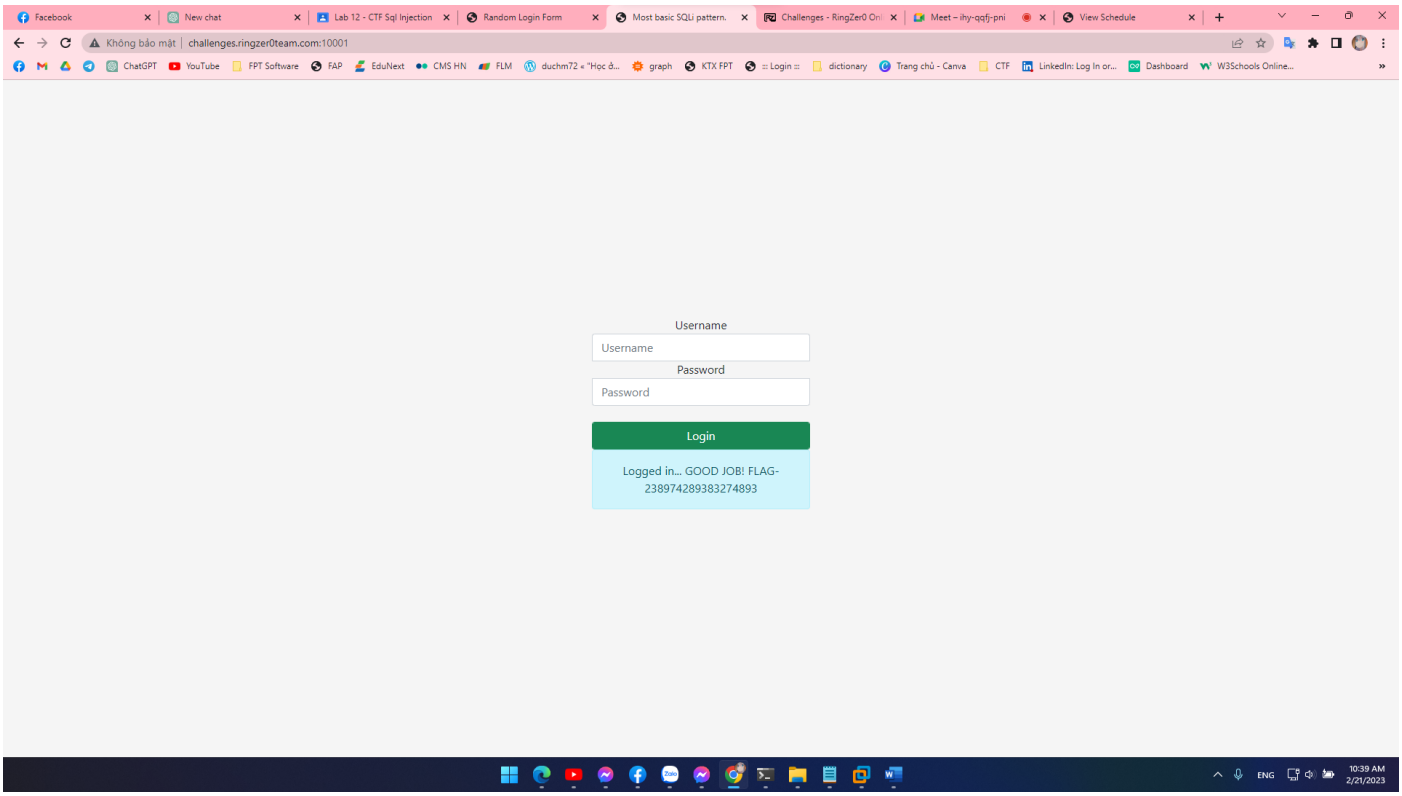
Lab 12 - CTF Sql Injection

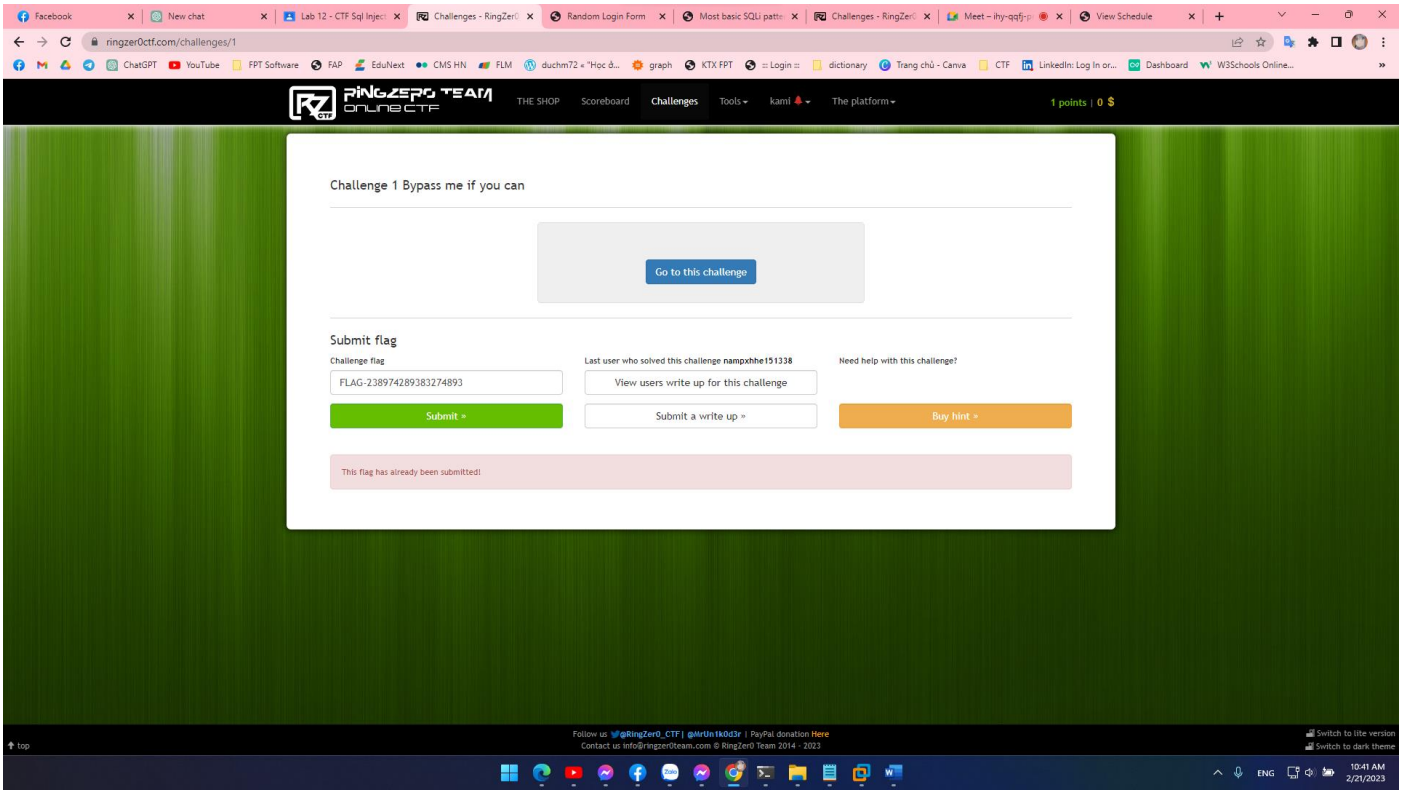
Most basic SQLi pattern

First we try to enter the basic command : 1' or 1=1 into the user,password then we get the result "You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' AND password = '1' or 1=1'' at line 1". From that we can guess that the query will look like: SELECT ..... FROM ..... Where username='$user' AND password='$password';

so we just need to comment(#) everything after 1=1 (always true) then we will get flag

1' or 1=1#

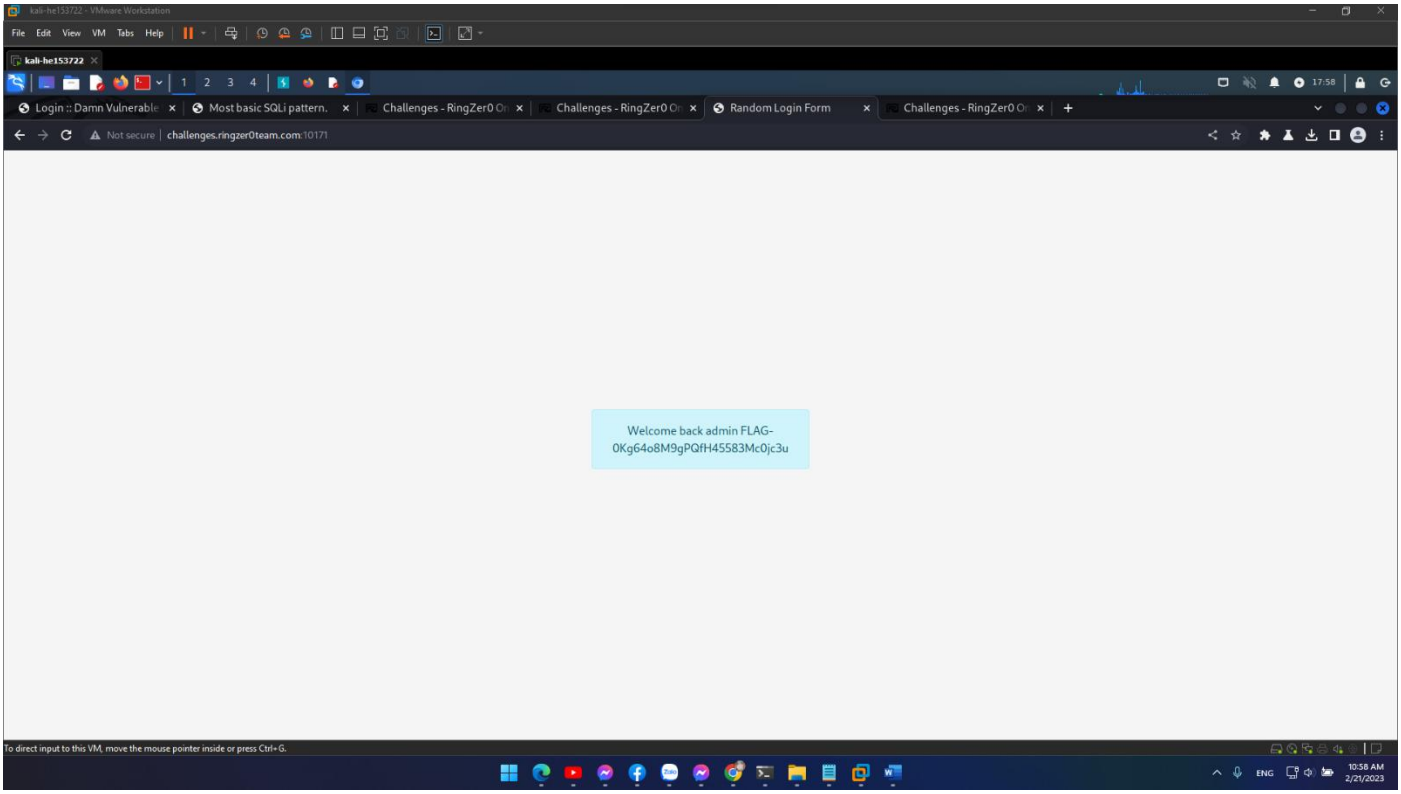


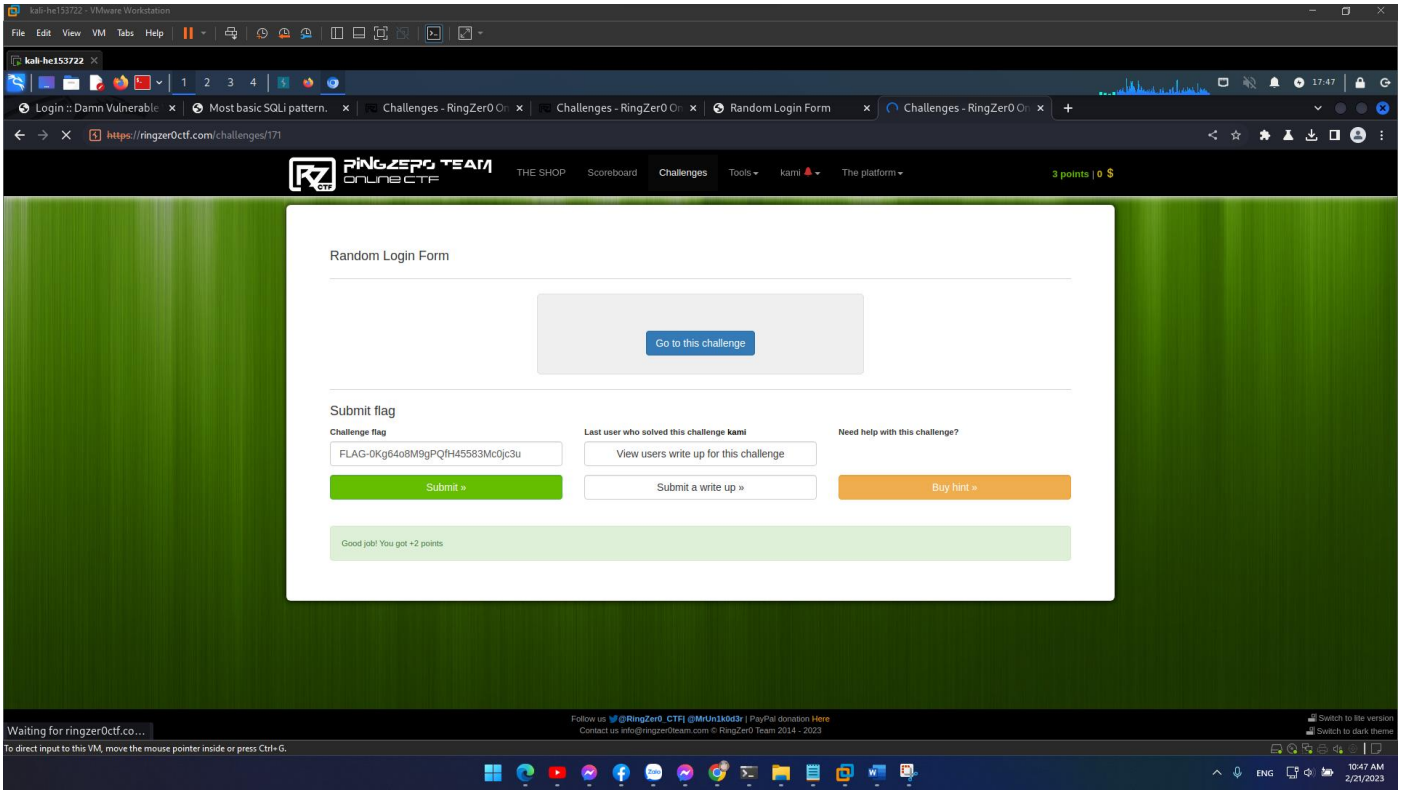


Random Login Form

First create any account, log in but receive the message "Welcome back a, Seems like your not an admin!".

then go back to register for an account with the user "admin" and receive the message "This account already exists.". After a few tries when adding a space before admin "admin" I still get the message "This account already exists." from that we can guess that the site removed the whitespace with "trim()". because "trim()" only removes spaces at the beginning, so we try to register for an "ad min" account, it was successful and we log in to that account, we will get a flag



