RAPORT: TESTY BEZPIECZEŃSTWA	
Autor: Robert Jaszewski	**Wersja dokumentu:** ID02
	Data: 02.06.2023
Przedmiot testów	Aplikacja webowa: Sklep internetowy z grami
Adres strony	https://www.gog.com/

1. Analiza bezpieczeństwa

Rejestracja oraz logowanie wymagają podania poufnych danych w postaci adresu email. Przeglądanie strony i wiele aktywności nie wymaga podawania wrażliwych danych, jednak dokonywanie płatności za produkt oraz wpłata środków na wirtualny portfel zobowiązuje do podania prawdziwych informacji. Jak wskazuje dokumentacja, poufność każdej transakcji jest gwarantowana przez bezpieczne szyfrowanie (SSL). Ponadto dla dodatkowej ochrony, aplikacja nie zachowuje żadnych danych kart kredytowych na serwerach. Aplikacja przetwarza dane osobowe w zgodności z właściwymi przepisami prawa dotyczącymi ochrony danych osobowych obowiązującymi w Unii Europejskiej lub USA (w tym Ustawy o Ochronie Danych Osobowych Dzieci w Internecie - COPPA) i innych krajach. Producent współpracuje jedynie z Zaufanymi Partnerami. Powyższe informacje pozwalają wnioskować o tym, że aplikacja jest potencjalnie bezpieczna.

Obszary aplikacji szczególnie narażone na luki bezpieczeństwa:	
Obszar	**Ryzyko**
Formularz rejestracji	Wyciek poufnych danych
Formularz logowania	Wyciek poufnych danych
Formularze kontaktowe	Wyciek poufnych danych
Wirtualny portfel	Przepadek przechowywanych środków Wyciek wrażliwych danych przy dokonywaniu wpłaty za pomocą poszczególnych metod
Dokonywanie płatności	Wyciek poufnych danych
Komunikacja z zewnętrznymi aplikacjami	Wyciek i przejęcie poufnych danych przez organizacje trzecie

2. Podejście do testów bezpieczeństwa

W celu zweryfikowania tych informacji oraz potwierdzenia, że aplikacja jest wolna od defektów bezpieczeństwa należy przeprowadzić odpowiednie testy. Zwrócić uwagę należy jednak, że nie wszystkie obszary, które są narażone na luki bezpieczeństwa mogą zostać przetestowane pod każdym względem z uwagi na brak dostępu do odpowiedniego środowiska testowego. Przeprowadzenie testów penetracyjnych oraz dokładne zbadanie procesu dokonywania płatności czy też wirtualnego portfelu w testowanej aplikacji wymagałoby przeprowadzenia testów API, posiadania wymaganych uprawnień, zgody właściciela serwisu oraz wspomnianego środowiska testowego. Z tego powodu testy bezpieczeństwa w tym przypadku należy przeprowadzić w miarę dostępnych możliwości.

Wykorzystane narzędzia:

- HostedScan – narzędie zapewniające zautomatyzowane skanowanie online pod kątem luk w zabezpieczeniach
- SSL Labs - przeprowadza głęboką analizę konfiguracji dowolnego serwera WWW SSL.
- Chrome DevTools - zestaw narzędzi dla programistów aplikacji webowych, który jest wbudowany bezpośrednio w przeglądarkę Google Chrome. Narzędzie to służy zarówno do edycji stron internetowych, jak i szybkiej diagnozie problemów.
- Sucuri SiteCheck - Skaner stron internetowych. Oferuje dokładną kontrolę strony internetowej w poszukiwaniu wirusów, ataków spamerskich, uszkodzeń kodu itp.

- VirusTotal - narzędzie analizujące podejrzane pliki, domeny, adresy IP i adresy URL w celu wykrycia złośliwego oprogramowania i innych naruszeń, automatycznie udostępnia je społeczności zajmującej się bezpieczeństwem.

3. **Rezultaty przeprowadzonych testów**

3.1. Uwagi i sugestie dotyczące wybranych obszarów

Formularz rejestracji:
Zbyt prosta odbiegająca od przyjętych powszechnie standardów struktura wymaganego hasła przy rejestracji konta. Stwarza to istotne ryzyko utworzenia przez użytkownika zbyt łatwego hasła, co może skutkować późniejszym przejęciem konta użytkownika.
Sugeruje się zmianę wymagań dotyczących pola z hasłem przy rejestracji oraz wprowadzenie bardziej restrykcyjnej walidacji hasła dla użytkownika. Obecnie pole hasło wymaga jedynie 8 znaków w tym jednej litery oraz aby nie kwalifikowało się na liście 500 najmniej bezpiecznych haseł (cokolwiek to znaczy, pole nadal przyjmuje najprostszy ciąg liter). Wprowadzenie kolejnych wymagań w postaci dużej litery, małej litery, co najmniej jednego numeru oraz znaku specjalnego, w dużym stopniu zwiększyłoby poziom bezpieczeństwa kont użytkowników.

