# Schematic

A screenshot of a computer

AI-generated content may be incorrect.

მოცემულ ლაბზე გადასვლისთანავე ჩვენ ვხედავთ login გვერდს. დავაბრუტფორსოთ admin password, admin admin…

Brute-force-მა არ იმუშავა, გავუშვათ dirsearch და ვნახოთ რა საქაღალდეები და ფაილები არის:

A screen shot of a computer

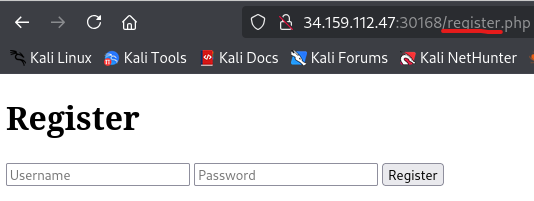
AI-generated content may be incorrect.

წავაწყდი ძალიან საინტერესო path-ს:

A screen shot of a computer screen

AI-generated content may be incorrect.

დავარეგისტრიროთ მომხმარებელი:



A screenshot of a computer

AI-generated content may be incorrect.

რეგისტრაციის შედეგად გადავდივართ ჩვენს პროფილზე, სადაც გვაქვს input ველი.

მოცემული ველი შესაძლოა მოწყვლადი იყოს sql თავდასხმებზე.

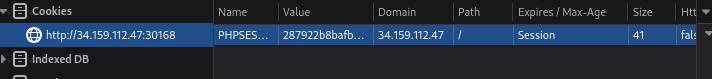
A screenshot of a computer

AI-generated content may be incorrect.

საეჭვო ველია, ამიტომ გამოვიყენებ sqlmap-ს, რათა დავაზუსტო მოწვლადია თუ არა sql თავდასხმაზე.

SQL-Injection თავდასხმის ტიპია, როდესაც თავდამსხმელს შეუძლია მოიპოვოს ინფორმაცია სხვადასხვა იუზერზე, განახორციელოს მონაცემთა ბაზებზე მანიპულაციები და ასე შემდეგ.

Inspect elements-ში ჩახედვისას, cookie სექციაში გვაქვს მომხმარებლის სესია:



კარგი იქნება თუ გამოვიყენებთ მას.



(--forms – გავპარსოთ ჩვენი ვებ გვერდის ველები, --dbs მონაცემთა ბაზების გამოტანა)

იმუშავა sqlmap-მა, ნამდვილად sql-injection არის:

A screen shot of a computer

AI-generated content may be incorrect.

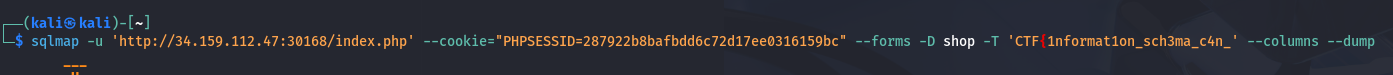
დავუყვეთ ბაზებს და მოვიძიოთ ინფორმაცია, დავიწყებ shop-ით, რადგან ჩვენი input ველს გამოაქვს პროდუქტების სია:



A black background with white text

AI-generated content may be incorrect.

როგორც ჩანს shop ბაზას ctf ფლეგი გააჩნია



A black background with white text

AI-generated content may be incorrect.

მივაგენით ფლეგს:

CTF{1nformat1on\_sch3ma\_c4n\_cont41n\_us3ful\_d4t4}