Politechnika Częstochowska

Wydział Inżynierii Mechanicznej i Informatyki

PROJEKT ZESPOŁOWY

System rezerwacji pojazdów – raport z testów bezpieczeństwa

Car Rental

GRUPA 2 PAI

ZESPÓŁ 1:

Kacper Foks - kierownik
Michał Robak
Mateusz Karaś
Mateusz Hatalewicz

Spis treści

1. Zestawienie wyników 3
1.1 Wyłączenie z zakresu 3
1.2 Klasyfikacja podatności 3
1.3 Zestawienie 4
3. Wykryte podatności 5
3.1 Cross-Site Request Forgery (podatność o średnim znaczeniu) 5
3.2 Nieprawidłowa kontrola dostępu (podatność o niskim znaczeniu) 6
3.3 Inefficient Regular Expression Complexity in nth-check (podatność o niskim znaczeniu) 7
3.4 Brak polityki haseł (Ogólne zalecenia) 8

1. Zestawienie wyników

1.1 Wyłączenie z zakresu

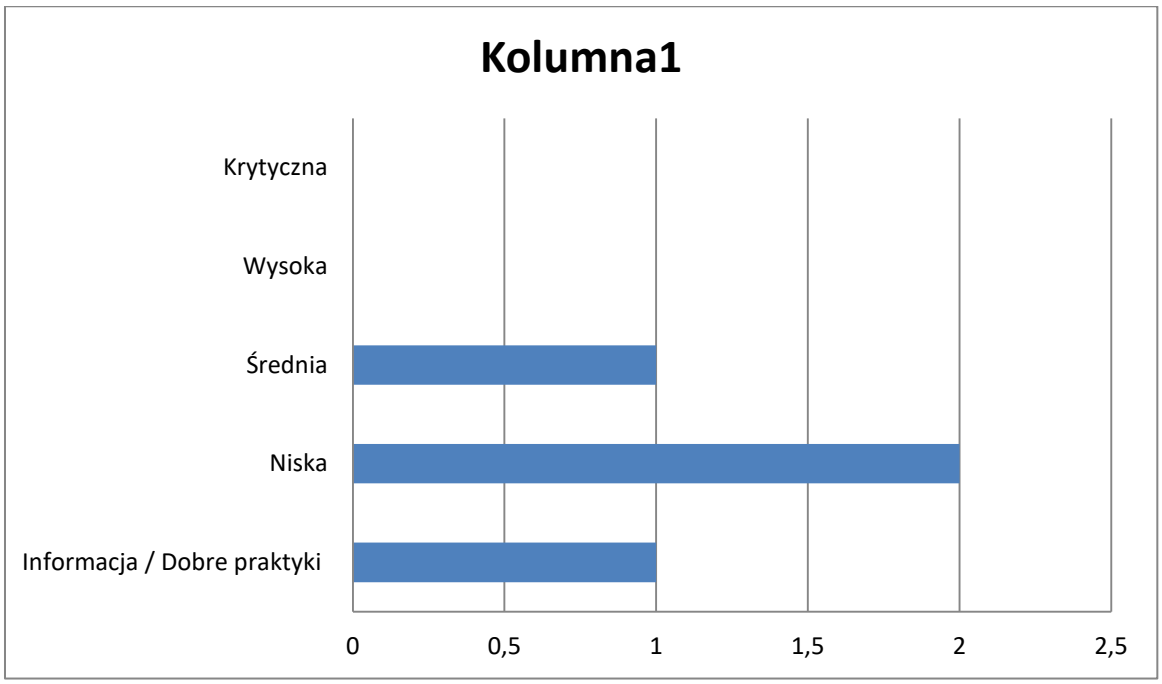
Testy bezpieczeństwa odbył się na lokalnym specjalnie przygotowanym do tego serwerze testowym, przez co pod uwagę nie była brana konfiguracja serwera webowego czy infrastruktura sieciowa. W testach nie brała udziału infrastruktura usługi Google Firebase, ze względu na brak wymaganych pozwoleń. Głównym celem testów był frontend aplikacji webowej Cloud, w raz z jej kodem źródłowym.

