**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:

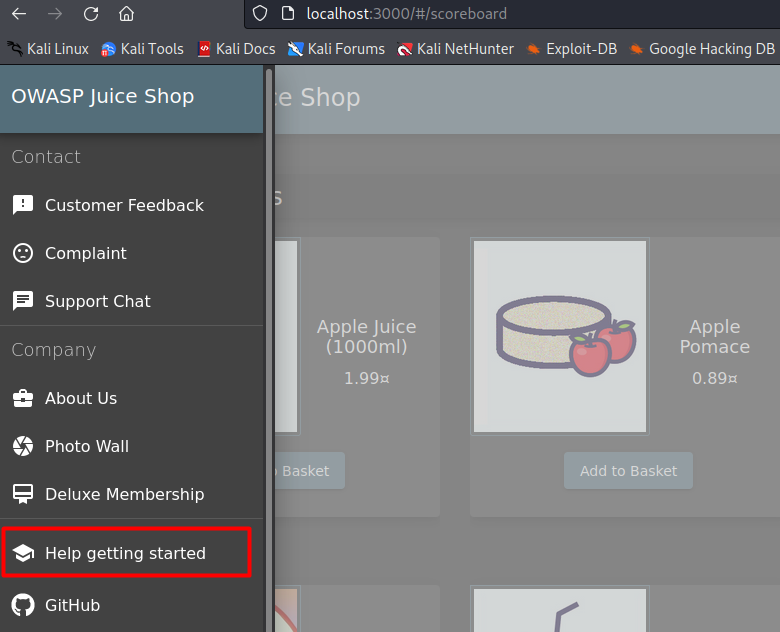
* Trivial challenge
* Easy challenge
* Medium challenge
* Hard challenge
* Dreadful challenge
* Diabolic challenges.

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

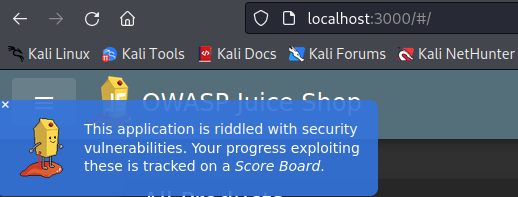
* Broken Access Control
* Broken Anti Automation
* Broken Authentication
* Cryptographic Issues
* Improper Input Validation
* Injection
* Insecure Deserialization
* Miscellaneous Challenges
* Security Misconfiguration
* Security through Obscurity
* Sensitive Data Exposure
* Invalidated Redirects
* Vulnerable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

## Score Board

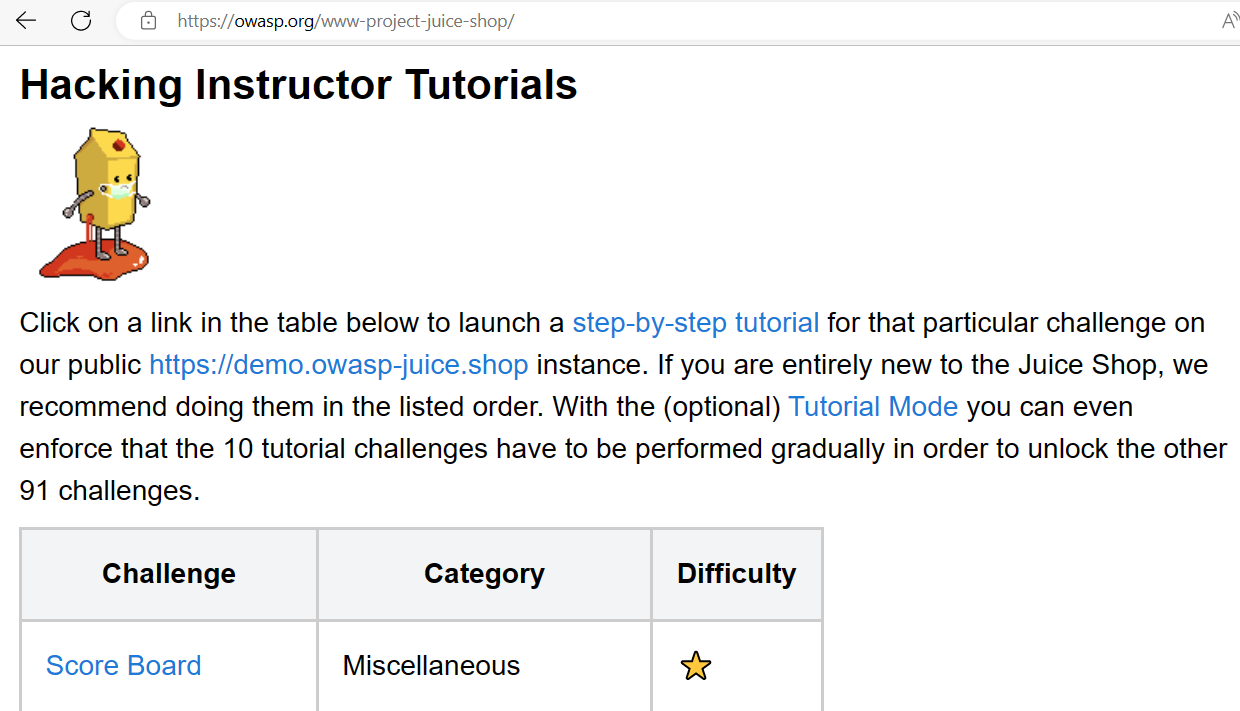
Po uruchomieniu aplikacji, zarejestrowaniu użytkownika oraz zalogowaniu się, postanowiliśmy uruchomić przewodnik, aby dowiedzieć się, w jaki sposób zacząć.



