# Sweet and Sour

A screenshot of a computer

AI-generated content may be incorrect.

საიტზე გადასვლისას გვაქვს შემდეგი ტიპის გამოსახულება. Inspect-ში არაფერია.

Storage, Cookie სექციაში გვაქვს რაღაც სესია:

A blue and white rectangle with white text

AI-generated content may be incorrect.

gANYCwAAAFRyeSBIYXJkZXIhcQAu - შესაძლოა base64 იყოს. ვცადოთ და დეკოდირება მოვახდინოთ:

A screenshot of a computer

AI-generated content may be incorrect.

ბარპში დეკოდირების შემდეგ, ვხედავთ, რომ try harder-გამოაქვს. თუ ჩავიხედებით, ვნახავთ, რომ back არის დაწერილი python-ზე:

A screenshot of a computer error

AI-generated content may be incorrect.

პითონში არსებობს pickle ბიბლიოთეკა, რომელიც ობიექტების სერიალიზაციისა და დესერიალიზაციისათვის გამოიყენება. მოცემული ბიბლიოთეკა მოწყვლადია და არ უნდა გამოვიყენოთ არასანდო ობიექტებზე.

პიკლს გააჩნია მოწყვლადი სკრიპტი:

A computer screen shot of text

AI-generated content may be incorrect.

რომლის წყალობითაც შესაძლოა შეტევა განვახორციელოთ...

გავამახვილოთ ყურადღება \_\_reduce\_\_ მეთოდზე. ის პიკლ ბიბლიოთეკას ამცნობს თუ როგორ გადატვირთოს ობიექტი (როგორ მოახდინოს ობიექტის რეკონსტრუქცია)

მოცემული მეთოდი, როგორც წესი, აბრუნებს tuple-ს.

Eval მეთოდი შეეცდება წაიკითხოს flag ფაილი...

SendPayload-ში ვიღებთ სერიალიზირებულ მონაცემს (p) ვშიფრავთ base64-ში და ვაგზავნით როგორც cookie-ს (data) მოცემულ ენდპოინტზე.

გავუშვათ ჩვენი სკრიპტი და ვნახოთ რა იქნება შედეგი:



A close up of a computer screen

AI-generated content may be incorrect.