1.2 Klasyfikacja podatności

- **Krytyczna** – podatności o tej klasyfikacji powinny zostać usunięte możliwe jak najszybciej. Konsekwencją wykorzystania tej podatności, jest pełne przejęcie dostępu nad aplikacją, lub do jej danych.
- **Wysoka** – Konsekwencją tej podatności może być utrata danych lub tymczasowa przerwa w działaniu aplikacji. Może dotyczyć dostępu do wrażliwych danych.
- **Średnia** – do wykorzystania tej podatności muszą zajść pewne warunki, często są one związane z działalnością użytkownika w aplikacji.
- **Niska** – wykorzystanie podatności o tej klasyfikacji, ma nie wielkie znaczenie na wpływ bezpieczeństwa aplikacji, lub może zostać wykorzystane tylko w pewnych, specyficznych warunkach.
- **Informacja / Dobre praktyki** – nie są to podatności bezpieczeństwa, jednakże warto zastosować się do zaleceń, aby zwiększyć holistyczny poziom bezpieczeństwa aplikacji.

1.3 Zestawienie

Zestawienia przedstawia w formie wykresu ilość odnalezionych



3. Wykryte podatności

3.1 Cross-Site Request Forgery (podatność o średnim znaczeniu)

Opis:

Podatność polega na wymueszeniu przeglądarki użytkownika do wykonania pewnej nie autoryzowanego żądania HTTP.

Więcej informacji:

- Czym jest podatność CSRF (Cross-Site Request Forgery)? (sekurak.pl)
- Cross Site Request Forgery (CSRF) | OWASP Foundation

Szczegóły techincze:

Podatność została wykryta poprzez wykonanie skanu narzędziem OWASP ZAP.

Absence of Anti-CSRF Tokens

Source	raised by a passive scanner (Absence of Anti-CSRF Tokens)
CWE ID	352
WASC ID	9
Reference	▪ http://projects.webappsec.org/Cross-Site-Request-Forgery ▪ http://cwe.mitre.org/data/definitions/352.html

Zalecenia:

Prawidłowe wdrożenie obsługi tokenu CSRF spowoduje usunięcie tej podatności. Można do tego użyć gotowej paczki: *csurf*.

3.2 Nieprawidłowa kontrola dostępu (podatność o niskim znaczeniu)

Opis:

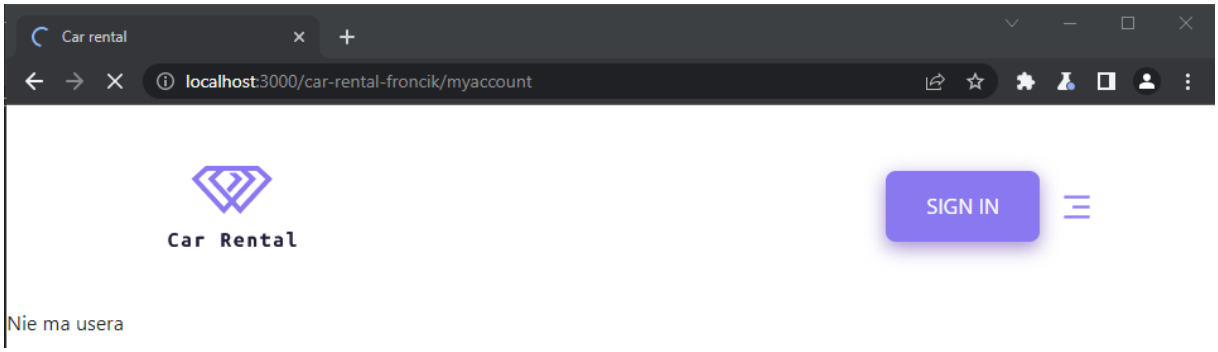
Kontrolą dostępu są zasady, dzięki którym użytkownicy nie mogą działać poza ich przydzielone uprawnienia. Wykorzystanie podatności zazwyczaj prowadzą do nieautoryzowanych ujawniania, modyfikowania lub niszczenie wszystkich danych lub pełnienie funkcji biznesowej poza granicami użytkownika.

