## API-only XSS oraz Forged Review

Zadanie polega na wykonaniu ataku XSS, lecz w tym przypadku konieczne będzie wykorzystanie wystawionego przez aplikację API. Głównym celem wyzwania jest wykazanie, że aplikacja nieodpowiednio waliduje, oczyszcza lub chroni dane wejściowe otrzymane z zapytań API, co umożliwia wstrzyknięcie i wykonanie kodu JavaScript w aplikacji OWASP Juice Shop. By zrealizować zadanie należy wyświetlić odpowiedni alert, którego treść potwierdza wykonanie ataku XSS.

Pierwszym krokiem w celu odnalezienia API, które mogłoby posłużyć jako cel ataku, było skorzystanie z wbudowanej w przeglądarkę sposobności podglądu kodu pliku main.js, w którym wyszukana została fraza „api”.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

Wyświetlonych zostało kilka różnych API – na przykład: powiązane z użytkownikami oraz produktami z menu. Z uwagi na fakt, iż produkty dostępne są z poziomu bazowej strony, wykorzystane zostało ów API.

W celu zainicjowania połączenia z API skierowanym do obsługi produktów zamieszczony został testowy wpis, a następnie ciąg wydarzeń został wyszukany w aplikacji BurpSuite pozwalającej na prześledzenie poszczególnych zapytań kierowanych do aplikacji webowej.

Obraz zawierający tekst, zrzut ekranu, Oprogramowanie multimedialne, oprogramowanie

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Ikona komputerowa

Opis wygenerowany automatycznie

Odnalezione zostało zapytanie kierowane bezpośrednio do API

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Ikona komputerowa

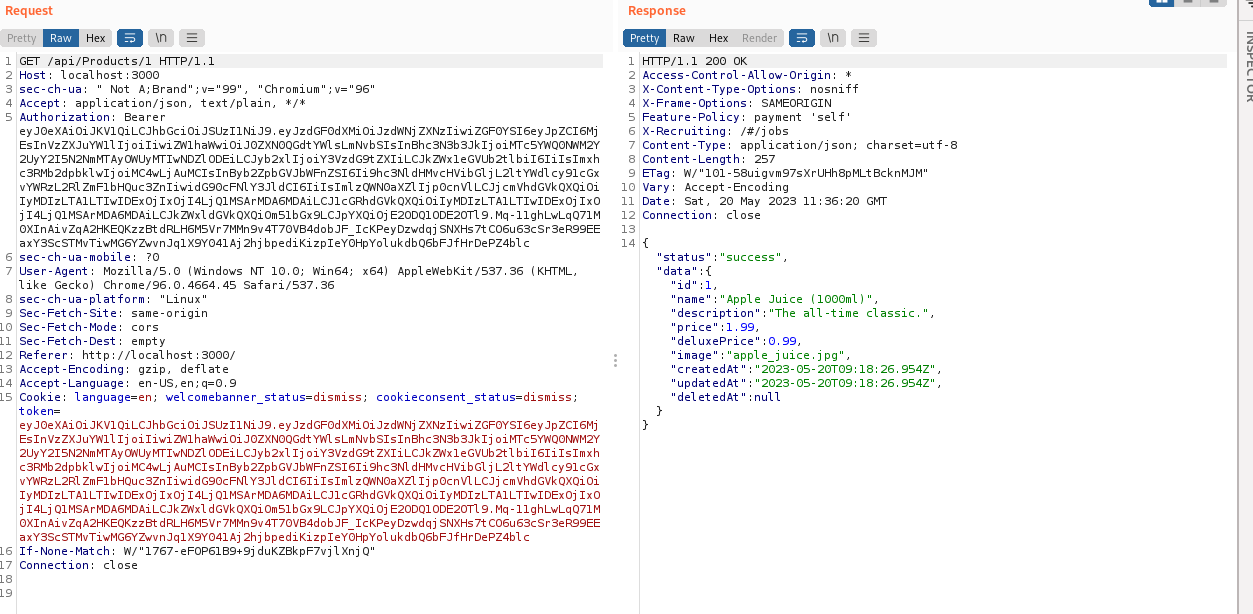
Opis wygenerowany automatycznie

Następnie zmieniona została treść zapytania, tak by odwoływało się ono do API powiązanego z produktami dostępnymi z poziomu głównego menu. Metoda GET doprowadziła do wyświetlenia informacji powiązanych ze wszystkimi rodzajami soków.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Ikona komputerowa

Opis wygenerowany automatycznie

Kolejnym krokiem było odfiltrowanie jednego soku, na którym skupiona zostanie uwaga w dalszych krokach przeprowadzanego ataku. W tym przypadku będzie to sok jabłkowy.

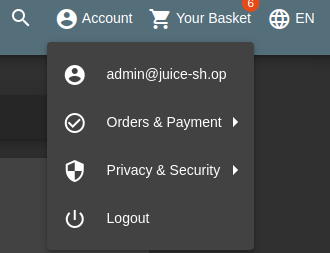


Skupiając swoją uwagę już wyłącznie na soku jabłkowym, wykonano próbę przesłania metody PUT z przekazywanymi atrybutami soku, mając nadzieję, iż dojdzie do zmiany wartości. Próba ta została jednak odrzucona, a zmiana nie została wprowadzona w obrębie aplikacji.

Obraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie

Opis wygenerowany automatycznie

Pierwszym podejrzeniem odnoszącym się do powodu braku powodzenia było powiązanie konkretnych ograniczeń uprawnień, które może posiadać w obrębie swojego konta przecięty użytkownik portalu. Wykonana została zatem próba zalogowania się jako użytkownik administracyjny, przy wykorzystaniu metody opisywanej w jednym ze wcześniejszych rozdziałów – było to bowiem również dostępne wyzwanie.



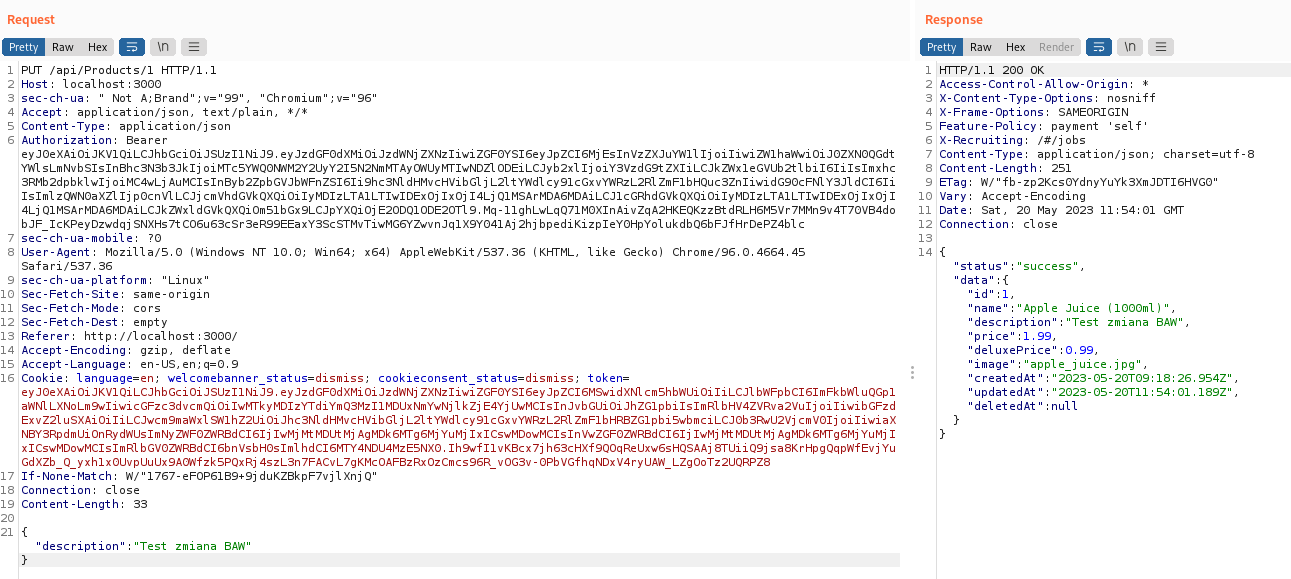
Po poprawnym zalogowaniu się na konto administratora, możliwe było wykonanie dowolnej akcji (tutaj wykorzystana, przeprowadzona akcja logowania się na portal) w celu pozyskania tokenu odpowiadającego za powiązane danej sesji z konkretnym użytkownikiem.

Obraz zawierający tekst, Czcionka, linia, zrzut ekranu

Opis wygenerowany automatycznie

Wspomniany token przekazany został jako podmieniona wartość jednego z atrybutów metody PUT, dzięki czemu wysyłane żądanie było obarczone powiązaniem z administratorem, który przeważnie posiada znacząco wyższe uprawnienia względem standardowego użytkownika.

Ponownie zmieniona została wartość parametru description odpowiedzialnego za opis pozycji z menu. Tym razem jednak akcja zakończyła się powodzeniem, a tym samym zmianą treści opisu na głównej stronie Juice Shop.



Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznie

Powyższe grafiki potwierdzają wprowadzoną w obrębie produktu zmianę. Czynność ta zobrazowała, że przytaczane pole tekstowe wchodzi w pełną interakcję z użytkownikiem. Ponadto wykonanie opisywanych akcji przyniosło skutek w postaci uznania przez systemem wyzwania towarzyszącego, którego celem było dokonanie zmiany w obrębie recenzji produktu z konta innego użytkownika, niż to które utworzył użytkownik. Tutaj nie doszło stricte do zmiany treści recenzji, lecz opisu produktu, natomiast – co wynika z przebiegu eksperymentu – to również pozwalało na uznanie wyzwania.

Pozostałą czynnością do wykonania poprawnego ataku XSS realizowanego przy wykorzystaniu API Juice Shop było dokonanie zmiany w obrębie wykorzystywanego pola tekstowego, oraz zaimplementowanie przykładowego kodu XSS (tutaj: wyświetla on komunikat o błędzie o treści „XSS”).

Obraz zawierający tekst, Czcionka, numer, zrzut ekranu

Opis wygenerowany automatycznie

Metoda PUT została zaakceptowana przez API, a zmiana wprowadzona w obrębie aplikacji webowej. W celu weryfikacji poprawności przeprowadzonej akcji udano się na główną stronę Juice Shop, wybrano z dostępnych pozycji sok jabłkowy, któremu poświęcane były wszystkie akcje. Wszystkie te kroki poskutkowały uznaniem wyzwania oraz wyświetleniem komunikatu o błędzie, którego treść odpowiadała wcześniej wprowadzonej w obrębie BurpSuite wartości: „XSS”.

