# Change Bender's password

W opisie zadania podane zostało, że hasło ma zostać zmienione na slurm4cl4ssic. Miało ono zostać zmienione użytkownikowi Bender, do którego konta udało się już dostać w jednym z wcześniejszych zadań.

W tym challengu nie można używać funkcji ‘Forgot password’, dlatego wykorzystano konto innego niż w zadaniu użytkownika w celu sprawdzenia dostępnych opcji.

Po zalogowaniu się na jedno z kont, w zakładce „Privacy and Security” dostępne było pole ‘Change password’. Pasowało więc ono do celu zadania.

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatyczniePo wpisaniu danych w wymagane pola ‘Current password’, ‘New password’ oraz ‘Repeat new password’, w narzędziach developerskich można było znaleźć żądanie GET, które zostało wygenerowane.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Czcionka

Opis wygenerowany automatycznie

http://localhost:3000/rest/user/change-password?current=asdf&new=12345h&repeat=12345h

Po próbach manipulacji tym linkiem, po usunięciu części z ‘current’ udało się zmienić hasło – i to bez podawania obecnego. Do wysyłania requestów trzeba było wkleić w pole Athorization token Bearer, który wysyłany jest przez serwer po zalogowaniu.

http://localhost:3000/rest/user/change-password?new=12345h&repeat=12345h

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

Skoro wiadomo już, że ta metoda zmiany hasła działa, należy teraz zalogować się na konto Bender’a, w celu uzyskania jego Bearer tokena w celu zmiany hasła na jego koncie. Ponieważ nie jest znane nam jego aktualne hasło, skorzystamy z metody wykorzystanej w poprzednich zadaniach.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

Po poprawnym zalogwaniu się z użyciem tej metody skopowiany został token.

Obraz zawierający tekst, zrzut ekranu, numer, Czcionka

Opis wygenerowany automatycznie

Udało się w ten sposób zmienić hasło i zadanie zostało zaliczone.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

# Leaked Access Logs

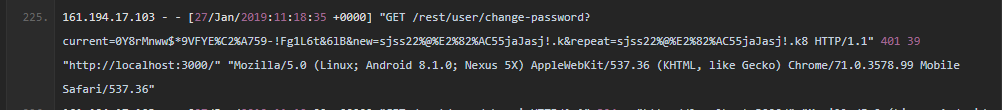
Następne zadanie opisane jest jako przeszukiwanie internetu w celu znalezienia zleakowanego hasła, a następnie zalogowanie się z jego pomocą do konta użytkownika, do którego należy.

Przeszukiwanie internetu doprowadziło do portalu stackoverflow i profilu Bjorna Kimminich’a, pierwotnego twórcy Juice Shopa. Znalezione zostało tam zadane przez niego pytanie dotyczące access logs, które pasowało do struktury znanej już z poprzednich zadań.

Obraz zawierający tekst, zrzut ekranu, Czcionka, Strona internetowa

Opis wygenerowany automatycznie

Przeglądając logi wklejone do pastebin, znalezione zostało hasło, o którym mowa w zadaniu:



**current**=0Y8rMnww$\*9VFYE%C2%A759-!Fg1L6t&6lB&**new**=sjss22%@%E2%82%AC55jaJasj!.k&**repeat**=sjss22%@%E2%82%AC55jaJasj!.k8

Widoczne jest, że w odpowiedzi zwrócony został błąd http 401 Unauthorized, co skłoniło do przyjrzenia się hasło podanym w new oraz repeat. Hasła te różnią się – w jednym na końcu jest znak ‘&’, a w drugim ‘8’.

Obraz zawierający tekst, oprogramowanie, zrzut ekranu

Opis wygenerowany automatycznie

Może oznaczać to, że hasło pozostało niezmienione, więc takie jak podane w ‘current’.

0Y8rMnww$\*9VFYE%C2%A759-!Fg1L6t&6lB

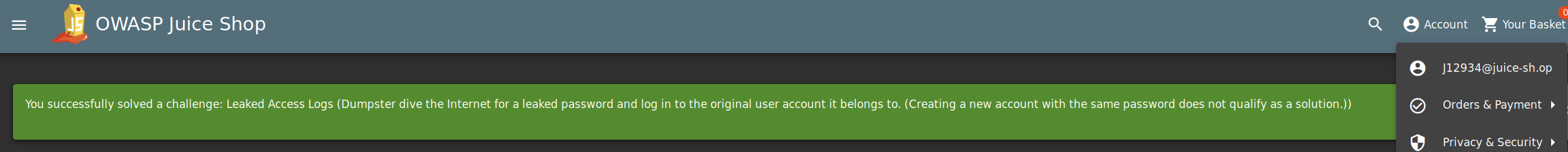
Ponieważ hasło to pochodzi z URLa musi zostać poddane operacji URL decode – wynikiem tego jest otrzymane hasło 0Y8rMnww$\*9VFYE§59-!Fg1L6t&6lB

Z pomocą znalezienia nazwy użytkownika przyszedł wcześniej odszukany panel administratora z rejestrem wszystkich użytkowników.

Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznie

Prawidłową nazwą użytkownika powiązaną z otrzymanym hasłem okazał się [J12934@juice-sh.op](mailto:J12934@juice-sh.op)



# Extra Language

Kolejnym challengem było odnalezienie języka, który nigdy nie znalazł się w systemie produkcyjnym.

W prawym górnym rogu aplikacji możliwa jest zmiana jej języka.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

Podczas zmiany języków w narzędziach developerskich można zauważyć, w jaki sposób nazywane są pliku zawierające poszczególne języki:

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Ikona komputerowa

Opis wygenerowany automatycznie

Podczas przeszukiwania internetu w celu znalezienia informacji o językach wspieranych przez Juice Shop oraz tego, w jaki sposób te tłumaczenia są wykonywane znaleziona została strona <https://crowdin.com/project/owasp-juice-shop>. Porównując języki znajdujące się w bazie na powyższej stronie odnaleziony został język Klingon, którego nie ma w aplikacji Juice Shop. Jest to wymyślony język, lecz na Wikipedii jest podany kod tego języka:

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Opis wygenerowany automatycznie

Znany więc jest już pierwszy człon nazwy pliku, potrzebny jest jeszcze drugi – pisany wielkimi literami dwuznakowy kod. W celu odnalezienia pliku na stronie napisany został skrypt przeprowadzający atak brute force, który próbuje na stronie różne rodzaje nazw pliku w formacie tlh\_XX.json.

Z wykorzystaniem tego skryptu (find\_language.py w repozytorium) udało się znaleźć plik, o który chodziło i zadanie zostało ukończone.

Obraz zawierający tekst, Czcionka, zrzut ekranu, Grafika

Opis wygenerowany automatycznie

W celu użycia skryptu należy go pobrać, a następnie uruchomić w odpowiednim miejscu (tam, gdzie jest pobrany) komendą:

*python find\_language.py*