaków)	N/D	INFO
9	Nieograniczona liczba sesji; brak panelu zarządzania sesjami	N/D	INFO
10	Brak nagłówków bezpieczeństwa (5 z 6)	N/D	INFO

3.2 Szczegółowy opis podatności

WYSOKI CVSS 3.1: 8,1 / 10	**Podatność 1 — Brak walidacji back-end**
Lokalizacja	Formularz rejestracji użytkownika; panel edycji danych użytkownika; potencjalnie również inne formularze w aplikacji.
Uprawnienia	Brak wymaganych uprawnień.
Opis	Brak walidacji po stronie serwera (back-end) dla danych kontrolowanych przez użytkownika. Atakujący może ominąć wszystkie mechanizmy walidacji front-endu i przesłać dowolne lub złośliwe dane bezpośrednio do bazy danych za pomocą specjalnie spreparowanych żądań HTTP. Potwierdzone przykłady: *dane usunięte*
Zrzuty ekranu	*[Zrzuty ekranu usunięte]*
Zalecenia	Wdrożyć kompleksową walidację po stronie serwera (backend) dla wszystkich danych kontrolowanych przez użytkownika. Jest to niezależne od walidacji frontend i stanowi jej uzupełnienie. Wszystkie pola wejściowe muszą być walidowane po stronie serwera przed zapisem jakichkolwiek danych. Walidacja wyłącznie po stronie klienta może być trywialnie pominięta przy użyciu narzędzi takich jak Burp Suite lub curl.

WYSOKI CVSS 3.1: 7,5 / 10	**Podatność 2 — Cross-Site Scripting (XSS)**
Lokalizacja	Potwierdzone: formularz dodawania/edycji użytkownika; formularz tworzenia wpisu na blogu. Prawdopodobnie również inne formularze.
Uprawnienia	Zalogowany użytkownik z dostępem do formularzy.
Opis	Zidentyfikowano wiele podatności XSS. Dane wprowadzane przez użytkowników są wyświetlane w przeglądarce bez kodowania HTML w większości widoków aplikacji. Potwierdzony wektor eksploatacji: *dane usunięte.* Potwierdzony wektor eksploatacji: *dane usunięte.* Przechowywany XSS tego rodzaju może być używany do przechwytywania sesji, tworzenia kont uprzywilejowanych i ukierunkowanego phishingu za pośrednictwem systemu e-mail aplikacji.
Zrzuty ekranu	*[Zrzuty ekranu usunięte — obowiązek ochrony danych]*
Zalecenia	Zastosować kodowanie wyjściowe odpowiednie do kontekstu dla wszystkich danych dostarczonych przez użytkownika przed ich renderowaniem. W kontekstach HTML należy kodować: & " ' < > → & " ' < > Walidacja i sanityzacja muszą być stosowane po stronie serwera, a nie tylko w przeglądarce. Dokumentacja: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

WYSOKI CVSS 3.1: 7,0 / 10	**Podatność 3 — Dane osobowe (e-mail) w adresie URL**
Lokalizacja	*Dane usunięte.*
Uprawnienia	Wymagane konto administratora.
Opis	Funkcja podszywania się pod użytkownika w panelu administratora tworzy adresy URL zawierające adres e-mail docelowego użytkownika jako parametr w postaci zwykłego tekstu. Adresy e-mail stanowią dane osobowe w rozumieniu RODO i nie mogą pojawiać się w adresach URL. Adresy URL są rutynowo przechowywane w logach serwera, historii przeglądarki, nagłówkach Referer i platformach analitycznych. Ujawnienie w adresach URL istotnie zwiększa ryzyko przypadkowego ujawnienia danych osobowych.
Zrzuty ekranu	*[Zrzuty ekranu usunięte]*
Zalecenia	*Dane usunięte.*