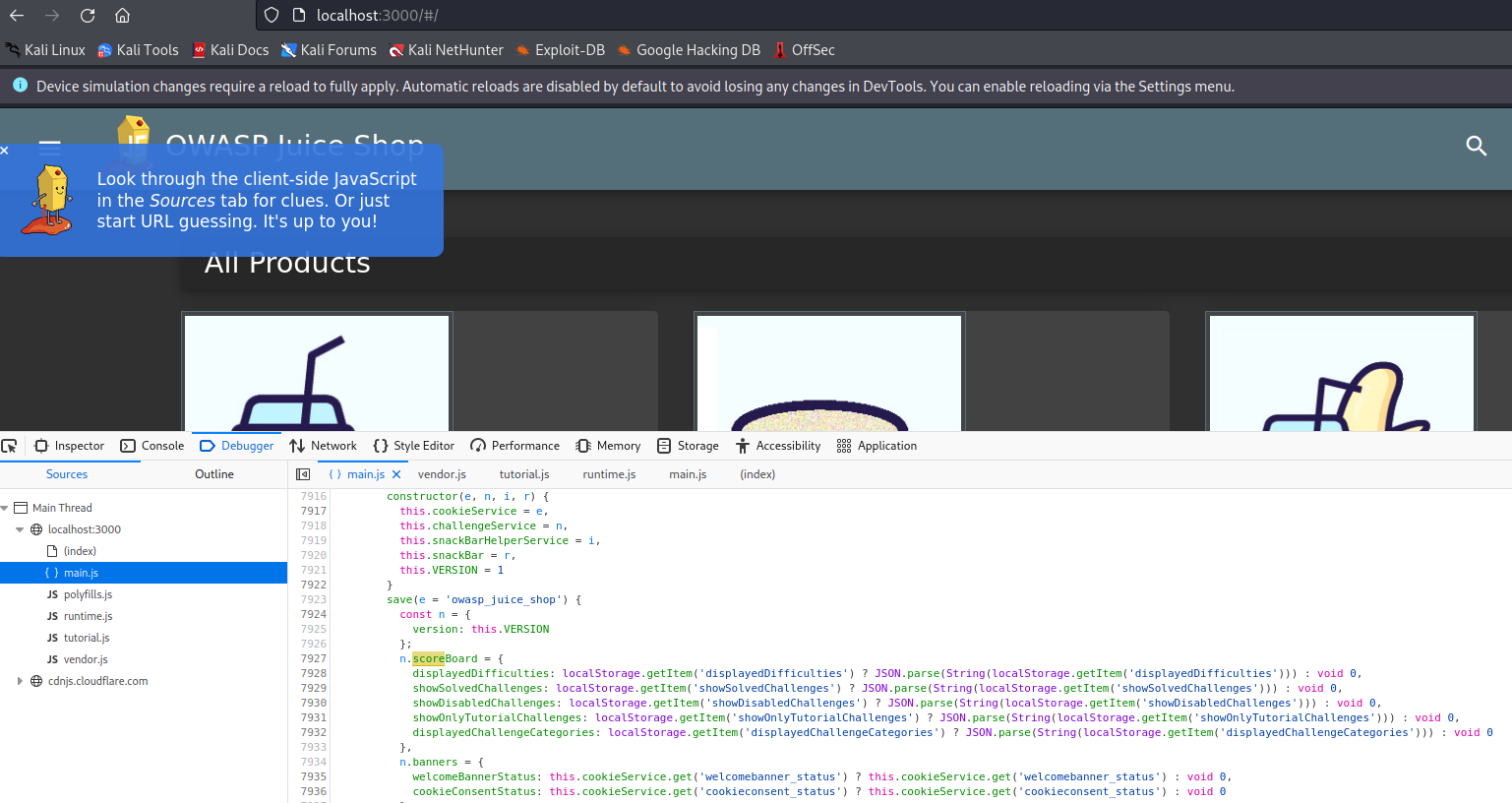
Wyświetlona została informacja, że aby lepiej monitorować postęp oraz znalezione podatności, należy przejść do Score Board (tablica wyników).



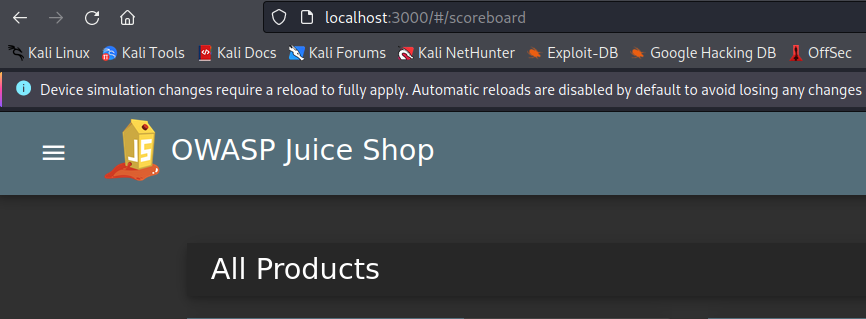
Niestety, w aplikacji nie udało się nigdzie znaleźć takowej zakładki. W związku z tym można wywnioskować, że jest to pierwszy challenge. Tak również podpowiadała dokumentacja aplikacji na stronie OWASP.



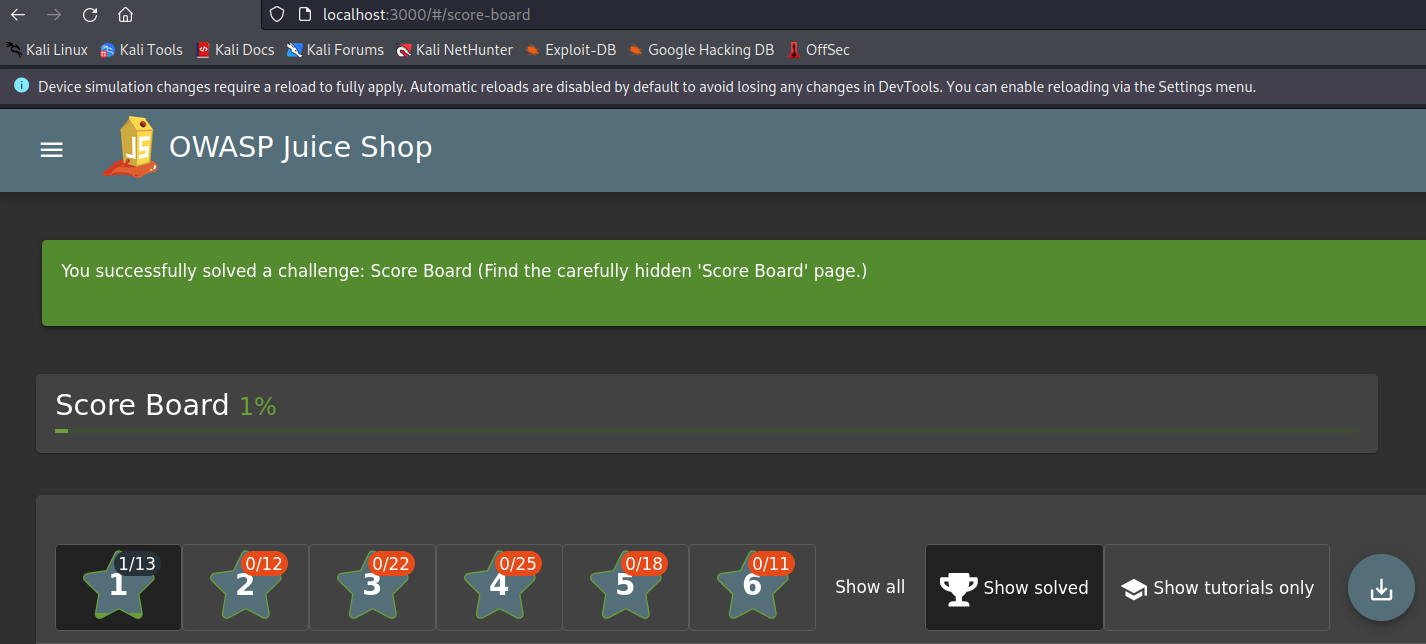
Kolejna podpowiedź w samej aplikacji dotyczyła zajrzenia do Developer Tools do zakładki Sources, gdzie udało się znaleźć odnośnik do Score Board po wyszukaniu słowa ‘score’.



Następnie pojawił się problem, ponieważ nie do końca wiedzieliśmy, co dalej można z tym zrobić. Przeczytaliśmy jeszcze raz wskazówki i zauważyliśmy wzmiankę na temat odgadnięcia URL.



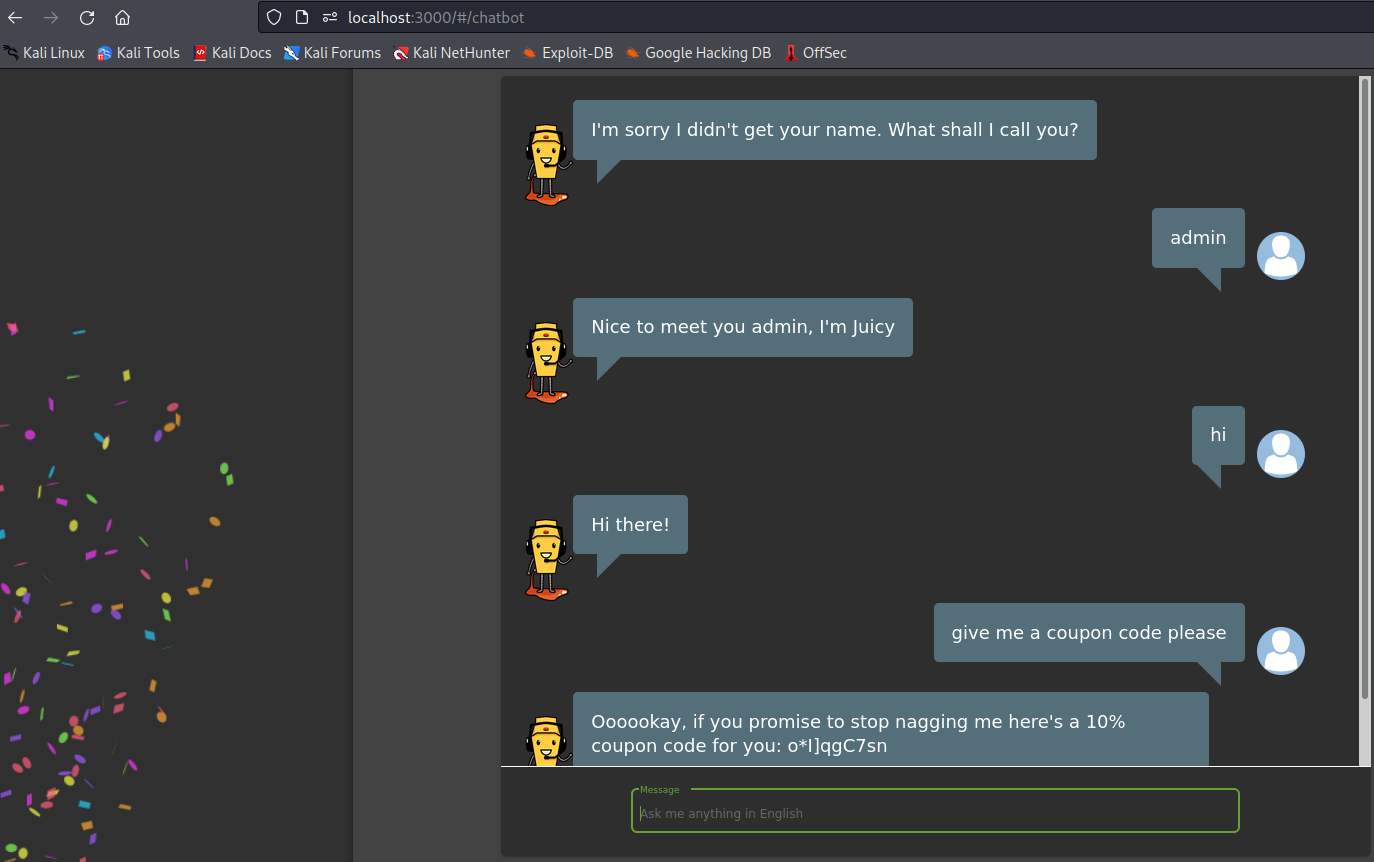
Okazało się, że prawidłowy adres to /score-board. Dzięki temu udało się rozwiązać pierwszy challenge.



