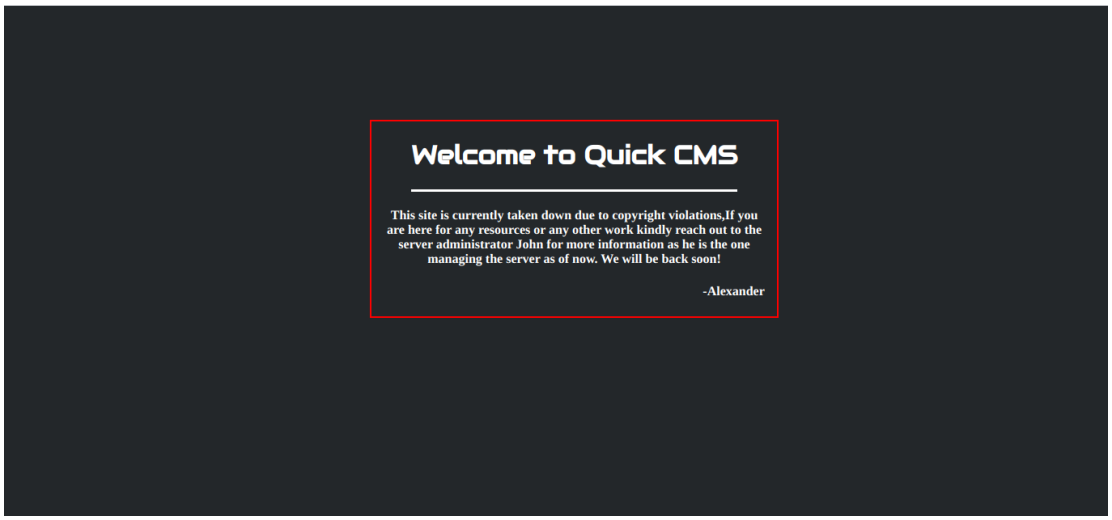
Quick CMS

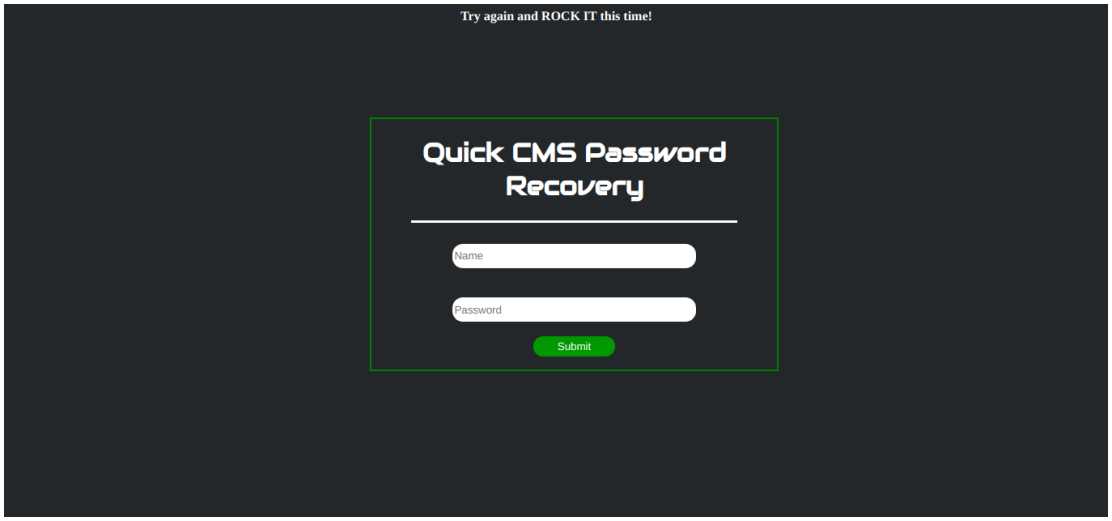
On opening the home page we see a notice that the site has been taken down and if we pay close attention on the content it says that the administrator's name is John



