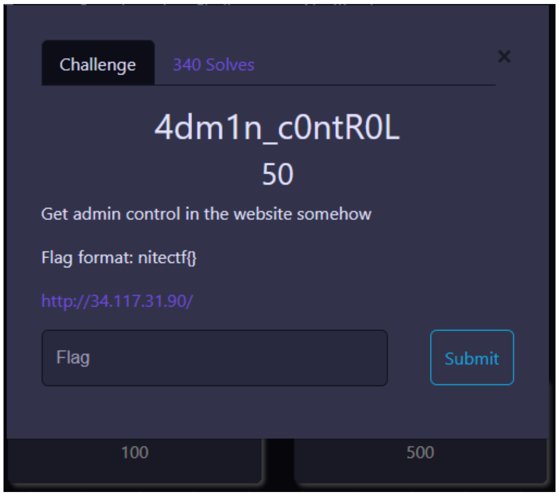
Nite CTF 2022

This one is the first Web challenge from Nite CTF 2022, and it’s pretty easy.



4dm1n_c0ntR0L

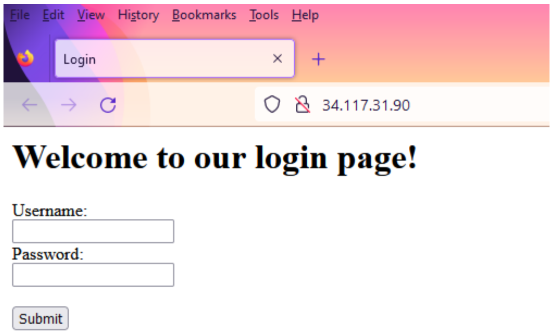
50

Get admin control in the website somehow

Flag format: nitectf{}

http://34.117.31.90/

We get a url, lets go check it out.



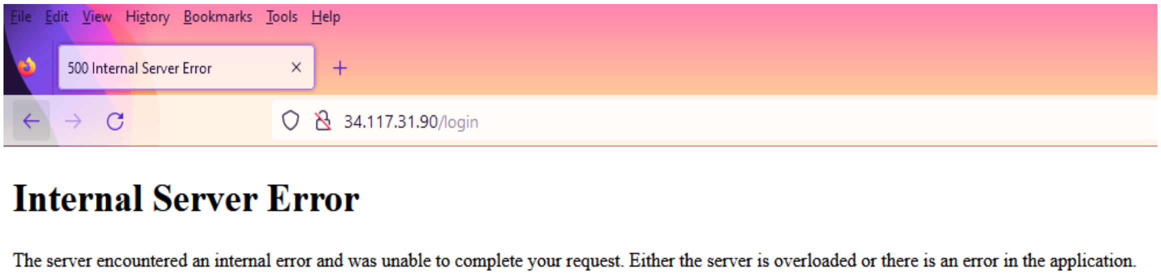
Welcome to our login page!

Username:

Password:

Very simple page, just a login form and a submit button to go off.

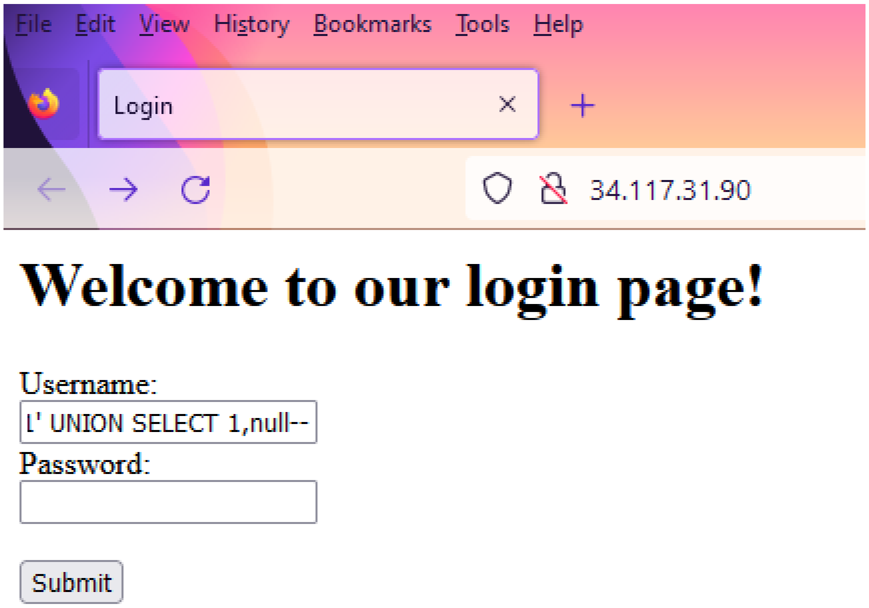
When I see a login form in a CTF I immediately try SQLi.


File Edit View History Bookmarks Tools Help
500 Internal Server Error
34.117.31.90/login

Internal Server Error

The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.

Trying out entries from hacktricks, we figure out that we can put in ‘) to get an internal service error. This confirms that something fishy is happening in the SQL here. Next, I think, what if we just give it another command in the input? Let’s try something like… 1’ UNION SELECT 1,null … but this doesn’t work, we just get another 500 Internal Service Error. I believe this is because when we think about the statements, the original statement looks something like “SELECT user, pass FROM table WHERE user LIKE $$$ … ” and is ended somewhere ahead by a semi-colon. However, we can just do an in-line comment to remove the last portion of the statement. Let’s try the same statement, but with an inline comment (--) appended.

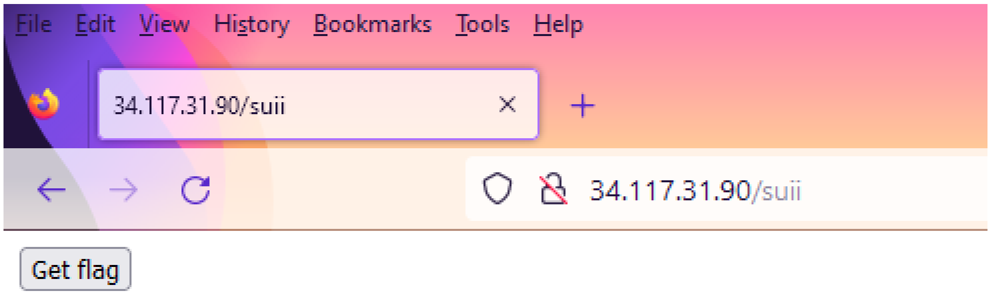


Welcome to our login page!

Username:

l' UNION SELECT 1,null--

Password:



Voila, we have flag.