Postanowiliśmy w pierwszej kolejności wykonać wyzwania z 1 gwiazdką.

## Bully Chatbot

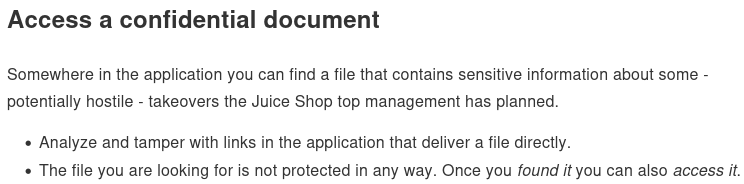
Kolejne wyzwanie polegało na zdobyciu kodu rabatowego od chatbota. Wyzwanie było bardzo łatwe, ponieważ praktycznie od razu chatbot postanowił podzielić się kodem (o\*I]qgC7sn).



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

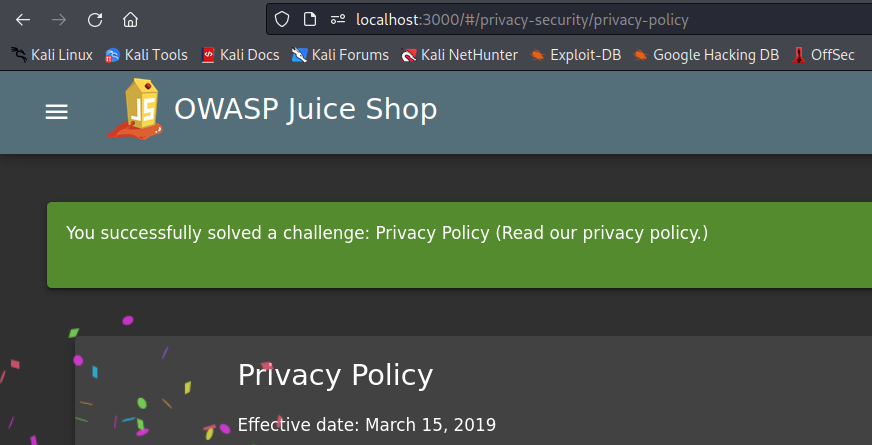
## Confidential Document

Polecenie „Access a confidential document” niewiele nam mówiło, dlatego w Score Board przeszliśmy do wskazówek.

