|  |  |
| --- | --- |
| **Raport:** Maciej Zbydniewski | Aplikacja webowa |
| Data | 07.02.2023 |

1. Cel zadania

Celem zadania jest przeanalizowanie wybranej aplikacji webowej pod kątem bezpieczeństwa.

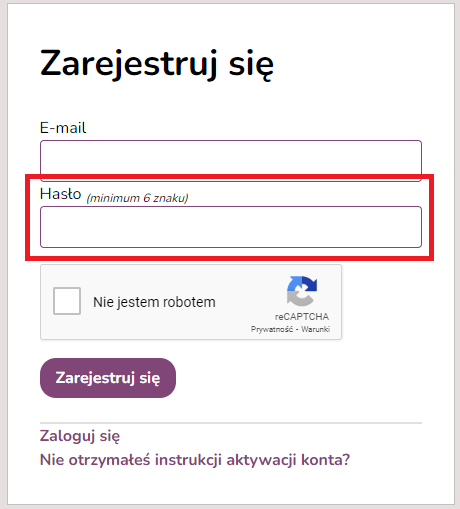
2. Wybrane oprogramowanie

|  |  |
| --- | --- |
| Przedmiot testów | Wyszukiwarka i porównywarka cen gier planszowych Planszeo |
| Adres strony | |  | | --- | | <https://planszeo.pl/> | |

3. Uwagi ogólne

Analizę aplikacji rozpocząłem od funkcji rejestracji oraz logowania się do konta.

Funkcja rejestracji może być ulepszona poprzez wymaganie od użytkownika dłuższego i bardziej skomplikowanego hasła – obecnie wymaga się hasła jedynie 6-znakowego. Bezpieczniejszą opcją byłoby hasło minimum 8-znakowe, zawierające przynajmniej 1 małą literę, 1 dużą literę, 1 cyfrę, a optymalnie również 1 znak specjalny.



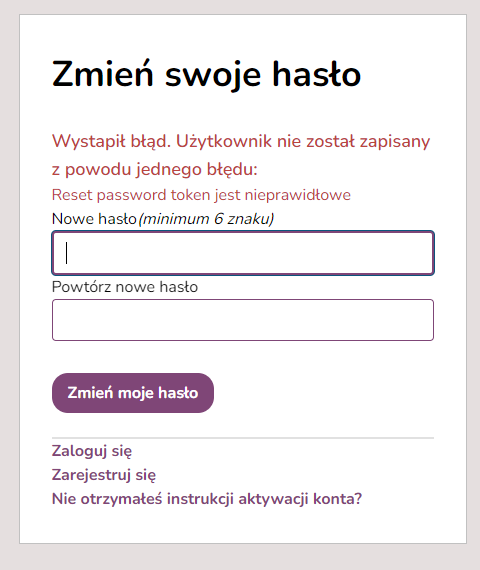
Dobrym rozwiązaniem jest dodanie do funkcji rejestracji captchy.

Jeśli chodzi o funkcjonalność zmiany i odzyskiwania hasła, to w tym wypadku również można podnieść standardy bezpieczeństwa.

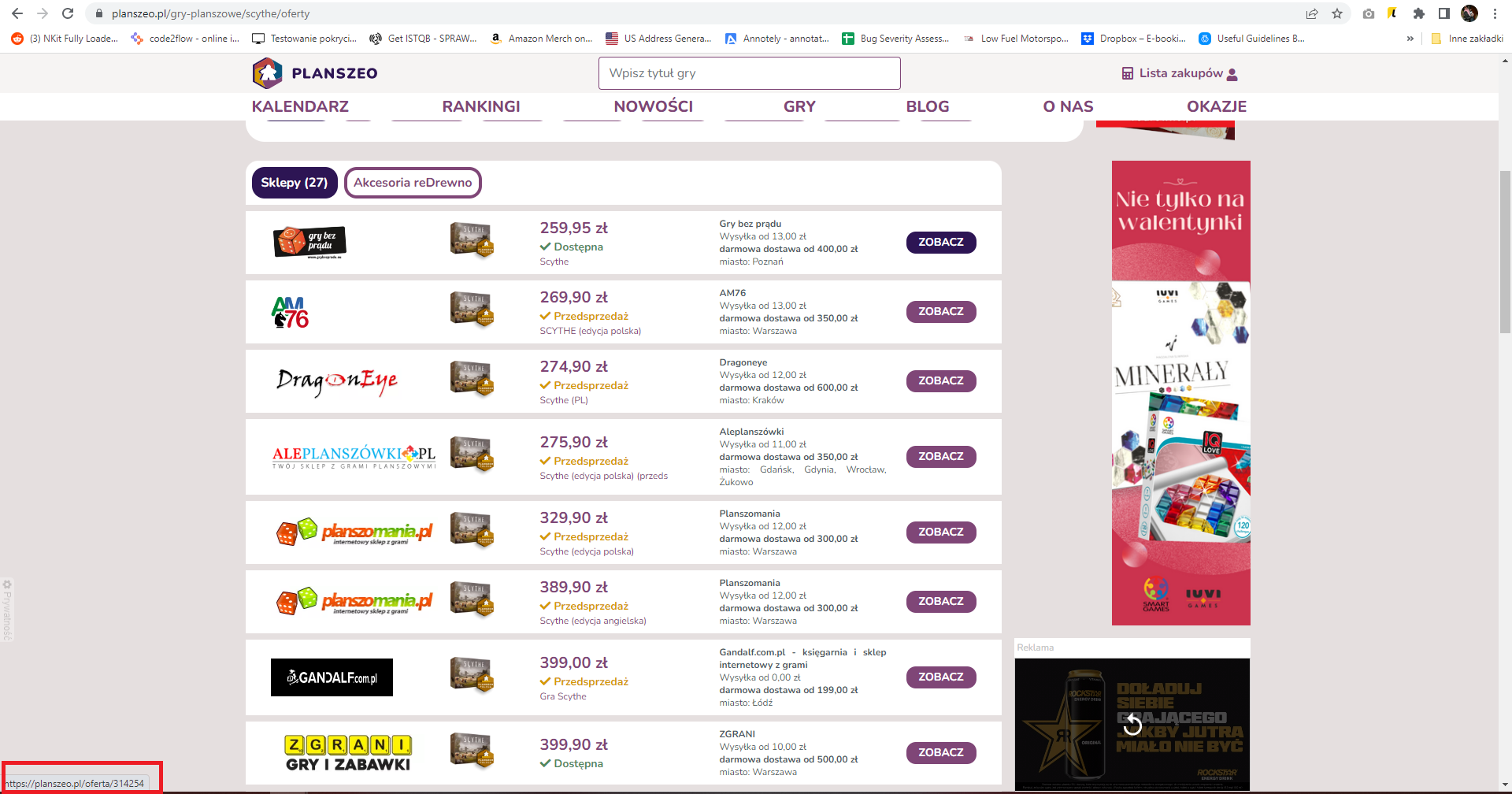
Przy próbie zmiany hasła z poziomu konta użytkownik jest w stanie zmienić hasło na poprzednio używane lub nawet na aktualne hasło – aplikacja w żadnej sposób nie informuje użytkownika o próbie zmiany hasła na takie samo lub używane uprzednio.

Podczas próby odzyskania hasła funkcją ‘Zapomniałeś hasła?’ z okna logowania użytkownik również jest w stanie zmienić zapomniane hasło na używane aktualnie lub poprzednie hasło.

Link-token do odzyskania hasła jest jednorazowy, co należy uznać za dobrą praktykę.



Aplikacja skupia się na porównywaniu cen gier planszowych, w związku z czym często odsyła użytkownika na strony zewnętrzne. W celu podniesienia poziomu bezpieczeństwa przy każdorazowej próbie sprawdzenia oferty na zewnętrznej stronie użytkownik powinien zostać zapytany czy na pewno chce przejść na daną stronę – w oknie z pytaniem powinien również znajdować się dokładny link strony, na którą użytkownik zostanie przekierowany. Aktualnie każda oferta ma ‘wewnętrzny’ adres serwisu Planszeo.



Do analizy serwisu użyłem również 3 skanerow witryn – <https://sitecheck.sucuri.net/>, <https://quttera.com/> oraz <https://www.ssllabs.com/ssltest/>. Żaden ze skanów nie wskazywał na problemy z bezpieczeństwem, jedyna sugestia ze strony witryny Sucuri dotyczyła monitoringu strony oraz firewalla. Poza tym narzędzia wskazywały na dobry poziom zabezpieczeń serwisu.

