VERCOM

Podsumowanie testu bezpieczeństwa

PRZEDMIOT PRAC
Podsumowanie testu bezpieczeństwa aplikacji webowej *.messageflow.com

DATA WYKONANIA TESTU
05.12.2024 - 16.12.2024

DATA PODSUMOWANIA
24.01.2025

AUDYTORZY
Gilewicz Michał

Podsumowanie wykonanych prac

Niniejszy raport jest podsumowaniem testów bezpieczeństwa prowadzonego przez Michała Gilewicza. Przedmiotem testów były aplikacje webowe z domeny *.messageflow.com m.in: app.messageflow.com oraz appbackend.messageflow.com obejmująca swoim zakresem panele marek Emaillabs, Redlink oraz MessageFlow.

W trakcie audytu szczególny nacisk położono na podatności mające lub mogące mieć negatywny wpływ na poufność, integralność oraz dostępność przetwarzanych danych.

Testy bezpieczeństwa przeprowadzono zgodnie z powszechnie przyjętymi metodykami testowania aplikacji webowymi, takimi jak: OWASP TOP10 czy OWASP ASVS które obejmowały m.in. testy mające na celu znalezienie błędów związanych z możliwością wstrzyknięcia złośliwego kodu (XSS, SQLi, SSTI itp.), błędów związanych z uwierzytelnianiem czy związanych z niepoprawną konfiguracją serwera. Ponadto w trakcie trwania audytu przeskanowano infrastrukturę w celu znalezienia podatnych oprogramowań / bibliotek, a także otwartych portów które mogły mieć wpływ na bezpieczeństwo sieci.

W ramach audytu wykorzystano podejście polegające na testach manualnych oparte o wyżej wymienione metodyki, jak i wsparcie tych czynności szeregiem narzędzi automatycznych, m.in. Burp Suite Professional, Dirbuster, Nessus Professional, Nmap, sqlmap, ffuf.

Potwierdzono że wszystkie błędy bezpieczeństwa znalezione w trakcie audytu bezpieczeństwa zostały naprawione i nie istnieje dalsza możliwość ich wykorzystania przez osoby trzecie.