BSK aplikacje webowe

Bartosz Kucypera, bk439964

12 listopada 2023

FLAGA z footera

Czytając kod aplikacji (start.sh i fixture) wiemy, że istnieje użytkownik admin który w treści footera ma flage.

Z folderu xss-bot wiemy też, że ten użytkownik otwiera wszystkie kartki jakie do niego przychodzą.

Treść footera, którą podajemy przy zakładaniu konta, jest wklejana bez żadnej serializacji do każdej kartki którą wysyłamy, więc możemy załadować tam złośliwy skrypt. (nie czytałem jakoś dogłębnie kodu aplikacji by się o tym przekonać, po prostu wkleiłem pierwszy lepszy skrypt na testa i sprawdziłem czy zadziała)

Piszemy, więc skrypt który wysyła żądanie POST z przesłaniem kartki do nas samych, wklejamy go do treści footera przy zakładaniu konta i wysyłamy kartkę do użytkownika admin.

Bot ją otwiera, uruchamia nasz skrypt i wysyłą nam spowrotem kartke i prawie uzyskujemy flagę.

Prawie, bo kopiując fetcha naszego żądania POST jest tam nasze ciasteczko csrf a nie admina. Musimy, więc jeszcze podkraść jego ciasteczko, które można znaleźć pod document.cookie.

Z tym fixem już uzyskujemy flagę FLAG{ToJestFlagaZeStopki}.

Fetch użyty w footerze znajduje się w pliku footer.js, ”przerabiator” js na tag htmlowy w pliku make_js.py.

FLAGA z pliku flag.txt

Podczas czytania kodu zauważamy, że skypt start.sh echo-uje flagę do pliku /flag.txt.

Długo nie mogłem znaleźć sposobu by ją zdobyć, ale podczas dogłębniejszczego czytania kodu aplikacji zwróciłem uwagę na to jak generowana jest kartka i co dzieje się w funkcji render_card w pliku utils.py.

Czytana jest tam templatka kartki wybrana przez użytkownika (normal/coffee).

Przynajmniej w tym miejscu, nie ma żadnej walidacji tego czy pod card.template jest normal/coffee czy nazwa jakiegoś innego pliku, albo całej ścieżki.

Możemy, więc wysłać żądnie POST stwożenia i wysłania kartki do nas samych i za template podać ścieżkę do flagi.

Jeśli nigdzie indziej nie ma walidacji poprawności argumentu template to dostaniemy flagę.

Faktycznie, metoda zadziałała, flaga to FLAG{JeszczeJednaFlagaZaPunkty}.

Fetch ze spreparowanym żądaniem POST zajduje się w pliku fake_template.js.

FLAGA ostatnia