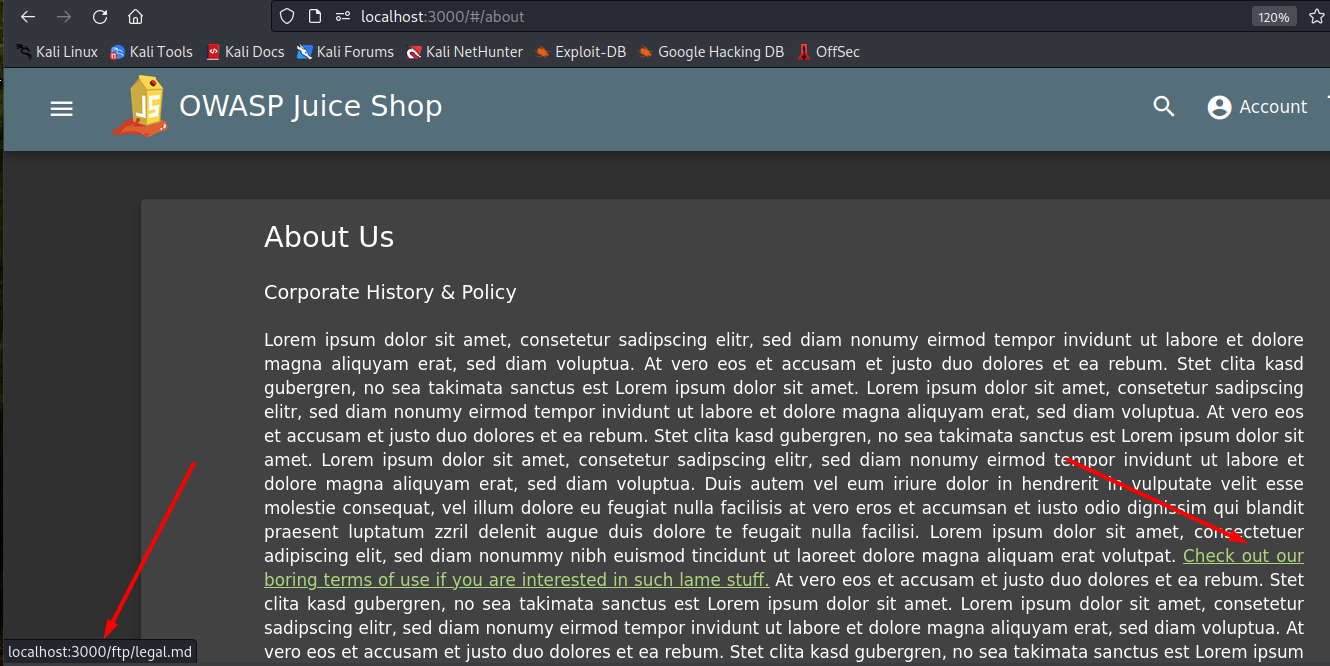


Zgodnie ze wskazówką, postanowiliśmy przeszukać aplikację, by znaleźć jakikolwiek odnośnik do pliku.

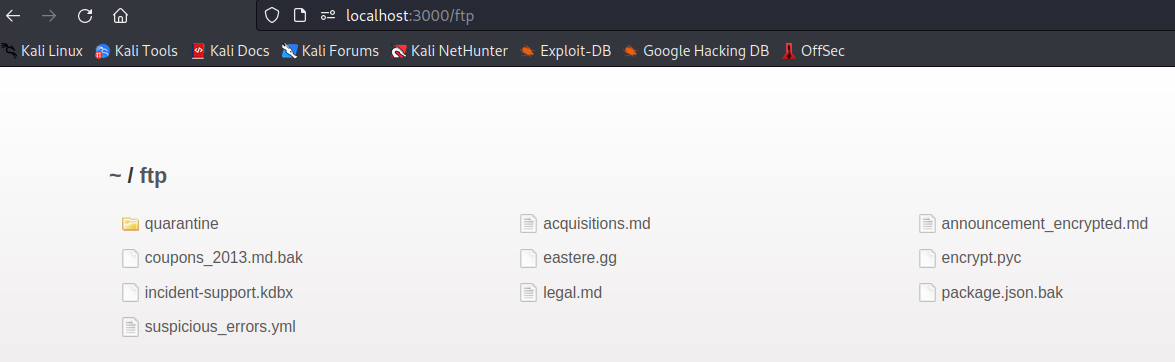
Po drodze przypadkowo udało nam się rozwiązać inne wyzwanie dotyczące przeczytania polityki prywatności:



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



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



Postanowiliśmy 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.

