BSK Zadanie zaliczeniowe - aplikacje webowe 19 listopada 2023

Rozwiązanie:

Autor: Zuzanna Ortenburger

1. FLAG{JeszczeJednaFlagaZaPunkty}
   Znaleziona podatność: Directory Traversal
   Sposób rozwiązania: Znalazłam, że funkcja render_card renderujaca kartkę wczytując motyw kartki wkleja nazwe pliku jako string. Dzięki temu można dostać się do każdego pliku znajdującego sie na serwerze. W tym do pliku flag.txt, który z skrypcie start.sh zostaje umieszczony w katalogu domowym
   Skrypt użyty do rozwiązania dostępny w pliku flag1.js

2. FLAG{ToJestFlagaZeStopki}
   Znaleziona podatność: JWT + XSS + CSRF
   Sposób rozwiązania: Druga flaga była umieszczona w stopce admina co odczytałam z pliku fixture udostepnionym jako plik źródłowy. Aby uzyskać tę flagę musiałam wysłać maila do admina który zmusi go do odesłania maila mi. Aby tego dokonać wysłałam adminowi maila z treścią jako java scriptem, który na początku wstrzykuje na strone iframe z adresem strony do tworzenia kartki, a nastepnie wypełnia wszystkie pola i klika wyślij. Musiałam też dodać czas na załadowanie się iframe.
   Skrypt użyty do rozwiązania dostępny w pliku flag2.js

3. FLAG{71a4b4fd2214b808e4942dfb06c717878399a04c}
   Znaleziona podatność: Directory Traversal + Server Side Request Forgery
   Sposób rozwiązania: Trzecia flaga znajdowała się w supersecret-microservice co odczytałam z pliku docker-compose, udostępniosego jako źródłowy. Podobnie jak w przypadku pierwszej flagi dzięki wklejeniu do template kartki ścieżki do pliku, odczytałam zawartość pliku \etc\hosts w którym możemy odczytać konfiguracje sieci. Dowiedziałam się, że jest tam adres 172.20.0.4 co świadczy o istnieniu dockerowej sieci o adresie 172.20.0.0\16. Nastepnie przeszukiwałam kolejne adresy z tej sieci. Dodatkowo znalazłam, że w przeciwności do GreetingCardDetailForPNGView funkcja GreetingCardDownloadPNGView wykonuje po stronie serwera odczytanie zawartości treści. Dlatego jako treść maila wstawiłam htmla z iframem wyświetlającym kolejne adresy z sieci dockerowej i przechodzilam do widoku download-png. Po paru próbach odkryłam że właściwym adresem jest 172.20.0.3 i tam znalazlam flage. Musiałam też poszerzyć iframe, bo cala flaga się nie pokazywała.
   Skrypt użyty do rozwiązania dostępny w pliku flag3.js

   W przypadku wszystkich tych 3 flag używałam skryptów w node js z fetchem, aby móc wysłać wiadomość która nie jest textem w tagach $< p >< /p >$