# Shark

A screenshot of a computer

AI-generated content may be incorrect.

მოცემულია საიტი, რომელიც შეიცავს მხოლოდ შესაყვან ველს, inspect ცარიელია.

ველში რასაც შევიყვანთ, ის გამოდის:

A screenshot of a computer

AI-generated content may be incorrect.

ჩავატაროთ ოპერაციები დავნახოთ SSTI ტიპის თავდასხმაზე მოწყვლადი ხომ არ არის...

SSTI (Server-Side Template Injection) არის თავდასხმის მექანიზმი, როდესაც თავდამსხმელი იტყენებს შაბლონებს (Template) რათა ველში არსებული სკრიპტის გამოყენებით შეაღწიოს სერვერზე. შაბლონები გამოიყენება ვებ აპლიკაციებში. მისი მეშვეონით ხერხდება პრეზენტაციის (HTML, CSS…) და აპლიკაციის ლოგიკის (PHP, Py …) განცალკევება.

არსებობს სხვადასხვა ტიპის შაბლონები.

Burp-ის გამოყენებით ვხედავთ, რომ ბექში პითონი გამოიყენება. დავსერჩოთ პითონში პოპულარული შაბლონები: Mako, Jinja2…

A screenshot of a computer

AI-generated content may be incorrect.

სხვადასხვა ენას თავისი შაბლონი შეიძლება გააჩნდეს. დავაბრუტვფორსოთ ჩვენს ლაბზე:

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

ვრწმუნდებით, რომ ლაბი მოწყვლადია SSTI თავდასხმაზე. გადავიდეთ ბარპში და ჩავატაროთ ოპერაციები:

A black rectangle with a white rectangle in the middle

AI-generated content may be incorrect.

Repeater-ში, name-ს მიეწოდება სტრიქონი, საჭიროა შაბლონების მეშვეობით შევაპაროთ პითონ სკრიპტი. Python shell exec სკრიპტი არის საჭირო, რათა ლინუქსის (ან ვინდოუსი... გააჩნია) ბრძანებეთან გვქონდეს წვდომა.

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen shot of a code

AI-generated content may be incorrect. A screen shot of a computer

AI-generated content may be incorrect.

A close-up of a computer code

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.

A computer screen shot of a computer code

AI-generated content may be incorrect.A black text on a white background

AI-generated content may be incorrect.

მეორე ხერხი:

