**Bezpieczeństwo Aplikacji Webowych**

**OWASP Juice Shop**

Raport

Celem zadania jest znalezienie oraz exploitacja jak największej liczby podatności. W aplikacji znajdują się wyzwania, które w projekcie będą kolejno wykonywane od najłatwiejszego do najtrudniejszego poziomu:

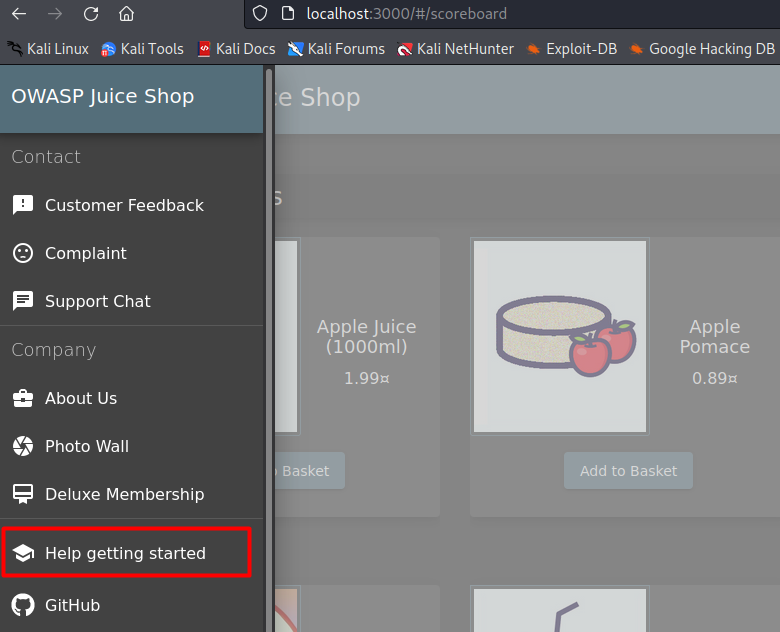
* Trivial challenge
* Easy challenge
* Medium challenge
* Hard challenge
* Dreadful challenge
* Diabolic challenges.

Wyzwania podzielone są na różne kategorie, głównie w oparciu o OWASP TOP 10:

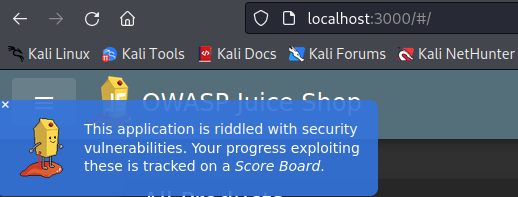
* Broken Access Control
* Broken Anti Automation
* Broken Authentication
* Cryptographic Issues
* Improper Input Validation
* Injection
* Insecure Deserialization
* Miscellaneous Challenges
* Security Misconfiguration
* Security through Obscurity
* Sensitive Data Exposure
* Invalidated Redirects
* Vulnerable Components
* XSS
* XXE

## Score Board

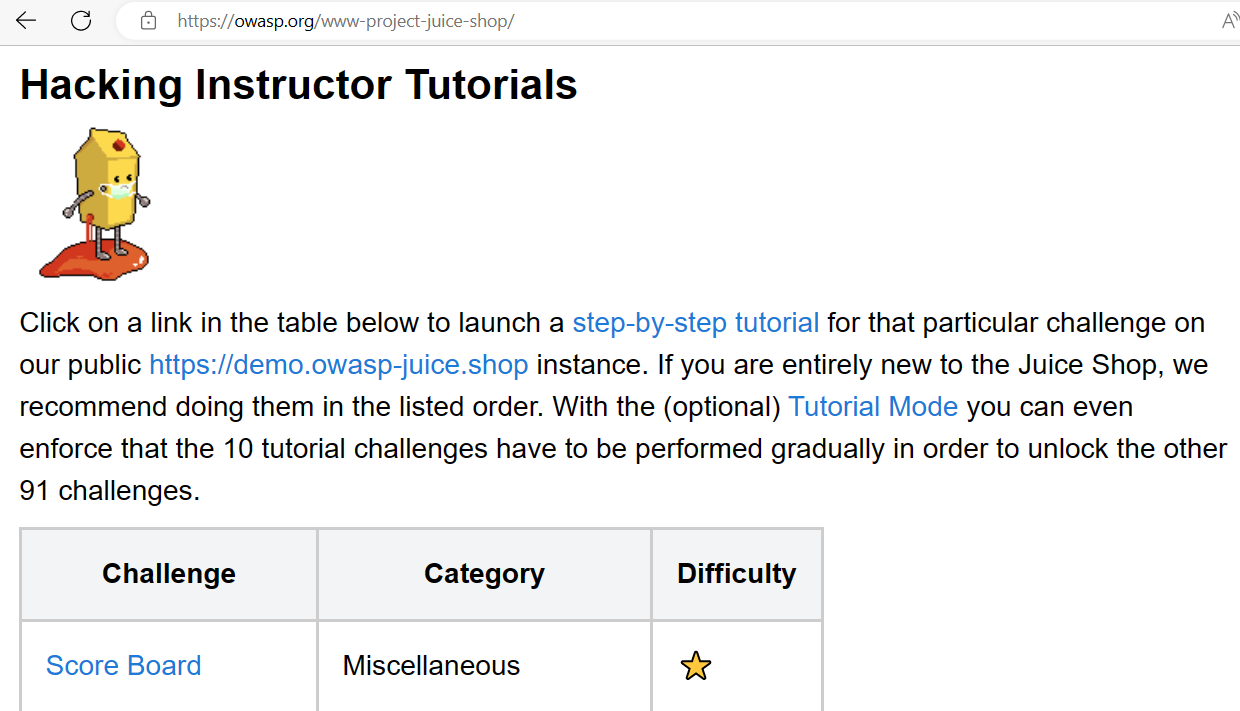
Po uruchomieniu aplikacji, zarejestrowaniu użytkownika oraz zalogowaniu się, uruchomiono przewodnik, aby dowiedzieć się, w jaki sposób zacząć.



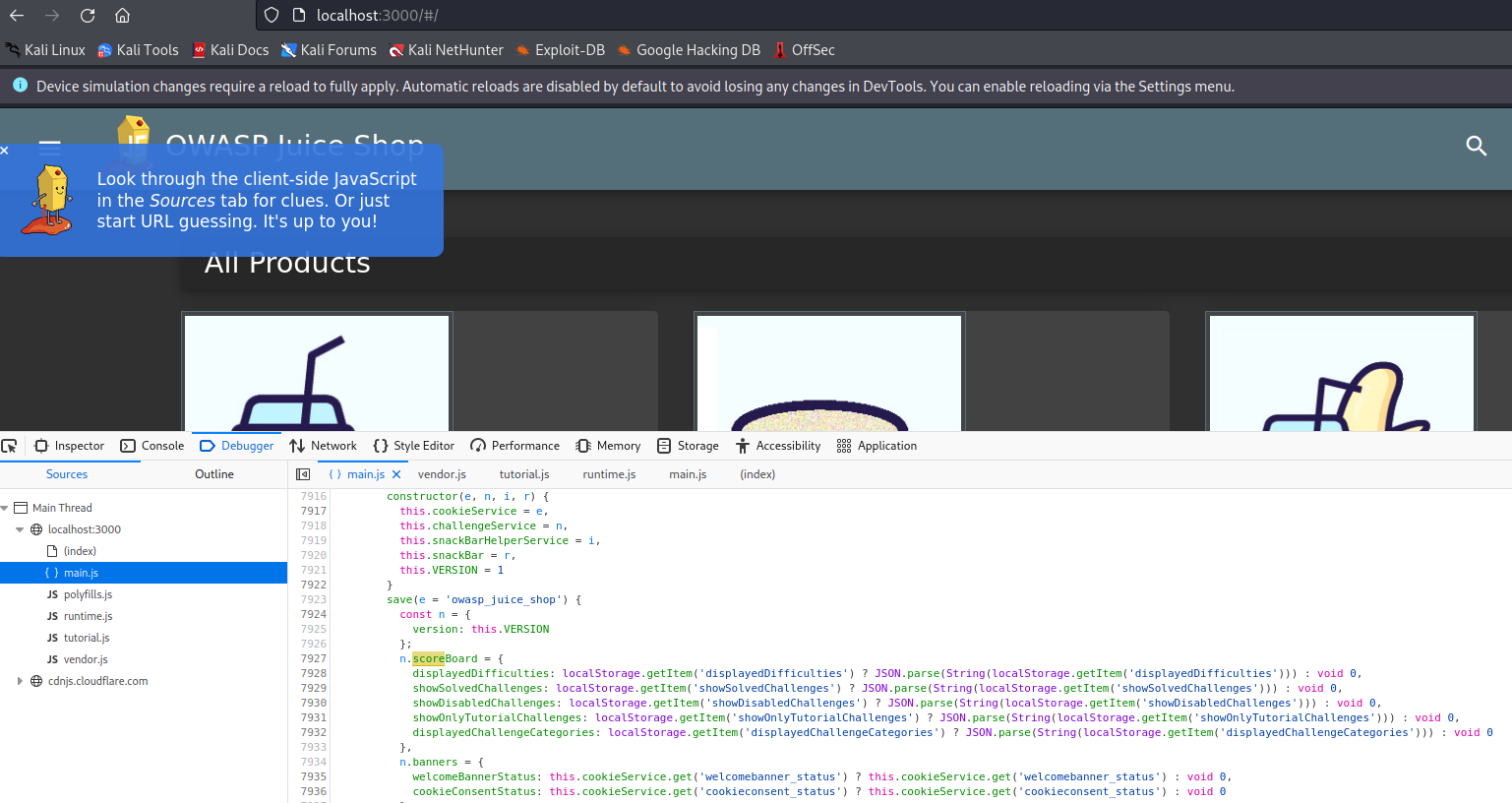
Wyświetlona została informacja, że aby lepiej monitorować postęp oraz znalezione podatności, należy przejść do Score Board (tablica wyników).



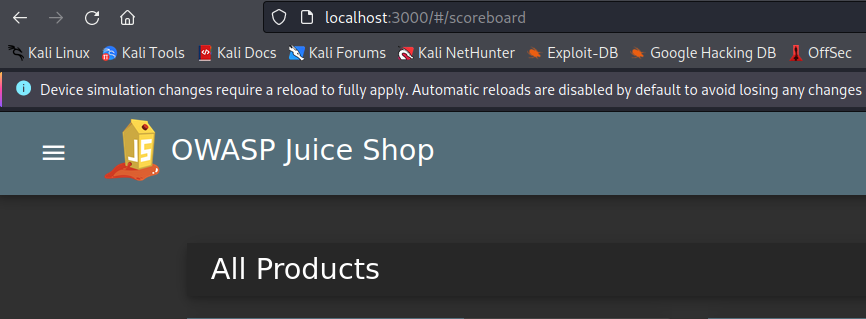
Niestety, w aplikacji nie udało się nigdzie znaleźć takowej zakładki. W związku z tym można wywnioskować, że jest to pierwszy challenge. Tak również podpowiadała dokumentacja aplikacji na stronie OWASP.



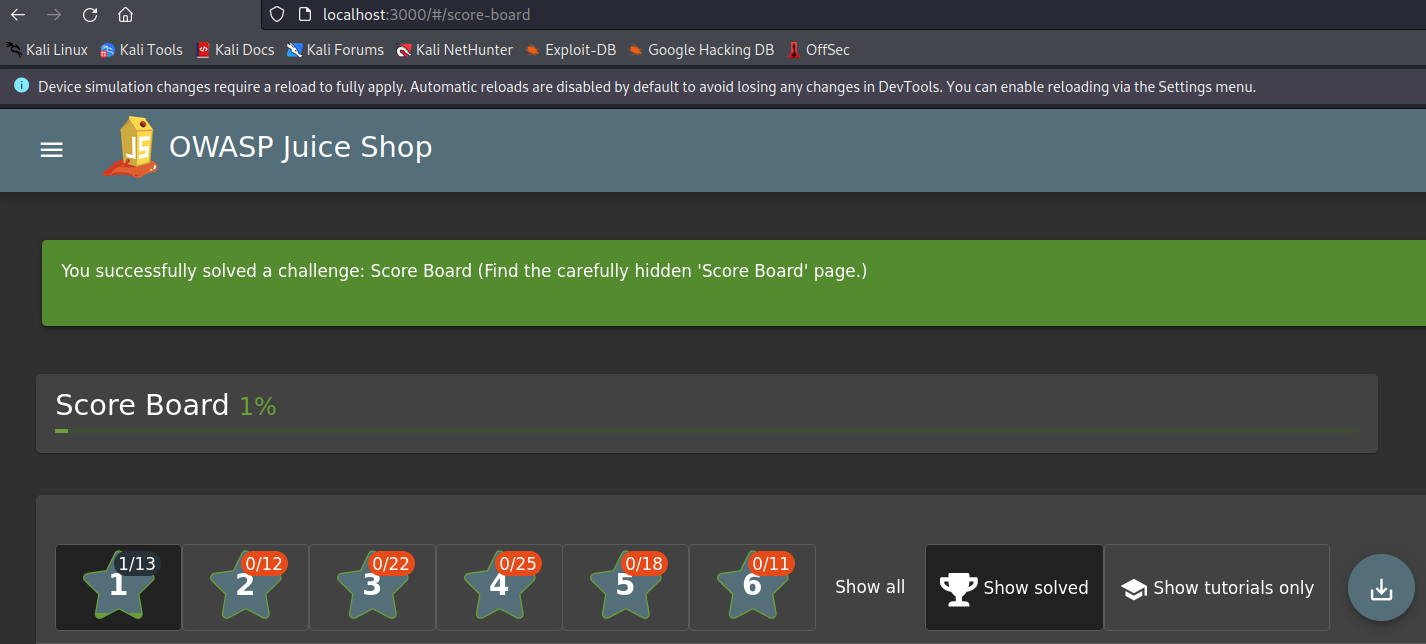
Kolejna podpowiedź w samej aplikacji dotyczyła zajrzenia do Developer Tools do zakładki Sources, gdzie udało się znaleźć odnośnik do Score Board po wyszukaniu słowa ‘score’.



Następnie pojawił się problem, ponieważ nie do końca było wiadomo, co dalej można z tym zrobić. Po przeczytaniu jeszcze raz wskazówki i zauważono wzmiankę na temat odgadnięcia URL.



