VERCOM

Certyfikat z testów bezpieczeństwa opartych na metodyce OWASP TOP10 i OWASP ASVS

PRZEDMIOT PRAC
Podsumowanie testów bezpieczeństwa aplikacji webowej *.serwersms.pl

DATA WYKONANIA TESTU
21.03.2023 – Audyt wewnętrzny (Skan aplikacji webowej *.serwersms.pl)
04.05.2023 – 11.05.2023 – Audyt zewnętrzny (Aplikacja Webowa)
05.05.2023 – 12.05.2023 – Audyt zewnętrzny (HTTPS API v2)
28.05.2023 – Audyt wewnętrzny (Skan CMS – serwersms.pl)
11.12.2023 – 19.12.2023 – Audyt wewnętrzny (Aplikacja Webowa + HTTPS API)

DATA PODSUMOWANIA
13.02.2024

AUDYTORZY
Pentester: Gilewicz Michał (Vercom)
Firma zewnętrzna: Securitum Audyty Sp. z o.o. Sp. k.

Podsumowanie wykonanych prac

Niniejszy raport jest podsumowaniem testów bezpieczeństwa prowadzonego przez Michała Gilewicz, jak również firmę zewnętrzną: Securitum z siedzibą w Krakowie. Przedmiotem testów były aplikacje webowe z domeny *.serwersms.pl m.in. serwersms.pl, panel.serwersms.pl, api.serwersms.pl, api2.serwersms.pl.

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.

Niniejszy dokument stanowi potwierdzenie wykonania audytu oraz zgodności ze standardami bezpieczeństwa OWASP TOP10 i OWASP ASVS

Certification from security tests based on OWASP TOP10 and OWASP ASVS methodology.

SUBJECT OF WORK

Summary of web application security testing *.serwersms.pl

DATES THE TESTS WERE PERFORMED

21.03.2023 – Internal audit (Scan of web application *.serwersms.pl)
04.05.2023 – 11.05.2023 – External audit (Web App)
05.05.2023 – 12.05.2023 – External audit (HTTPS API v2)
28.05.2023 – Internal audit (CMS Scan – serwersms.pl)
11.12.2023 – 19.12.2023 – Internal audit (Web App + HTTPS API)

SUMMARY DATE

13.02.2024

AUDITORS

Pentester: Gilewicz Michał (Vercom)
Third-party company: Securitum Audyty Sp. z o.o. Sp. k.

Summary of the work done

The following report is a summary of security tests conducted by Michal Gilewicz, as well as an external company: Securitum, based in Krakow. The subject of the tests were web applications from the *.serwersms.pl domain, including serwersms.pl, panel.serwersms.pl, api.serwersms.pl, api2.serwersms.pl.

During the audit, special emphasis was placed on vulnerabilities that have or may have a negative impact on the confidentiality, integrity and availability of processed data.

Security tests were carried out in accordance with widely accepted web application testing standards and methodologies, such as OWASP TOP10 or OWASP AVSV, which included tests aimed at finding errors related to the possibility of injecting malicious code (XSS, SQLi, SSTI, etc.), flaws related to authentication or related to incorrect server configuration. In addition, during the audit, the infrastructure was scanned to find vulnerable softwares / libraries, as well as open ports, that could affect network security.

The approach used during the audit was manual testing, based on the aforementioned methodologies, as well as supporting these activities with a number of automated tools, including Burp Suite Professional, Dirbuster, Nessus Professional, Nmap, sqlmap, ffuf.

It has been confirmed that all security flaws, found during the security audit, have been fixed and there is no further possibility of their exploitation by third parties.

This document is an acknowledgement of the audit and compliance with OWASP TOP10 and OWASP ASVS security standards.