Formularz logowania:
Formularz logowania jest zabezpieczony jedynie przez captcha. Brak dodatkowych zabezpieczeń. stwarza zagrożenie dla bezpieczeństwa konta oraz ryzyko jego przejęcia.

Sugerowane rozwiązanie:
- wprowadzenie dodatkowego zabezpieczenia w postaci funkcji zablokowania konta na pewien okres w sytuacji podjęcia przez użytkownika zbyt dużej ilości nieprawidłowych prób logowania.

Funkcja logowania dwuetapowego nie działa w pełnym zakresie tak jak wskazuje na to opis tej funkcji na stronie. Stwarza to zagrożenie, że osoba postronna może uzyskać dostęp do konta. (więcej informacji w raporcie defektu dotyczącym tej funkcjonalności)

Sugerowanie rozwiązanie:
- poprawienie tej funkcjonalności tak aby była kompletna z opisem i działała według powszechnie przyjętych norm.

3.2. Wyniki audytów bezpieczeństwa za pomocą narzędzi

Narzędzie HostedScan:
Raport wskazał na klika potencjalnych problemów sklasyfikowanych przez narzędzie jako średnie zagrożenia.

<u>Strona zawiera treści mieszane, czyli treści dostępne przez http zamiast HTTPS</u>

Sugerowane rozwiązanie:
- Strona dostępna przez SSL/TLS musi składać się w całości z treści przesyłanych przez SSL/TLS.
- Strona nie może zawierać żadnych treści przesyłanych przez niezaszyfrowany protokół HTTP.
- Obejmuje to treści z witryn stron trzecich.

<u>Błędna konfiguracja między domenami</u>

Ładowanie danych przeglądarki internetowej może być możliwe z powodu błędnej konfiguracji udostępniania zasobów między źródłami (CORS) na serwerze sieciowym

Sugerowane rozwiązanie:

- Upewnij się, że wrażliwe dane nie są dostępne w sposób nieuwierzytelniony (na przykład za pomocą białej listy adresów IP).
- Skonfiguruj nagłówek HTTP „Access-Control-Allow-Origin" na bardziej restrykcyjny zestaw domen lub całkowicie usuń wszystkie nagłówki CORS, aby umożliwić przeglądarce internetowej egzekwowanie zasad Same Origin Policy (SOP) w bardziej restrykcyjny sposób.

W formularzu przesyłania HTML nie znaleziono tokenów Anti-CSRF

Fałszowanie żądań między witrynami (ang. cross-site request forgery) to atak polegający na zmuszeniu ofiary do wysłania żądania HTTP do docelowego miejsca docelowego bez jej wiedzy lub zamiaru w celu wykonania działania jako ofiara.

Sugerowane rozwiązanie:

- Użyj sprawdzonej biblioteki lub platformy, która nie pozwala na wystąpienie tej słabości lub zapewnia konstrukcje, które ułatwiają uniknięcie tej słabości.
- Na przykład użyj pakietów anty-CSRF, takich jak OWASP CSRFGuard.

Brak nagłówka zapobiegającego przechwytywaniu kliknięć

Strona internetowa nie jest obecnie chroniona przed atakami typu „clickjacking". To rodzaj ataku, który nakłania użytkowników do kliknięcia czegoś, czego nie zamierzali kliknąć.

Sugerowane rozwiązanie:

- Nowoczesne przeglądarki internetowe obsługują nagłówki HTTP Content-Security-Policy i X-Frame-Options. Upewnij się, że jeden z nich jest ustawiony na wszystkich stronach internetowych zwracanych przez Twoją witrynę/aplikację.

Wrażliwa biblioteka JS

Zidentyfikowana biblioteka jquery w wersji 1.8.3 jest podatna na ataki.

Sugerowane rozwiązanie:
Uaktualnij do najnowszej wersji jquery.

Narzędzie SSL LABS:

Raport z analizy w ogólnej ocenie wyników wskazuje na przyznanie najwyższej noty „A".
Jedyne punkty oznaczone jako wady to:

Brak DNS CAA

CAA to akronim od Certification Authority Authorization. CAA jest rekordem DNS określającym, który z wystawców (Urzędów Certyfikacji) może wystawić certyfikat SSL dla określonej domeny.

Sugerowane rozwiązanie:

- Utworzenie rekordu DNS i CAA oraz sporządzenie listy urzędów certyfikacji, które będą wykorzystywane przez firmę.

