Zadanie 8 - Testy bezpieczeństwa

Nazwa testowanej aplikacji: https://warsawsneakerstore.com/

Data utworzenia raportu: 14.12.2022
Autor: Kurzydło Paweł

1. Lista defektów bezpieczeństwa:

- Brak CAPTCHA przy rejestracji
- Brak komunikatu przy wpisywaniu błędnego hasła przy logowaniu w oknie (działa tylko z poziomu https://warsawsneakerstore.com/login)
- Brak reakcji strony zamiast nałożenia blokady czasowej na logowanie po wpisaniu błędnego hasła, któryś raz z rzędu.
- Brakujące nagłówki bezpieczeństwa typu Content-Security-Policy, X-Content-Type-Options, Permissions-Policy
- Formularz Telefonu komórkowego przy rejestracji nie posiada limitu wprowadzonych cyfr

2. Sugestia usprawnień bezpieczeństwa:

- Dodatkowe potwierdzenie hasła podczas rejestracji
- Ustawienie limitu wprowadzonych cyfr w formularzu telefonu komórkowego np do ilości 15
- Komunikat przy wpisywaniu błędnego hasła również z poziomu wyświetlającego się okna logowania na stronie
- Dodanie CAPTCHA do rejestracji
- Uzupełnienie nagłówków bezpieczeństwa Content-Security-Policy, X-Content-Type-Options, Permissions-Policy
- Dodanie blokady czasowej po trzech nieudanych logowaniach przykładowo na 2 lub 3 minuty.

3. Użyte narzędzia do analiz bezpieczeństwa strony:

https://www.virustotal.com - Narzędzie, które użyłem do sprawdzenia aplikacji pod kątem wirusów

https://securityheaders.com/ - Strona, której użyłem do sprawdzenia nagłówków bezpieczeństwa

Trzecim ostatnim narzędziem były narzędzia deweloperskie w przeglądarce safari, użyte w celu monitorowania zachowania strony