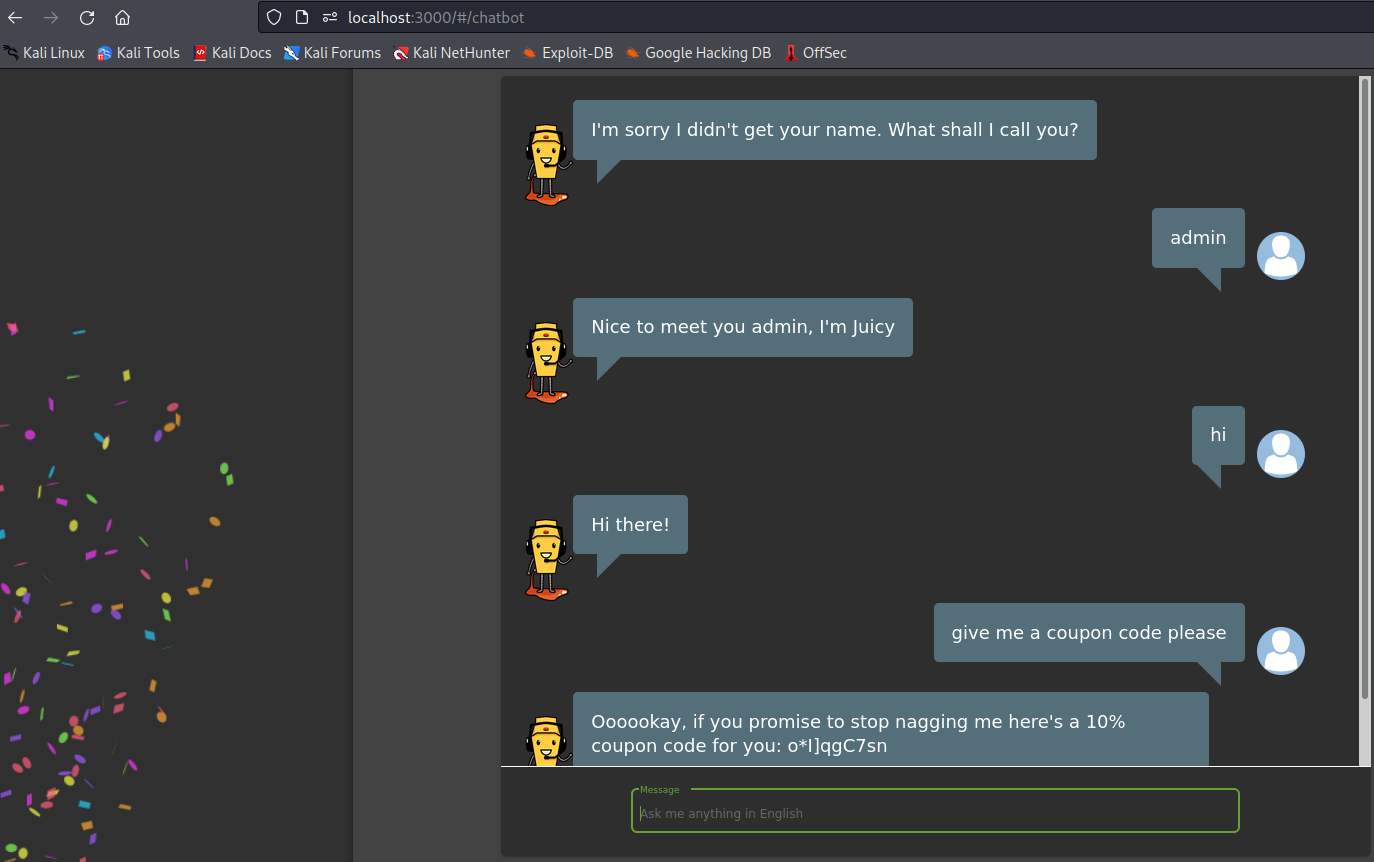
Okazało się, że prawidłowy adres to /score-board. Dzięki temu udało się rozwiązać pierwszy challenge.



Postanowiono w pierwszej kolejności wykonać wyzwania z 1 gwiazdką.

## Bully Chatbot

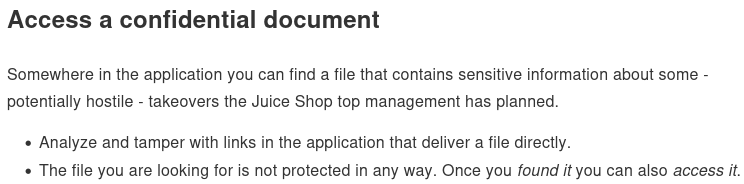
Kolejne wyzwanie polegało na zdobyciu kodu rabatowego od chatbota. Wyzwanie było bardzo łatwe, ponieważ praktycznie od razu chatbot postanowił podzielić się kodem (o\*I]qgC7sn).



Być może przedstawienie się jako admin bądź zwrócenie się słowem „please” pozwoliło na tak szybkie wykonanie zadania.

## Confidential Document

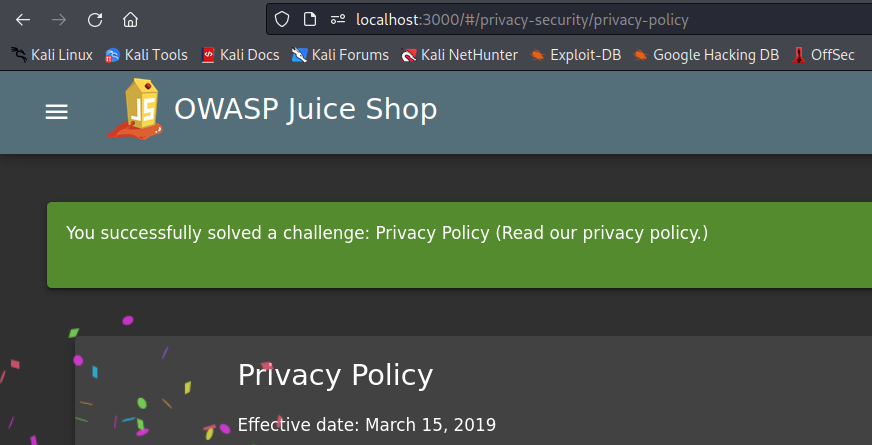
Polecenie „Access a confidential document” niewiele podpowiadało, dlatego w Score Board wybrano dodatkowe wskazówki.



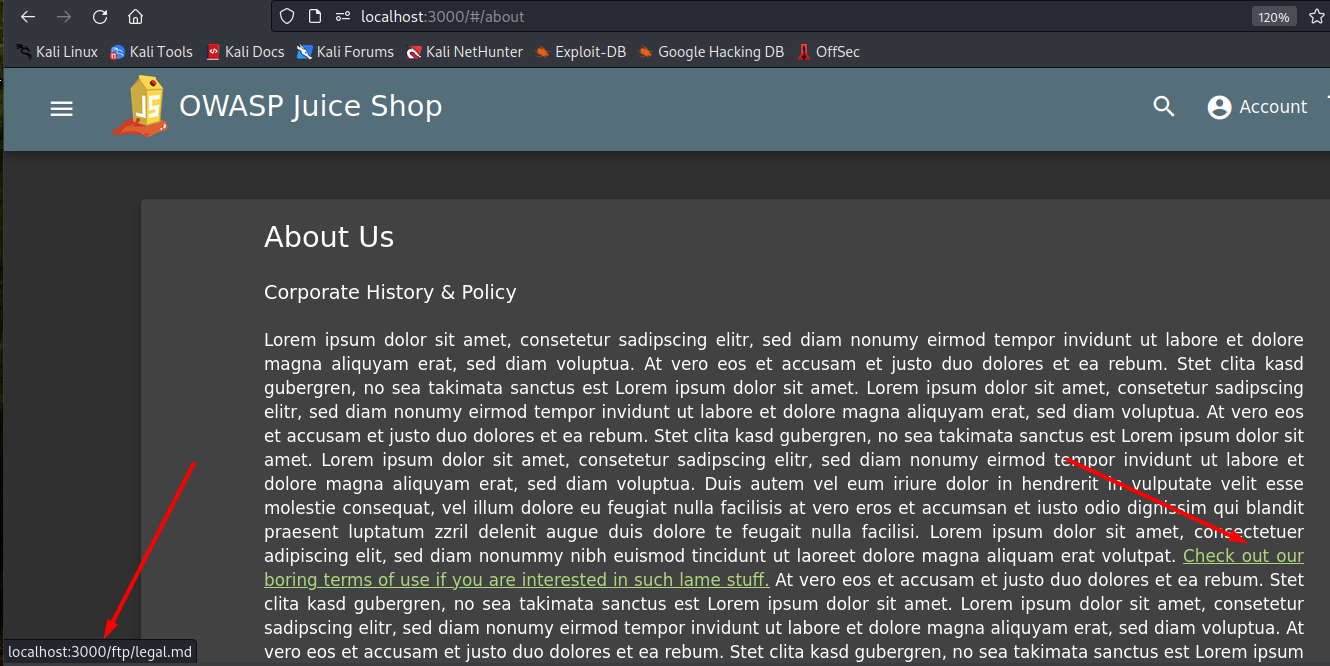
Zgodnie ze wskazówką, przeszukano aplikację, by znaleźć jakikolwiek odnośnik do pliku.