ŚREDNI CVSS 3.1: 6,5 / 10	**Podatność 4 — Ujawnienie informacji przez konsolę sieciową**
Lokalizacja	Endpoint logowania.
Uprawnienia	Brak wymaganych uprawnień.
Opis	Choć widoczne komunikaty o błędach na stronie logowania są generyczne, odpowiedzi HTTP serwera (widoczne w konsoli sieciowej przeglądarki) ujawniają, czy przesłany adres e-mail istnieje w bazie danych. Pozwala to atakującemu na wyliczenie zarejestrowanych kont użytkowników poprzez przesłanie kandydujących adresów e-mail i obserwację treści odpowiedzi serwera lub kodu statusu HTTP.
Zrzuty ekranu	*[Zrzuty ekranu usunięte]*
Zalecenia	Endpoint logowania musi zwracać identyczną odpowiedź — ten sam kod statusu HTTP, tą samą treść odpowiedzi, ten sam czas odpowiedzi — niezależnie od tego, czy przesłany adres e-mail istnieje w bazie danych.

ŚREDNI CVSS 3.1: 6,5 / 10	**Podatność 5 — Możliwość wysyłania żądań po wylogowaniu**
Lokalizacja	Endpoint zmiany nazwy użytkownika.
Uprawnienia	Zwykłe konto użytkownika; ID konta.
Opis	Tokeny sesji nie są unieważniane po stronie serwera po wylogowaniu. Atakujący, który przechwyci ważny token sesji (np. przez podsłuch sieci lub XSS), może nadal wykonywać uwierzytelnione działania po wylogowaniu się prawdziwego użytkownika. Zademonstrowany atak: użytkownik zmienia nazwę → wylogowuje się → atakujący odtwarza żądanie z przechwyconym tokenem → nazwa zostaje zmieniona ponownie. Token pozostaje ważny.
Zrzuty ekranu	*[Zrzuty ekranu usunięte]*
Zalecenia	Unieważnić token sesji po stronie serwera natychmiast po wylogowaniu. Serwer powinien odrzucać wszystkie kolejne żądania zawierające unieważniony token odpowiedzią 401 Unauthorized.

ŚREDNI CVSS 3.1: 6,5 / 10	**Podatność 6 — Brak weryfikacji uprawnień do pobierania plików**
Lokalizacja	Endpoint pobierania plików.
Uprawnienia	Zwykłe konto użytkownika (do przesłania pliku); brak do pobrania.
Opis	Po przesłaniu pliku do systemu staje się on dostępny przez bezpośredni adres URL dla każdej osoby posiadającej ten adres URL, w tym użytkowników nieuwierzytelnionych i osób spoza właściwego obszaru roboczego. Serwer nie weryfikuje, czy żądająca strona jest uwierzytelniona lub posiada uprawnienia dostępu do pliku. Stwarza to ryzyko nieautoryzowanego dostępu do danych i może być wykorzystane do phishingu. Ponadto funkcja przesyłania plików obecnie zezwala na przesyłanie plików wykonywalnych i skryptowych, w tym .PHP, .JAR i .ZIP. Zablokowany jest jedynie format .EXE.
Zrzuty ekranu	*[Zrzuty ekranu usunięte]*
Zalecenia	*Dane usunięte.*

NISKI CVSS 3.1: 5,0 / 10	**Podatność 7 — Możliwość usunięcia konta przy znaniu ID**
Lokalizacja	Endpoint usuwania konta.
Uprawnienia	Zwykłe konto użytkownika; ID konta docelowego.
Opis	Endpoint usuwania konta akceptuje żądania w oparciu o token Authorization zawierający wystarczające informacje do identyfikacji konta docelowego. Każdy użytkownik, który uzyska token innego użytkownika, może usunąć to konto. Token sesji nie wygasa po wylogowaniu lub wygasa ze znacznym opóźnieniem, co istotnie poszerza okno możliwej eksploatacji. *[Szczegóły struktury tokenu usunięte]*
Zrzuty ekranu	*[Zrzuty ekranu usunięte]*
Zalecenia	Wariant A: Wymagać potwierdzenia e-mailem przed wykonaniem usunięcia konta. Link potwierdzający musi być jednorazowy i ograniczony czasowo. Wariant B: Wdrożyć okres karencji (np. 7 dni), w trakcie którego konto jest oznaczone do usunięcia, ale może zostać przywrócone przez właściciela. W każdym przypadku: unieważnić token sesji natychmiast po wylogowaniu (patrz podatność 5).

INFO	**Podatność 8 — Słaba polityka haseł**
Lokalizacja	Wszystkie endpointy uwierzytelniania.
Uprawnienia	Brak wymaganych uprawnień.
Opis	Aplikacja wymaga minimalnej długości hasła wynoszącej sześć znaków bez wymogów złożoności. Pozwala to na stosowanie trywialnie słabych haseł (np. "123456", "abcdef") i istotnie zwiększa ekspozycję na ataki brute-force i credential stuffing.
Zrzuty ekranu	*[Zrzuty ekranu usunięte]*
Zalecenia	Wymusić minimalną długość hasła wynoszącą 12 znaków. Długość jest głównym czynnikiem siły hasła; obowiązkowe znaki specjalne są kwestią drugorzędną. Rozważyć wdrożenie uwierzytelnienia wieloskładnikowego (Multi-Factor Authentication, MFA) dla kont administratora jako priorytet.

INFO	**Podatność 9 — Nieograniczona liczba sesji; brak panelu zarządzania sesjami**
Lokalizacja	Warstwa zarządzania sesjami.
Uprawnienia	Brak wymaganych uprawnień.
Opis	Użytkownicy mogą być uwierzytelnieni w nieograniczonej liczbie równoległych sesji z różnych urządzeń i przeglądarek. Stan ten może być wykorzystany w ramach ataków CSRF. Brak interfejsu umożliwiającego użytkownikowi przeglądanie aktywnych sesji lub odwoływanie poszczególnych sesji.
Zrzuty ekranu	*[Zrzuty ekranu usunięte]*
Zalecenia	Wdrożyć panel zarządzania sesjami umożliwiający użytkownikom przeglądanie i kończenie aktywnych sesji (analogicznie do funkcji "Zarządzaj urządzeniami" Google), w tym opcję "wyloguj ze wszystkich sesji". Rozważyć wdrożenie polityki jednej aktywnej sesji (lub modelu tokenów per urządzenie) z automatycznym unieważnieniem poprzednich sesji przy nowym logowaniu.

INFO	**Podatność 10 — Brak nagłówków bezpieczeństwa**
Lokalizacja	Wszystkie endpointy aplikacji.
Uprawnienia	Brak wymaganych uprawnień.
Opis	Pięć z sześciu zalecanych nagłówków bezpieczeństwa jest nieobecnych w odpowiedziach HTTP: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy. Szczegółowe informacje zawarte są w sekcji 2.5 niniejszego raportu.
Zrzuty ekranu	*[Zrzuty ekranu usunięte]*
Zalecenia	*Dane usunięte.*

3.3 Testy dodatkowe — brak odkryć

Poniższe testy przeprowadzono podczas oceny podatności i nie wykryto żadnych podatności możliwych do eksploatacji.

Test	Wynik
Cross-Site Scripting — pola czat/nazwa użytkownika	**ZALICZONY**
SQL Injection — pole nazwy użytkownika	**ZALICZONY**
Brute Force — logowanie i endpointy nazwy użytkownika	**ZALICZONY**
Verbose Error Messages (szczegółowe komunikaty błędów)	**ZALICZONY**
Clickjacking	**ZALICZONY**
Przesłanie plików (File Upload)	**ZALICZONY — WYMAGANE DZIAŁANIE (patrz Podatność 6)**
Entropia tokenów sesji	**ZALICZONY**
Testy bezpieczeństwa API	**ZALICZONY**
Brute Force — strona logowania	**ZALICZONY**
Przegląd zgodności RODO	**ZALICZONY**