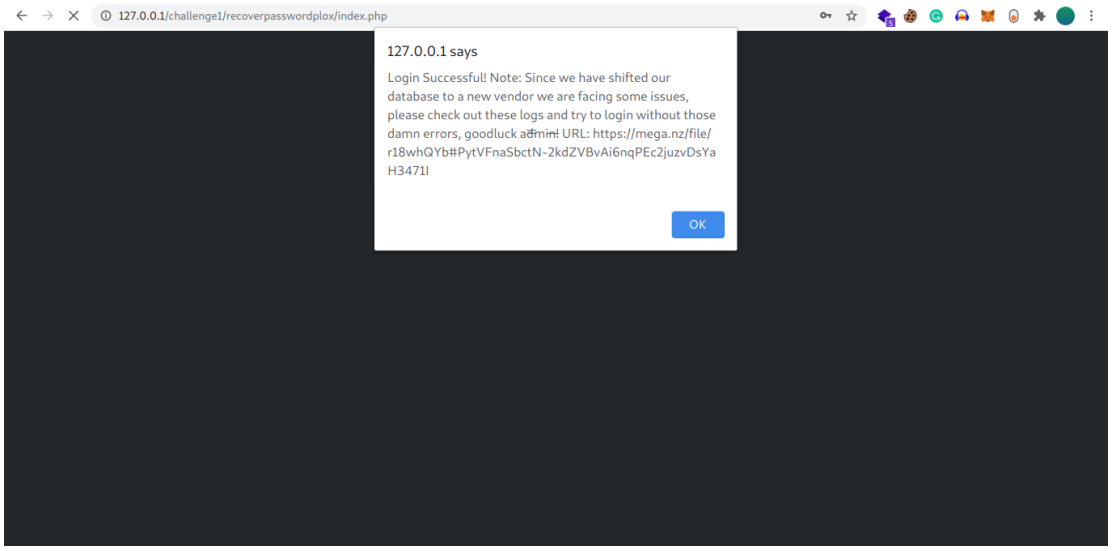
Upon doing some quick recon we discover the robots.txt file which actually contains the following line as a comment:

 # Have you tried checking out /recoverpasswordplox

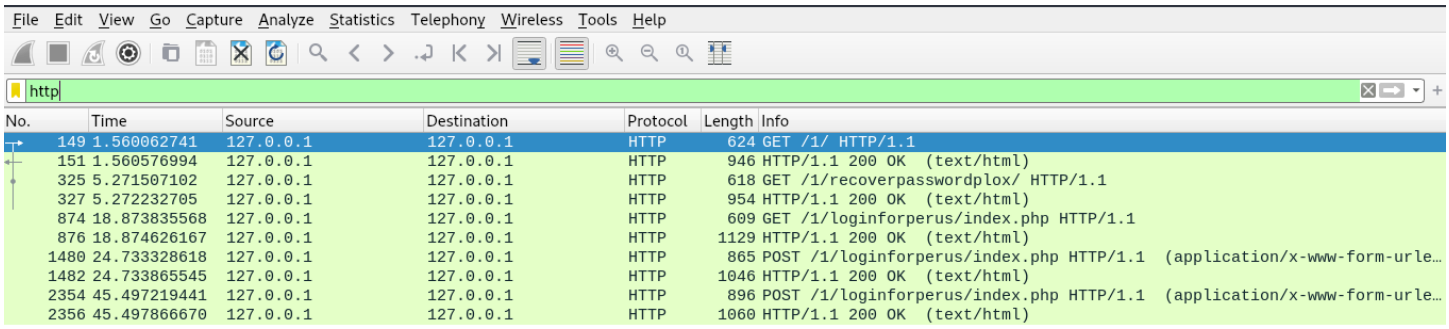
This is actually a directory which once opened will lead to a password recovery page which probably is for the admin to reset the password of other users.



If we check the top of the page, it is actually a hint for rockyou.txt file which lets us assume that we need to bruteforce this page with rockyou.txt . We know the username will be **John** which we discovered from the homepage and the password will be fuzzed with the rockyou.txt file . The password here will be **secret.**



Once we use the credentials we get a pop up with a mega.nz link. The link contains a pcap file which we will open in wireshark for now.



If we filter the http traffic we discover some traffic to a different directory which is **/loginforperus**

Once we filter the follow the HTTP stream we will find the unencrypted requests made to the login panel on that directory and will give us the credentials as well as the session id which we need to use for the login request.

Now we just need to replace the session cookie with **c242492cme2gd8n3j8kdptjpdq** , use **John** for username and **admin1234** for password then we will get our flag: **vulncon{session_ids_are_fun_right?}**