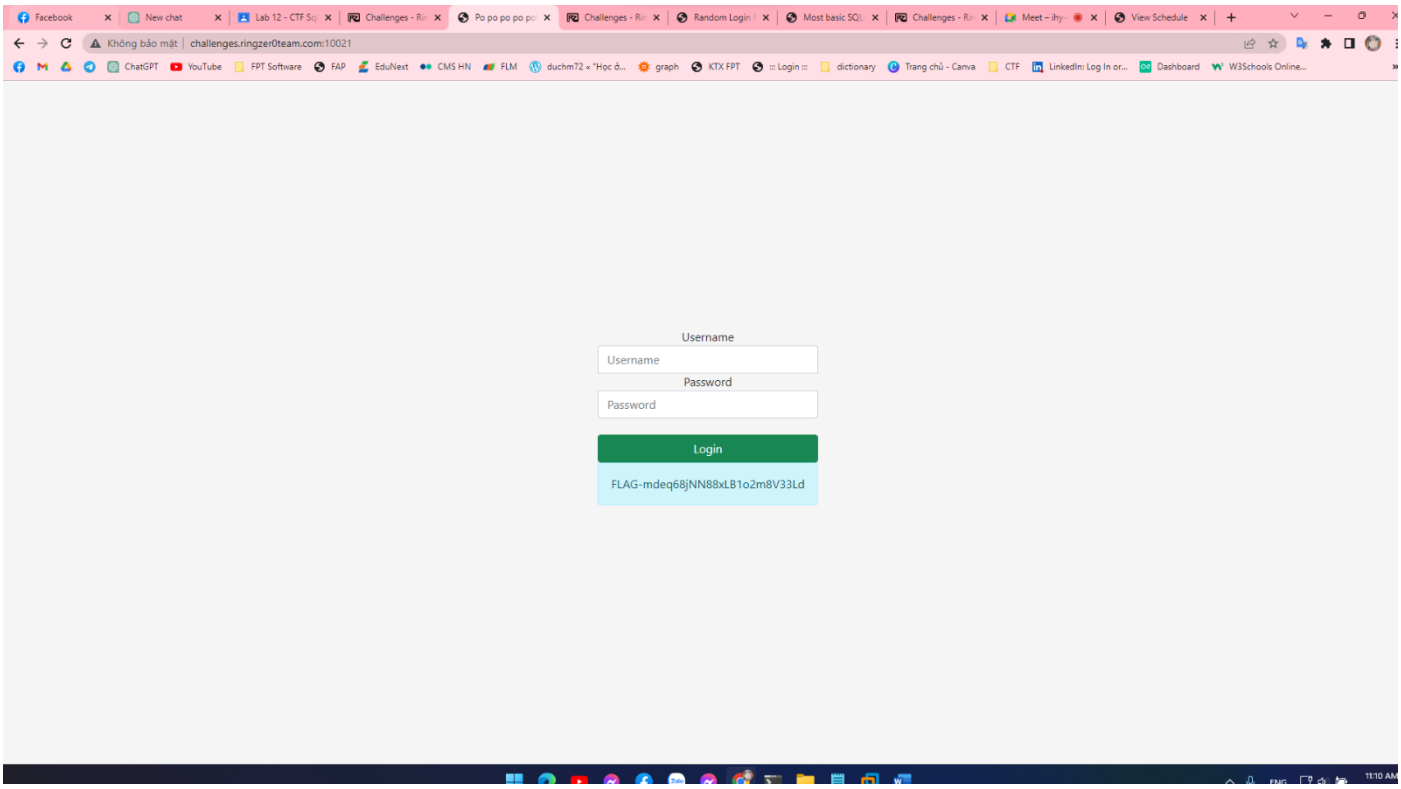


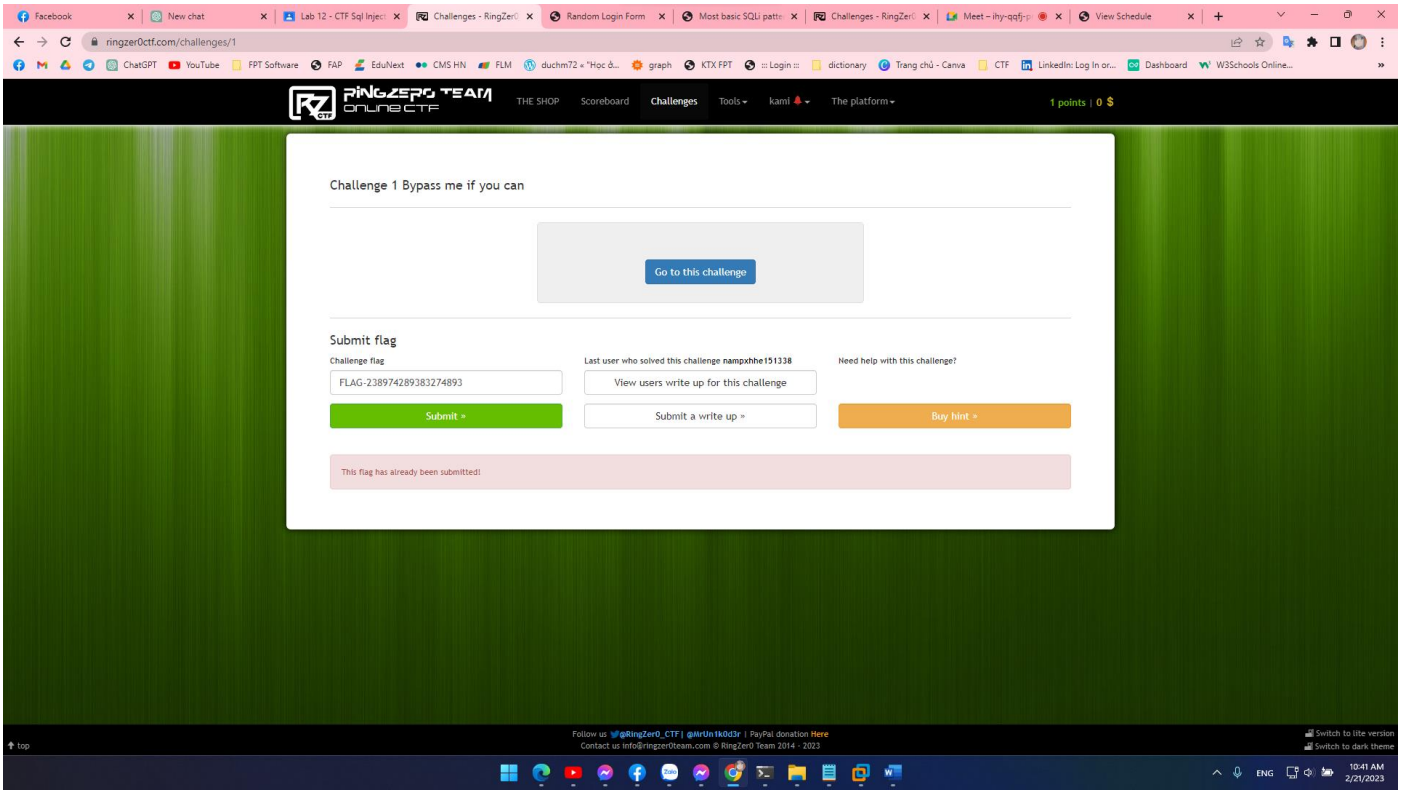
Po po po po postgresql

First we try to enter the basic command: 1' or 1=1 into the user, the password will get the result "Illegal characters detected." so we can guess the match "=" has been filtered out. then we try again with: 1' then we get the result: "ERROR: syntax error at or near "da39a3ee5e6b4b0d3255bfef95601890afd80709" LINE 1: ...M users WHERE (username = ('1'') AND password = ('da39a3ee5e... ^" from that we can guess that the query will look like: "SELECT ..... FROM ..... Where (username=('...') AND password=('.. ...'));"

so to get the result we need to always be true on the user part and omit the password because the "=" sign has been removed so we will replace to “true”: 1')) or true --

the query will be: SELECT ..... FROM ..... Where (username=('1')) or true --') AND password=('.....'));




Facebook
New chat
Lab 12 - CTF Sql Injec
Challenges - RingZer0
Random Login Form
Most basic SQLi patte
Challenges - RingZer0
Meet – ihy-qqfj-p
View Schedule
ringzer0ctf.com/challenges/1
ChatGPT
YouTube
FPT Software
FAP
EduNext
CMS HN
FLM
duchm72 « "Học đ...
graph
KTX FPT
:: Login ::
dictionary
Trang chủ - Canva
CTF
LinkedIn: Log In or...
Dashboard
W3Schools Online...
RingZero Team Online CTF
THE SHOP
Scoreboard
Challenges
Tools
kaml
The platform
1 points | 0 $
Challenge 1 Bypass me if you can
Go to this challenge
Submit flag
Challenge flag
FLAG-238974289383274893
Submit »
Last user who solved this challenge nampxhhe151338
View users write up for this challenge
Submit a write up »
Need help with this challenge?
Buy hint »
This flag has already been submitted!
top
Follow us @RingZer0_CTF | @MrUn1k0d3r | PayPal donation Here
Contact us info@ringzer0team.com © RingZer0 Team 2014 - 2023
Switch to lite version
Switch to dark theme
ENG
10:41 AM
2/21/2023