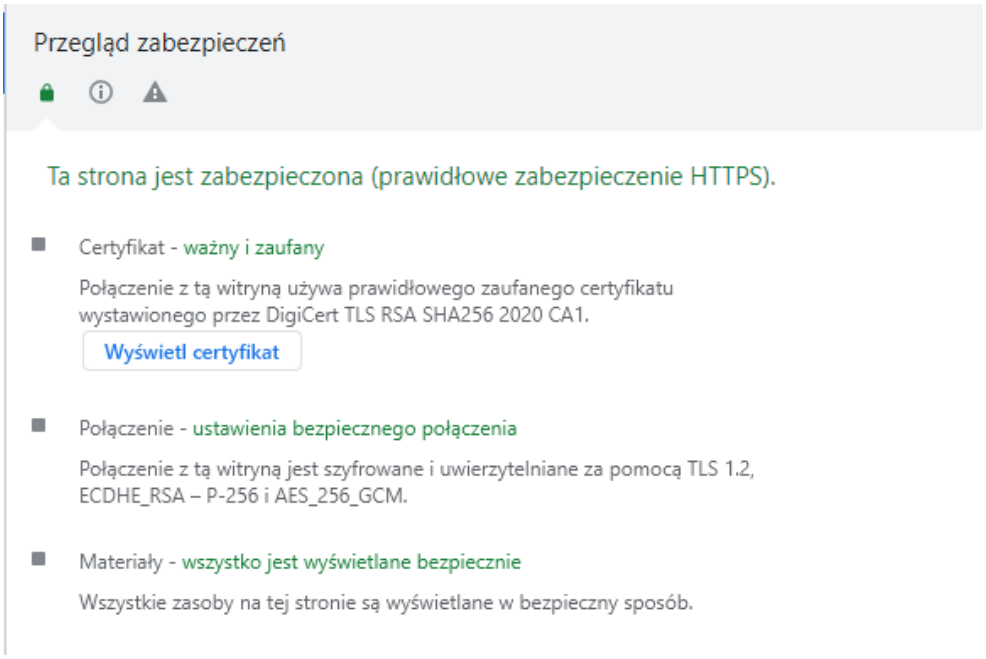
Niektóre z protokołów TLS są oznaczone jako słabe

TLS (ang. Transport Layer Security) jest szeroko stosowanym protokołem bezpieczeństwa zaprojektowanym w celu ułatwienia ochrony prywatności i danych podczas komunikacji przez Internet.

Sugerowane rozwiązanie:

- Konfiguracja serwera TLS powinna umożliwiać tylko wymianę silnych kluczy, a wymiana kluczy powinna zapewniać co najmniej 224-bitowe zabezpieczenia.

Narzędzie Chrome DevTools:
Wykonany przegląd zabezpieczeń przez Chrome Devtools dla głównej strony aplikacji nie wskazuje na występowanie wad zabezpieczeń.



Sucuri SiteCheck:
Skan przez narzędzie Sucuri nie wykrył żadnych wirusów znajdujących się na stronie. Ponadto wskazał, iż strona nie znajduje się na tzw. czarnej liście, która oznacza niebezpieczne strony. Raport oznaczył kilka obszarów stwarzających potencjalne zagrożenie bezpieczeństwa.

<u>Nie wykryto zapory sieciowej aplikacji</u>

Sugerowane rozwiązanie:
Zainstaluj Web Application Firewall w chmurze, aby zapobiec włamaniom do witryny i atakom DDoS.

<u>Brak nagłówka bezpieczeństwa zapobiegającemu Content Type sniffing</u>

Sugerowane rozwiązanie:
Aby poprawić bezpieczeństwo Twojej witryny (i użytkowników) przed niektórymi typami podsłuchiwania pobierania zaleca się dodanie do witryny następującego nagłówka:
X-Content-Type-Options: nosniff

<u>Brak nagłówka bezpieczeństwa Strict-Transport-Security</u>

Sugerowane rozwiązanie:
Utwórz nagłówek Strickt-Transport-Security za pomocą jednej z dostępnych metod

Narzędzie VirusTotal:
Narzędzie wskazało listę zawierającą analizę wykonaną przez dostawców zabezpieczeń. Każdy z dostawców, który dokonał analizy oznaczył stronę jako wolną od wirusów. Ponadto wszystkie głosy oddane na stronę w związku z bezpieczeństwem w zakładce społeczność są pozytywne.

