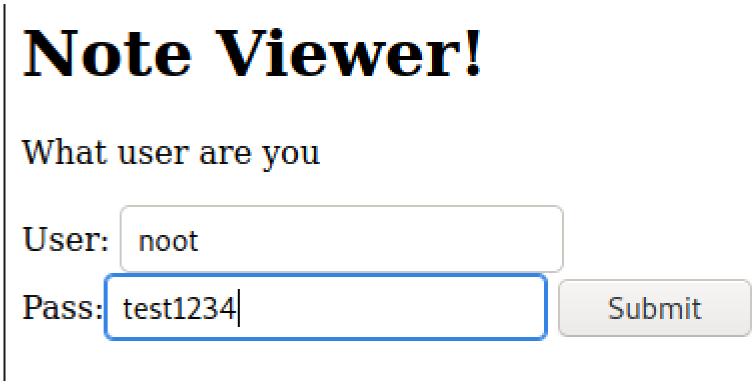
Mark Seliternikov

TryHackMe - OWASP Top 10 - [Severity 5] Broken Access Control [Easy]

Scenario: a website with broken authentication.
We are given a user to start with:



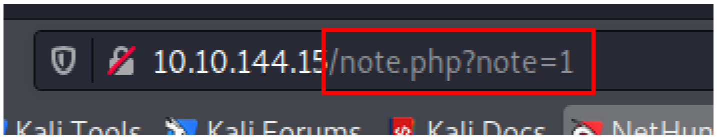
Note Viewer!

What user are you

User: noot

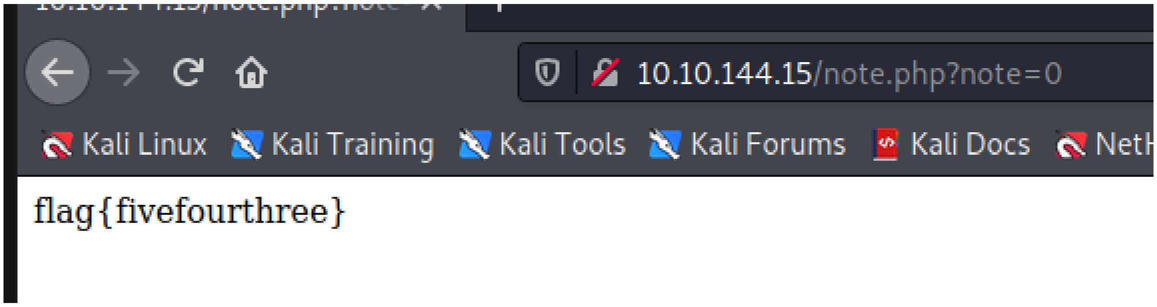
Pass: test1234

When logging in you can see something interesting in the URL.



10.10.144.15/note.php?note=1

When changing the parameter "note" to 0 you get to see this:



10.10.144.15/note.php?note=0

flag{fivefourthree}

There is no validation or checking to see if I'm authorized to access this page! The note belongs to a different ID and not noot's.