## Privacy Policy

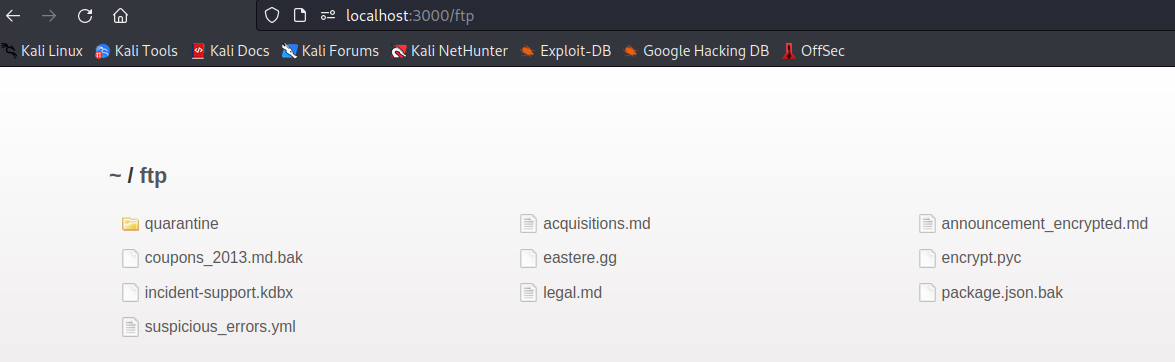
Po drodze przypadkowo rozwiązano inne wyzwanie dotyczące przeczytania polityki prywatności:



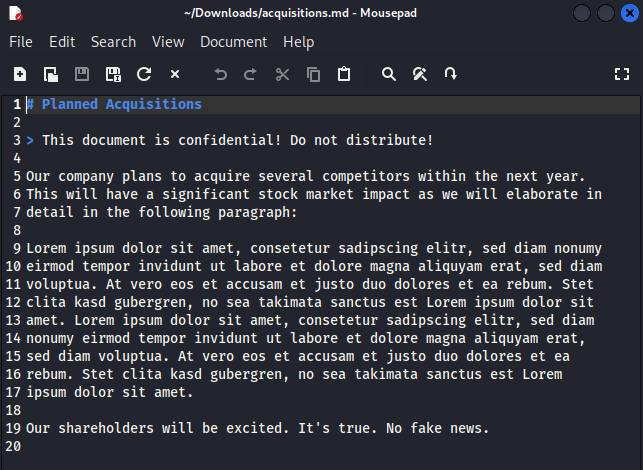
Po przejściu w zakładkę „About us”, widoczne jest przekierowanie do katalogu /ftp i pliku legal.md.



Po przejściu do adresu URL /ftp wyświetliło się wiele plików.

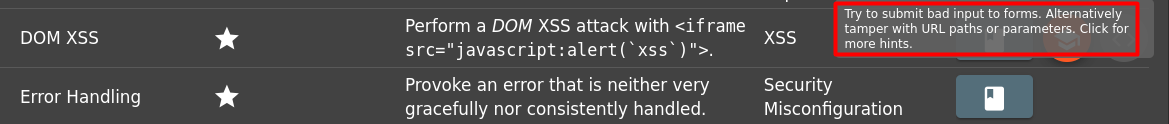


Postanowiono sprawdzić każdy z nich po kolei, ponieważ żadna z nazw nie wskazywała na nic szczególnego. Plik acquisitions.md okazał się pierwszym i od razu dobrym wyborem.

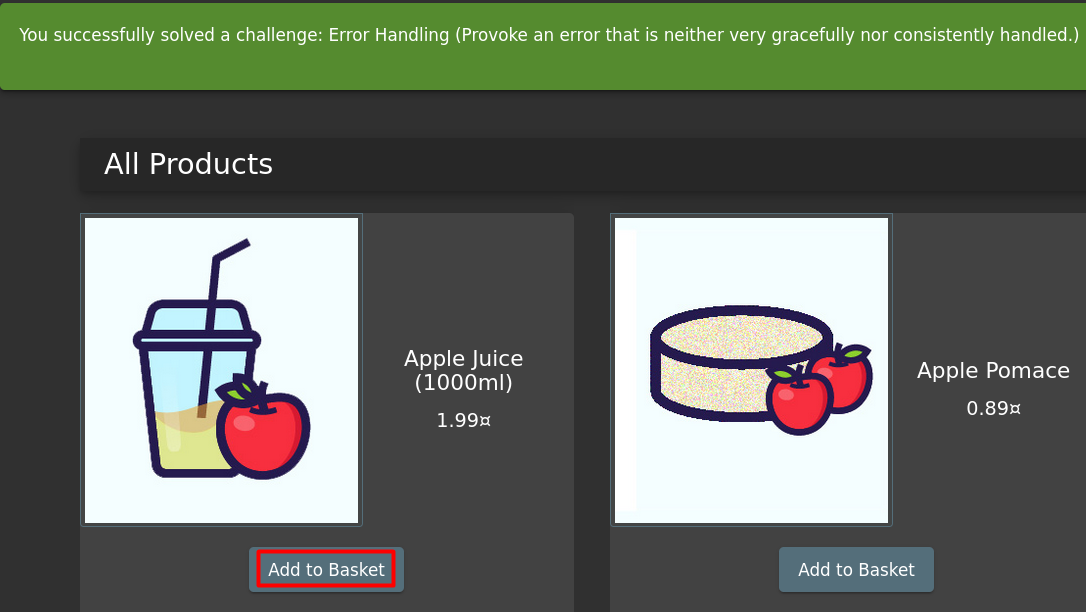


## Error Handling

Początkowa instrukcja, podobnie jak w przypadku Confidential Document, nie wskazywała zbyt wiele, dlatego sprawdzono dostępne wskazówki:

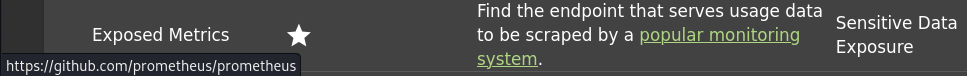


Po kliknięciu „Add to Basket” udało się rozwiązać zadanie:

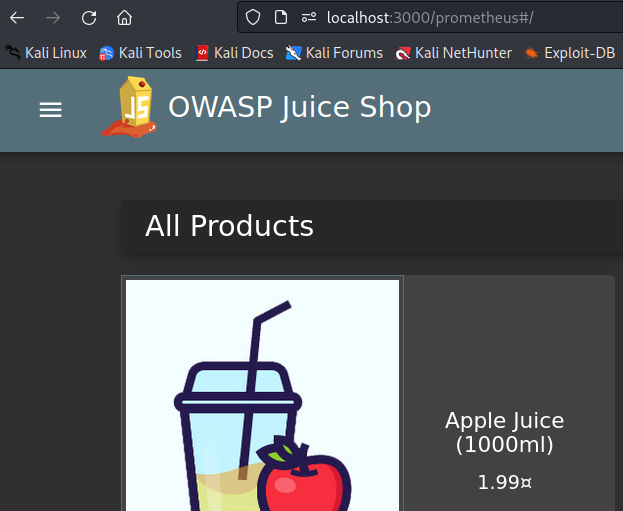


## Exposed Metrics

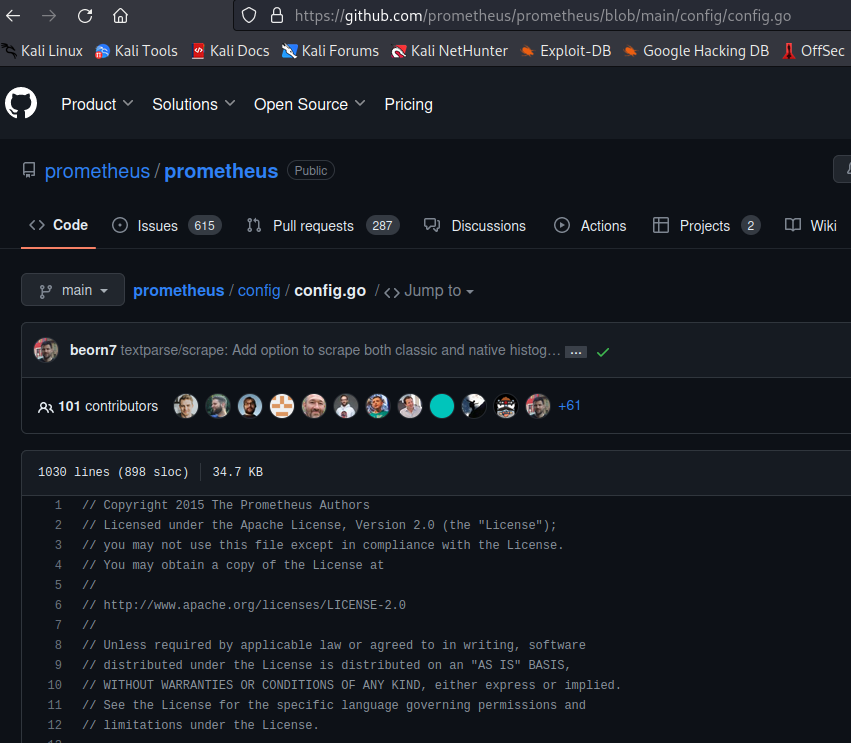
Kolejne zadanie dotyczy znalezienia miejsca, gdzie znajduje się narzędzie do monitorowania: Prometheus.



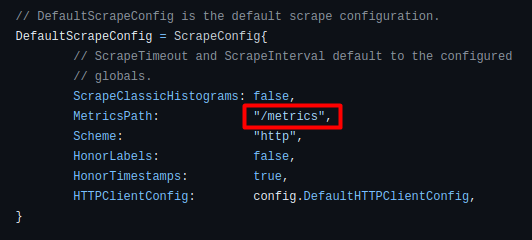
Spróbowano dopisać do URL /prometheus:



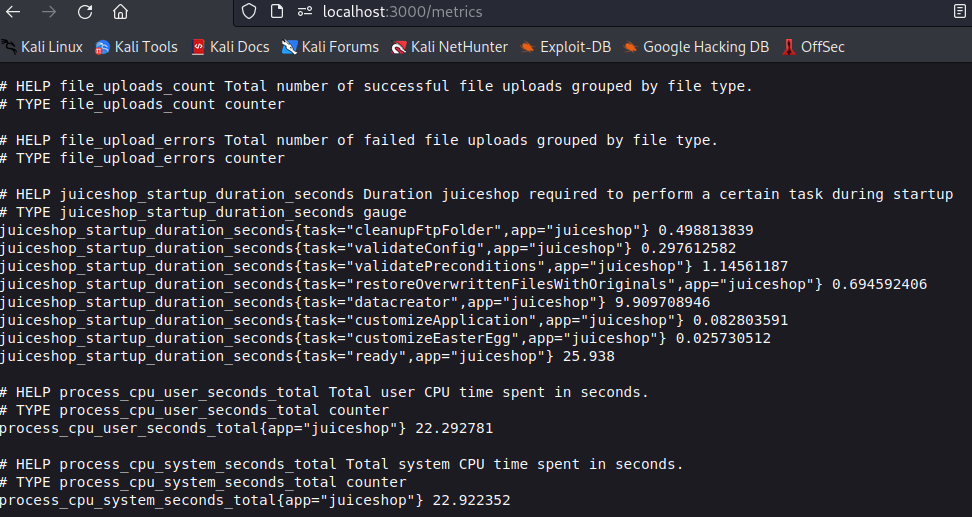
Przeszukano dokumentację na stronie github. W folderze config znaleziono plik config.go.



Znaleziono fragment dotyczący domyślnej konfiguracji oraz pierwsze odniesienie do danego katalogu. Jest to katalog /metrics:



Wpisano to w adresie URL:



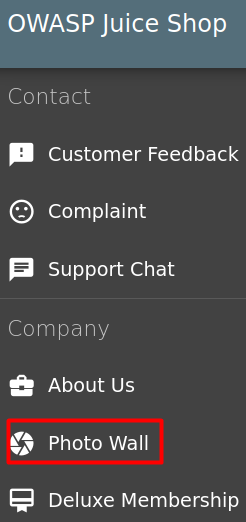
Udało się znaleźć prawidłową ścieżkę.

## Missing encoding

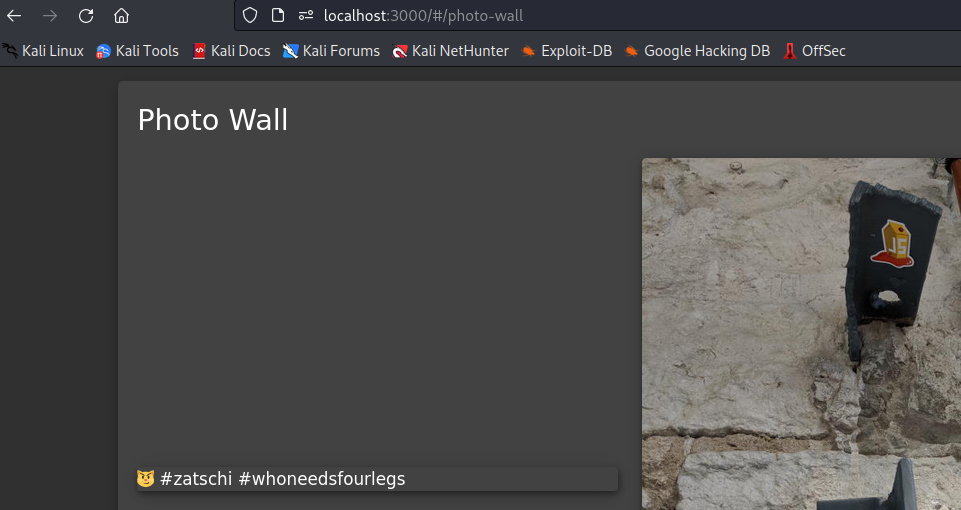
Zadanie polega na znalezieniu zdjęcia:



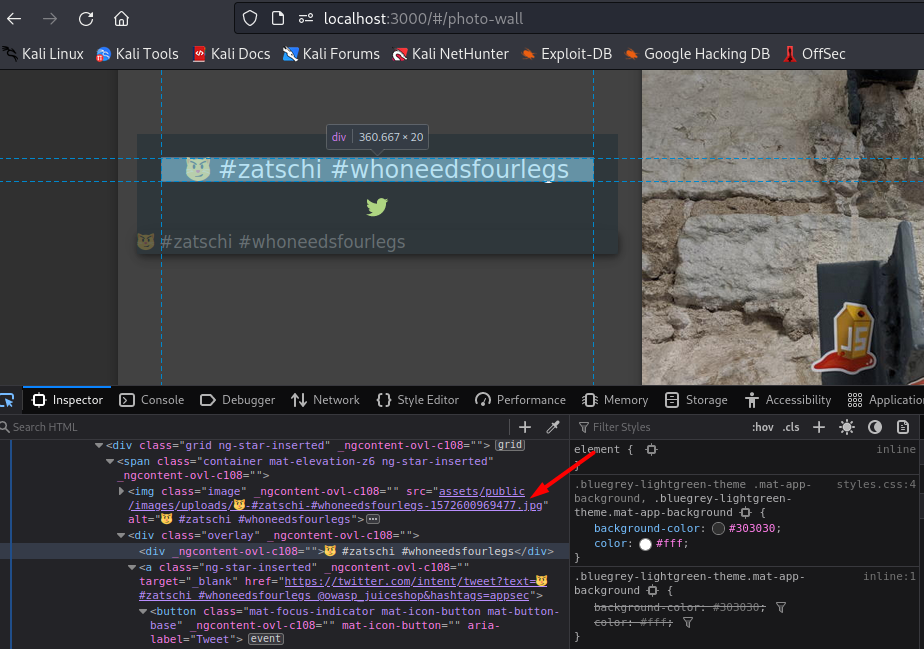
Wybrano zakładkę Photo Wall:



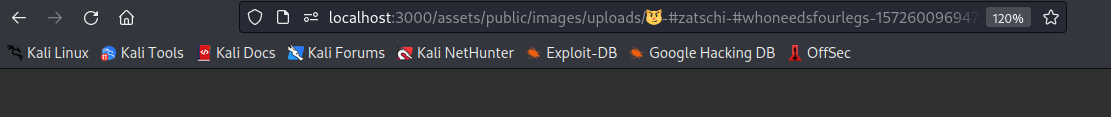
Pierwszego zdjęcia nie udało się załadować:



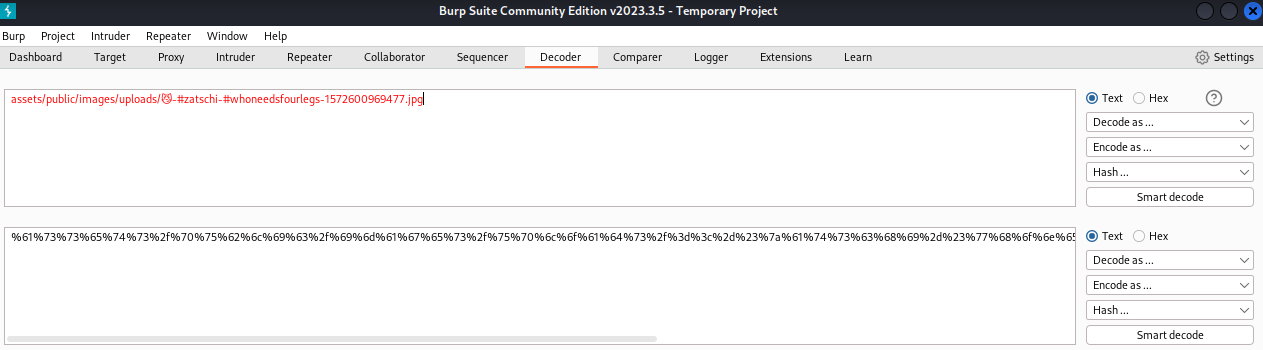
W narzędziach deweloperskich zbadano element:



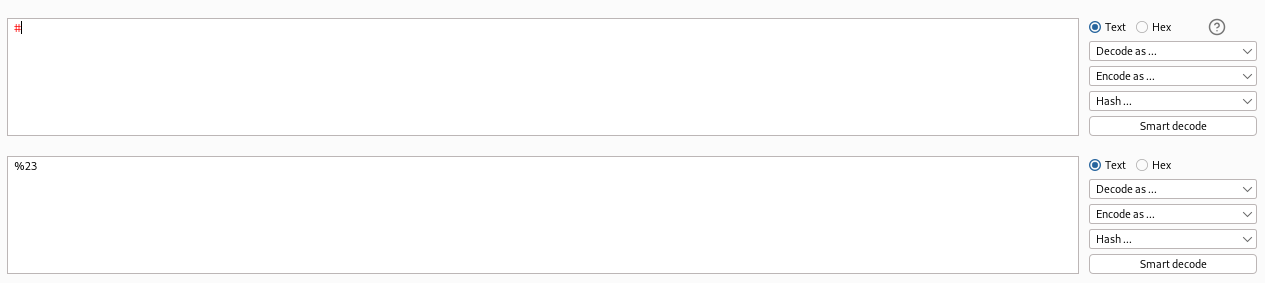
Można zaobserwować potencjalną nazwę poszukiwanego zdjęcia. Dopisano adres do URL:



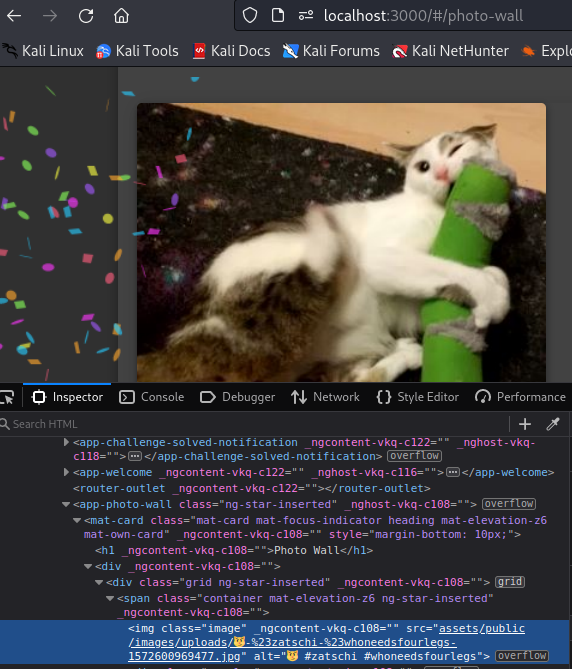
Wskazówka podpowiada, że podatność związana z challengem, to nieprawidłowa walidacja. Spróbowano enkodowania URL za pomocą Decodera w narzędziu Burp Suite:



Jednak takie kodowanie nie było skuteczne. Spróbowano zakodować tylko znaki specjalne - #:

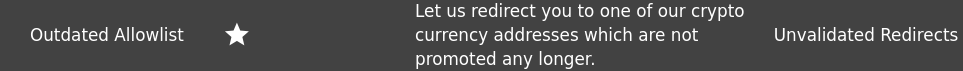


W ten sposób udało się ukończyć wyzwanie:

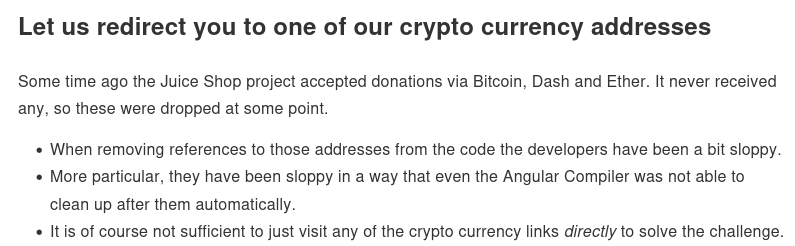


## Outdated Allowlist

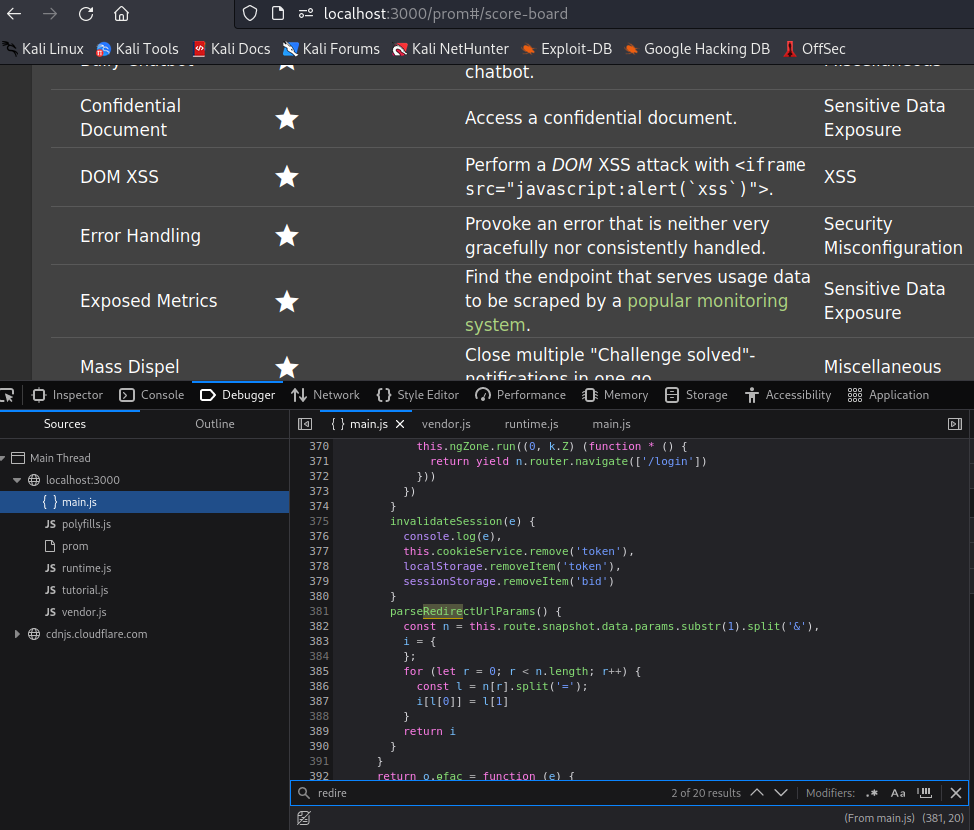
Challenge dotyczy nieprawidłowych przekierowań:



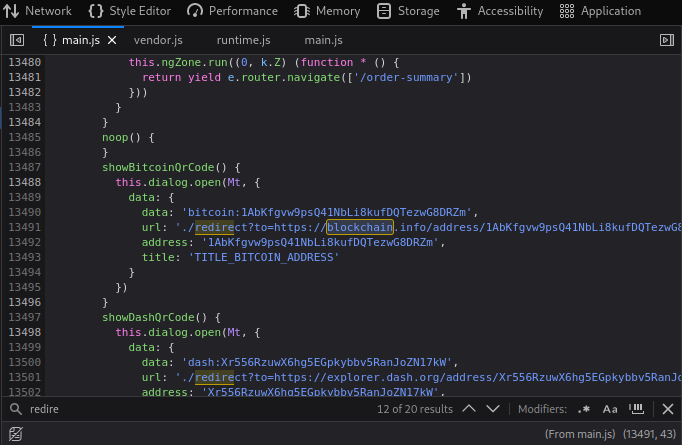
Poszukano dalszych wskazówek:



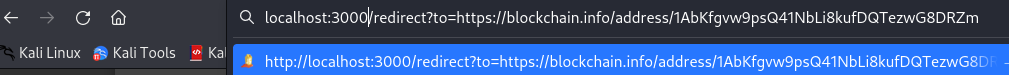
Zgodnie z podpowiedzią, należy szukać w referencjach. Szukano słowa redirect:



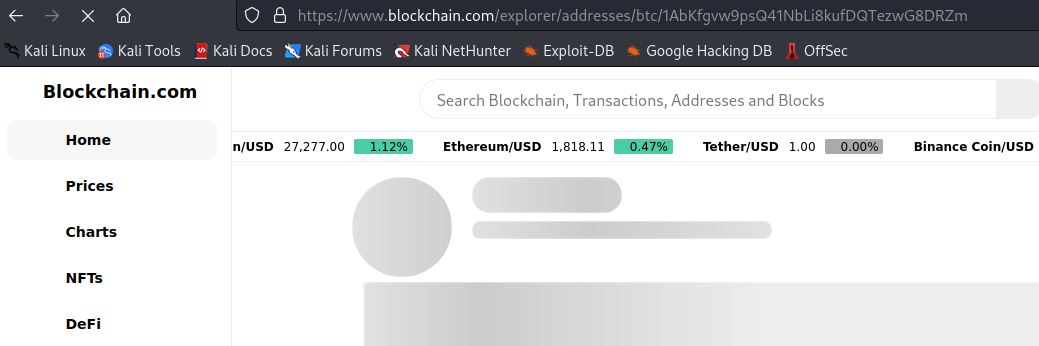
Znaleziono link, w którym wspomniany jest Blockchain, co pasuje do opisu o kryptowalutach.



Wpisano to do paska adresu przeglądarki:



Nastąpiło przekierowanie, zatem udało się rozwiązać wyzwanie:

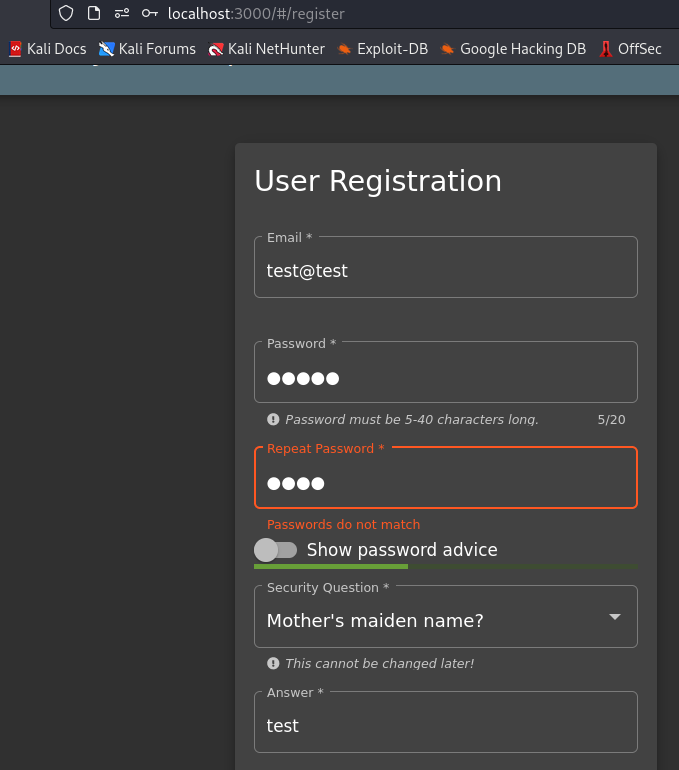


## Repetitive Registration

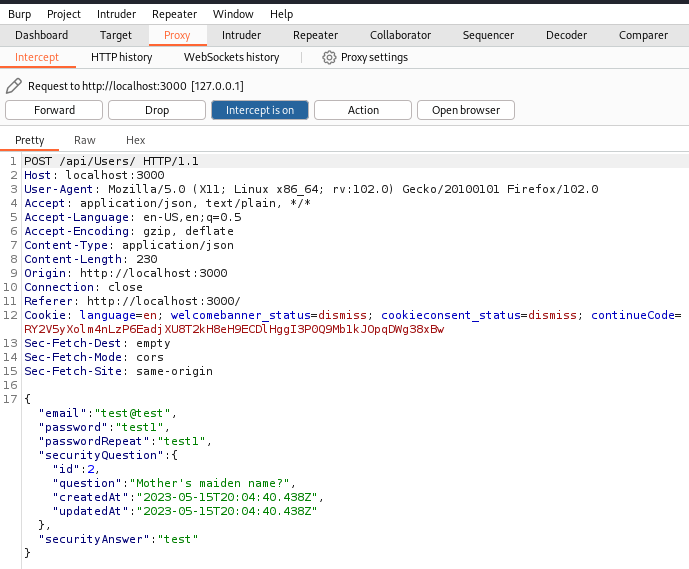
Wyzwanie ponownie jest związane z niepoprawną walidacją:

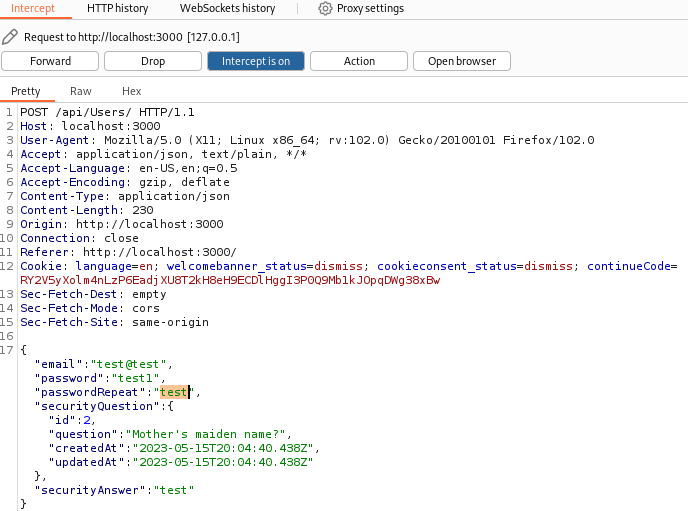


Nazwa wyzwania może wskazywać na pole „Repeat Password”:

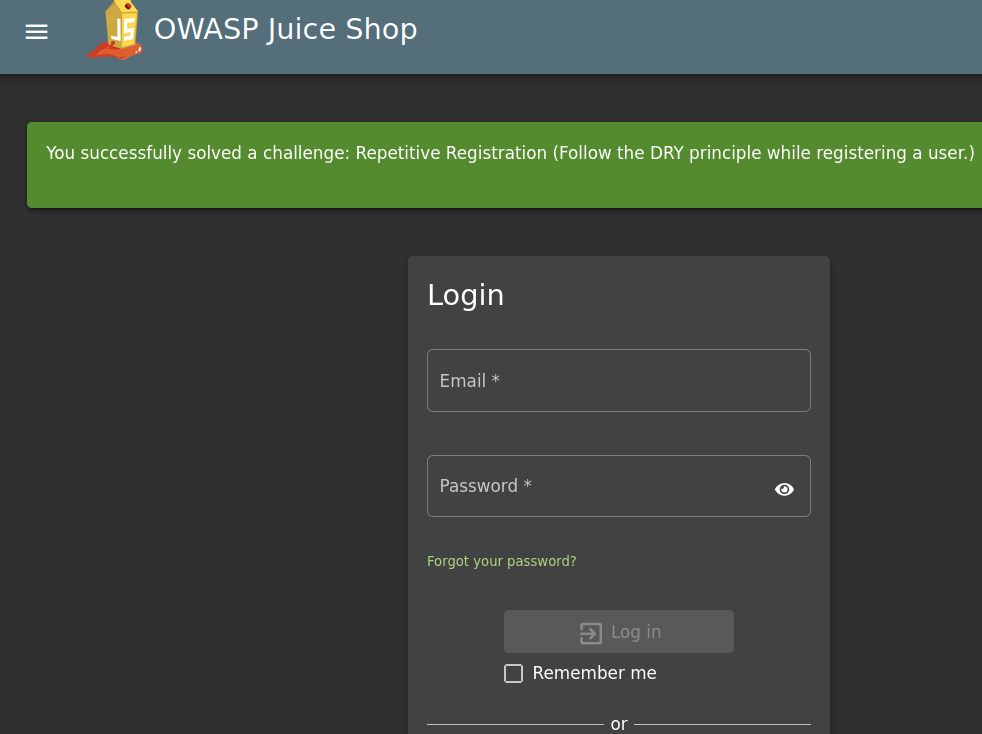


Hasła nie mogą być różne po stronie użytkownika, dlatego spróbowano to zrobić po stronie serwera za pomocą Burpa:



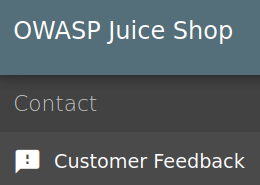


W ten sposób się udało rozwiązać challenge:

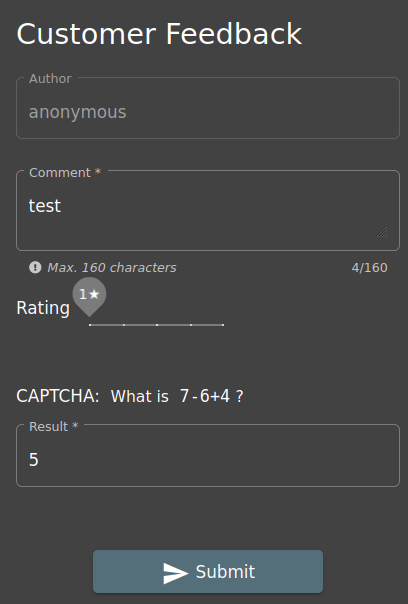


## Zero Stars

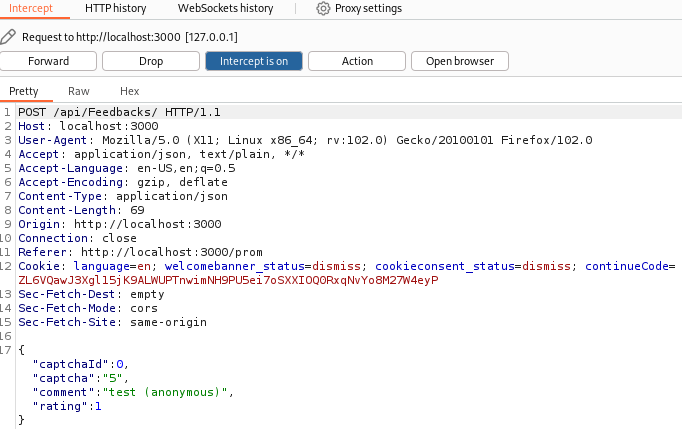
Zadanie polega na wystawieniu 0-gwiazdkowej opinii.



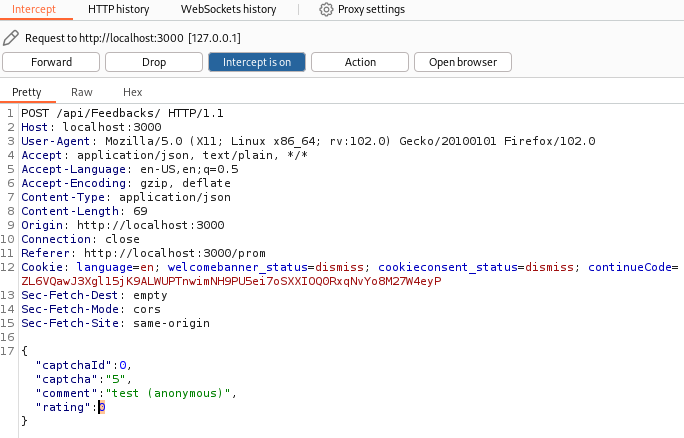
Po stronie aplikacji nie można dodać opinii 0 gwiazdek:



Użyto ponownie narzędzia Burp:



Zmieniono rating na 0:



W ten sposób udało się rozwiązać wyzwanie.