Więcej informacji:

- A01 Broken Access Control - OWASP Top 10:2021

Szczegóły techniczne:

Poprzez adres URL można przejść do panelu użytkownika. Nie można wyświetlić zawartości panelu, lecz wraz z dalszym rozwojem aplikacji może to doprowadzić to incydentu bezpieczeństwa.



Zalecenia:

Dodanie prywatnego routingu po stronie reacta. Aktualnie wykorzystanie tej podatności nie wiążę się z większymi lukami bezpieczeństwa, lecz wraz z dalszym rozwojem aplikacji może spowodować bardziej krytyczne skutki, w szczególności poprzez dodanie nowej roli użytkownika.

3.3 Inefficient Regular Expression Complexity in nth-check (podatność o niskim znaczeniu)

Opis:

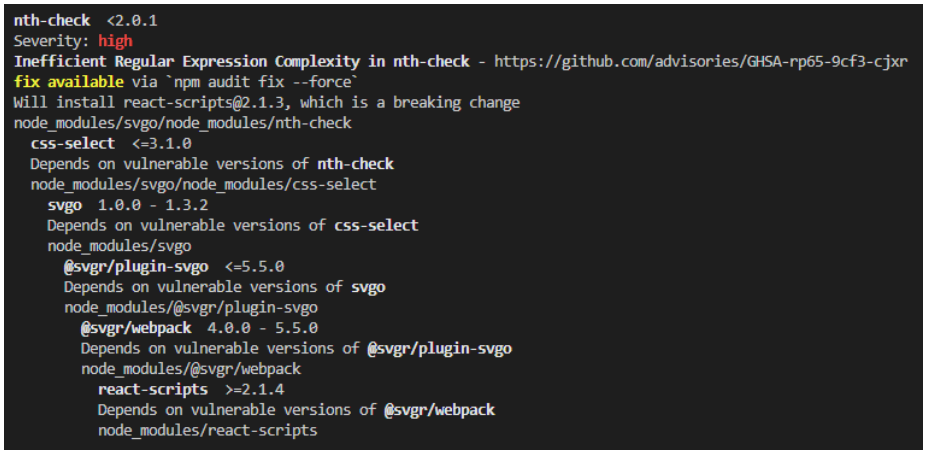
Aplikacja Car Rental korzysta z paczki ze znaną podatnością. Atak ten może spowodować atak typu „odmowa usługi”, poprzez nieprawidłowe *nth-check*. Podatność jest oceniana jako krytyczna, lecz jej wykonanie może zostać wykonane tylko na serwerze deweloperskim.

Więcej informacji:

- NVD - CVE-2021-3803 (nist.gov)
- Inefficient Regular Expression Complexity vulnerability found in nth-check (huntr.dev)
- Help, `npm audit` says I have a vulnerability in react-scripts! · Issue #11174 · facebook/create-react-app (github.com)

Szczegóły techniczne:

Podatność została wykryta poprzez narzędzie *npm audit*.



Zalecenia:

Jest to znana podatność, i podatna paczka nie powinna się znaleźć w środowisku produkcyjnym, aby temu zapobiec należy użyć polecenia: *npm audit –production*.

3.4 Brak polityki haseł (Ogólne zalecenia)

Opis:

W aplikacji brakuje dokładnych wymagań odnośnie złożoności haseł.

Więcej informacji:

- Rekomendacje techniczne CERT Polska dla systemów uwierzytelniania | CERT Polska

Zalecenia:

Zaprojektowanie i wdrożenie odpowiedniej polityki haseł dla tej aplikacji. Jako przykład można wybrać rekomendacje techniczne CERT Polska.