4. Raport odnalezionego defektu bezpieczeństwa.

<table>
<tr><td colspan="2">ID: DE007</td><td>Data: 07.06.2023</td></tr>
<tr><td colspan="3">Autor: Robert Jaszewski</td></tr>
<tr><td colspan="3">Tytuł: Funkcja logowania dwuetapowego nie działa w pełnym zakresie</td></tr>
<tr><td>Obszar: Funkcjonalność, Bezpieczeństwo</td><td>Wpływ: Poważny</td><td>Priorytet: Wysoki</td></tr>
<tr><td colspan="3">Warunki wstępne:
1. Otwarta strona: https://www.gog.com/
2. Dostęp do utworzonego konta w systemie
3. Funkcja logowania dwuetapowego zaznaczona w ustawieniach konta
4. Użytkownik już raz uzyskał dostęp do konta poprzez dwuetapowy proces logowania na jakimkolwiek urządzeniu lub przeglądarce w tej samej lokalizacji co docelowe środowisko testowe</td></tr>
<tr><td>Kroki do reprodukcji (opis)
1. Zaloguj się do konta z aktywną funkcją logowania dwuetapowego na nieużywanej przez to konto dotychczas przeglądarce lub urządzeniu</td><td>Rezultat oczekiwany
Po wpisaniu i zatwierdzeniu prawidłowych danych logowania, uruchamia się drugi etap weryfikacji, a użytkownik wciąż nie jest zalogowany</td><td>Rezultat rzeczywisty
Po wpisaniu i zatwierdzeniu prawidłowych danych logowania, użytkownik zostaje zalogowany z pominięciem drugiego etapu weryfikacji</td></tr>
<tr><td colspan="3">Środowisko testowe:
Przeglądarki: Google Chrome v. 114.0.5735.91 (x64), Firefox Wersja 113.0.2 (64 bity), Opera Wersja: 99.0.4788.3, Safari Wersja 16.5.1
System: Windows 10 (x64), macOS 10.15.7, Ubuntu 20.04.6 LTS, Android 10</td></tr>
<tr><td colspan="3">Status incydentu: Oczekuje na rozpatrzenie</td></tr>
<tr><td colspan="3">Załączniki: https://drive.google.com/file/d/1XUE4OY-lcthzxeVP4Wkvc3B9ycQrHMza/view?usp=drive_link</td></tr>
<tr><td colspan="3">Komentarz: Zgodnie z opisem funkcjonalności dwuetapowego logowania, który widnieje w ustawieniach konta w zakładce „login i bezpieczeństwo” i w dokumencie na stronie aplikacji, za każdym razem, gdy użytkownik loguje się na konto z aktywną tą funkcjonalnością przez niezweryfikowane dotychczas urządzenie lub przeglądarkę, niezależnie od tego czy przeszedł uprzednio weryfikacje dwuetapową na innym urządzeniu lub przeglądarce w tej samej lokalizacji, powinien uruchomić się drugi etap logowania. Jeśli jednak któreś z nieużywanych dotychczas urządzeń lub przeglądarek znajduje się w tej samej lokalizacji, w której już raz nastąpiło zalogowanie na to konto, funkcja nie działa, a drugi etap logowania zostaje pominięty. Funkcjonalność nie działa zatem zgodnie z jej opisem, który wprowadza użytkownika dodatkowo w błąd. W takiej sytuacji dopiero zmiana lokalizacji powoduje, że funkcja ta zostanie uruchomiona. Stwarza to niebezpieczeństwo, iż w pewnych okoliczność osoba postronna może uzyskać dostęp do konta użytkownika.</td></tr>
</table>

5. Podsumowanie raportu

Przeprowadzona analiza oraz testy bezpieczeństwa pozwalają stwierdzić, że aplikacja w ogólnym rozrachunku jest bezpieczna dla użytkownika oraz wolna od wirusów. Strona jest aktywna już od wielu lat i dotychczas społeczność nie zgłaszała żadnych poważnych problemów dotyczących bezpieczeństwa. Firma prowadząca stronę ma dobrą renomę oraz zyskała sobie zaufanie użytkowników. Mimo wszystko aplikacja nie jest całkowicie wolna od pewnych wad wpływających na bezpieczeństwo. Narzędzia skanujące stronę pod względem ryzyka bezpieczeństwa choć nie wykryły poważnych zagrożeń, wskazują na pewne obszary, które mogą wymagać poprawy. Podczas wykonywania testów manualnie zaobserwowano również takie problemy jak nieprawidłowe działanie funkcji logowania dwuetapowego oraz słabe wymagania dotyczące utworzenia hasła dla konta przy rejestracji. Wprowadzenie przytoczonych w tym raporcie sugestii i rozwiązań problemów może pozytywnie wpłynąć na poprawę bezpieczeństwa strony.