4. Podsumowanie i zalecenia

4.1 Ogólna ocena

Audyt wykrył 10 podatności na czterech poziomach krytyczności. Trzy z nich zostały ocenione jako WYSOKIE i wymagają natychmiastowego usunięcia przed jakimkolwiek wdrożeniem produkcyjnym lub audytem zewnętrznym. Trzy podatności na poziomie ŚREDNIM powinny zostać usunięte w kolejnym sprincie deweloperskim.

Konfiguracja SSL/TLS jest ogólnie silna (95/100), a wymagania RODO są spełnione za pośrednictwem infrastruktury Firebase. Główna powierzchnia ryzyka koncentruje się w mechanizmach kontroli warstwy aplikacyjnej: walidacja danych wejściowych, kodowanie danych wyjściowych oraz zarządzanie sesjami.

4.2 Zalecenia priorytetowe

#	Zalecenie	Priorytet
1	Wdrożyć walidację po stronie serwera dla wszystkich pól wejściowych kontrolowanych przez użytkownika. To działanie o najwyższym wpływie spośród wszystkich zawartych w raporcie.	WYSOKI
2	Zastosować kodowanie wyjściowe dla wszystkich danych dostarczonych przez użytkownika przed renderowaniem w kontekstach HTML. Przeprowadzić pełny audyt XSS wszystkich formularzy.	WYSOKI
3	Usunąć dane osobowe (adresy e-mail) z adresów URL. Stosować zabezpieczone identyfikatory (UUID) w całej aplikacji.	WYSOKI
4	Unieważniać tokeny sesji po stronie serwera natychmiast po wylogowaniu. Zapewnić, aby endpoint logowania zwracał identyczne odpowiedzi dla wszystkich przypadków błędów.	ŚREDNI
5	Wymusić sprawdzanie autoryzacji przy pobieraniu plików. Ograniczyć dopuszczalne typy plików do przesłania do jawnej listy dozwolonych (allowlist).	ŚREDNI
6	Wdrożyć wszystkie pięć brakujących nagłówków bezpieczeństwa HTTP zgodnie z zaleceniami OWASP.	INFO
7	Włączyć TLS 1.3; wyłączyć TLS 1.1. Zwiększyć minimalną długość hasła do 12 znaków.	INFO

4.3 Wynik końcowy

Poniższy wynik odzwierciedla subiektywną ocenę audytorów dotyczącą ogólnego poziomu bezpieczeństwa aplikacji w momencie przeprowadzania testów, w skali od 0 do 100.

[dane usunięte]

4.4 Oświadczenie audytora

Podpisani audytor(rzy) potwierdzają, że niniejszy raport dokładnie odzwierciedla wyniki oceny bezpieczeństwa przeprowadzonej na ww. systemie, przy użyciu profesjonalnych narzędzi i standardowych metodologii branżowych. Wszystkie testy zostały przeprowadzone na podstawie pisemnego upoważnienia właściciela systemu i zgodnie z uzgodnionym zakresem zlecenia.

Główny tester/audytor	**Weryfikacja**
Podpis	Podpis
[dane usunięte]	*[dane usunięte]*

ZASTRZEŻENIE — WERSJA DEMONSTRACYJNA

Niniejszy dokument stanowi wersję demonstracyjną rzeczywistego raportu z testu bezpieczeństwa. Część danych została zanonimizowana. Każde zlecenie jest indywidualnie określone i realizowane; wyniki zawarte w niniejszym dokumencie odzwierciedlają stan ocenianego systemu w momencie przeprowadzania testów i nie mogą być interpretowane jako aktualna reprezentacja jego poziomu bezpieczeństwa. Dystrybucja ograniczona wyłącznie do upoważnionych odbiorców.