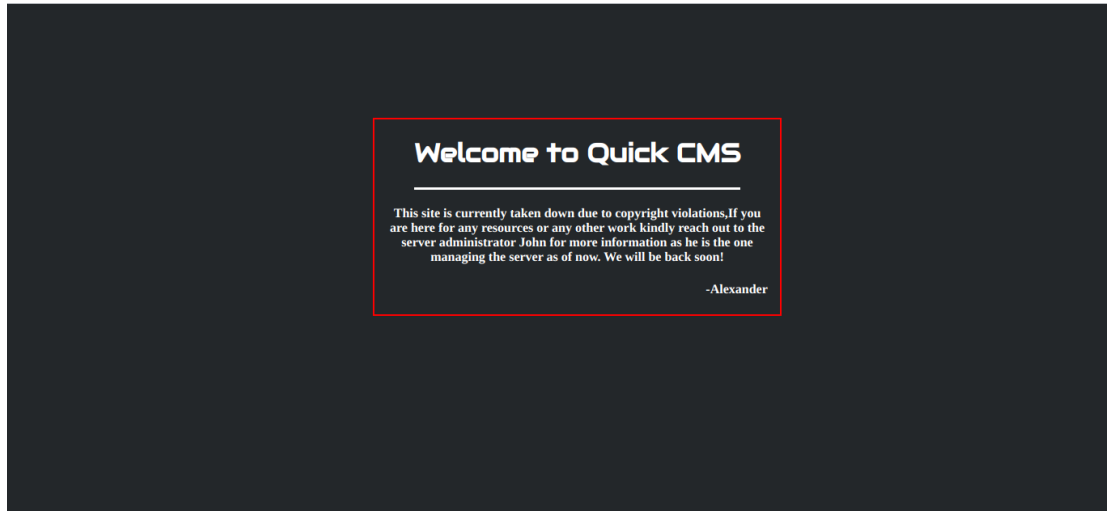


# Quick CMS

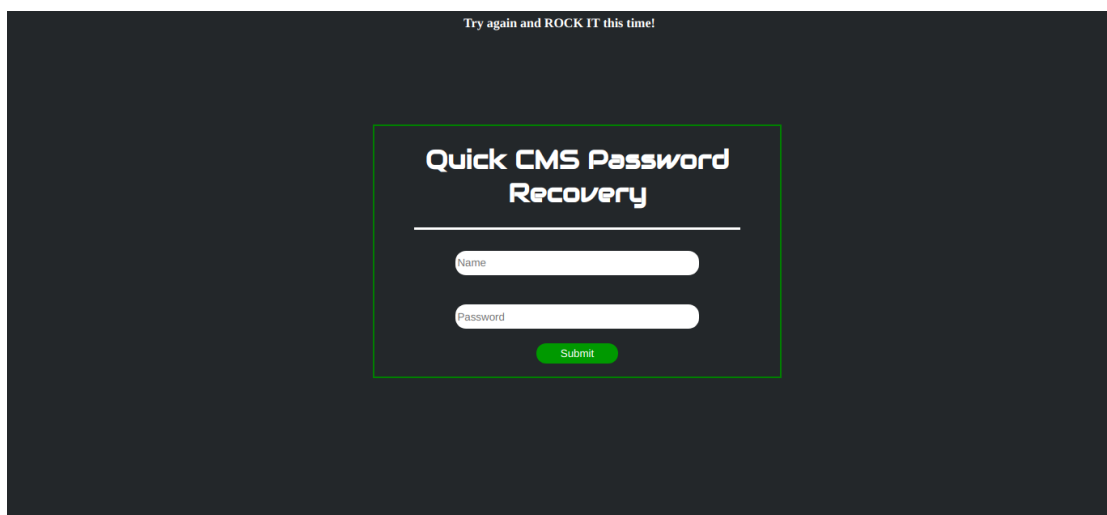
On opening the home page we see a notice that the site has been taken down and if we pay close attention on the content it says that the administrator's name is John



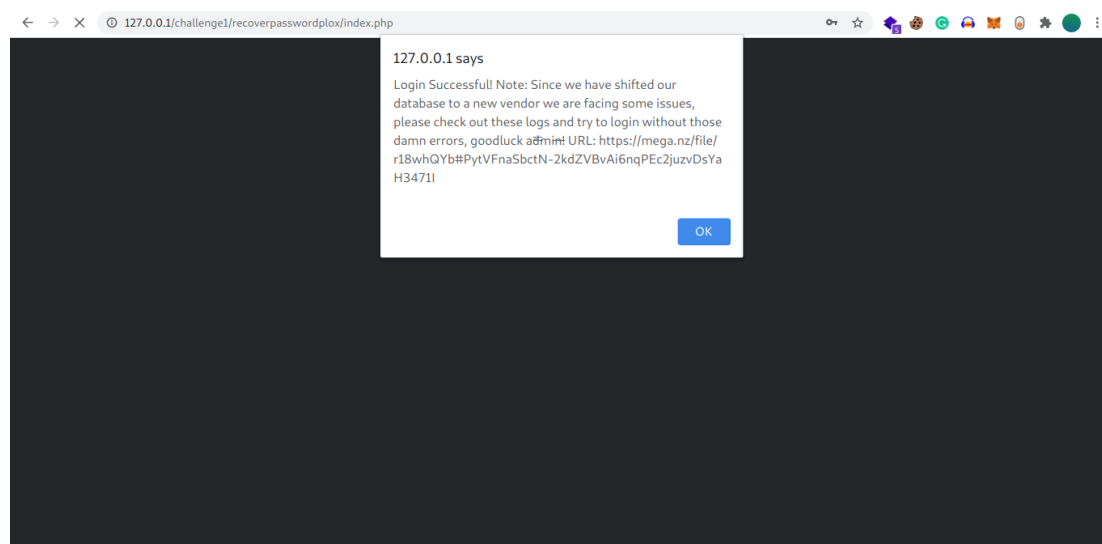
Upon doing some quick recon we discover the robots.txt file which actually contains the following line as a comment:

## # 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.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help							
http							
No.	Time	Source	Destination	Protocol	Length	Info	
149	1.560062741	127.0.0.1	127.0.0.1	HTTP	624	GET /1/ HTTP/1.1	
151	1.560576994	127.0.0.1	127.0.0.1	HTTP	946	HTTP/1.1 200 OK (text/html)	
325	5.271507102	127.0.0.1	127.0.0.1	HTTP	618	GET /1/recoverpasswordplo/ HTTP/1.1	
327	5.27232705	127.0.0.1	127.0.0.1	HTTP	954	HTTP/1.1 200 OK (text/html)	
874	18.873835568	127.0.0.1	127.0.0.1	HTTP	609	GET /1/loginforperus/index.php HTTP/1.1	
876	18.874626167	127.0.0.1	127.0.0.1	HTTP	1129	HTTP/1.1 200 OK (text/html)	
1480	24.733328618	127.0.0.1	127.0.0.1	HTTP	865	POST /1/loginforperus/index.php HTTP/1.1 (application/x-www-form-urle...	
1482	24.733865545	127.0.0.1	127.0.0.1	HTTP	1046	HTTP/1.1 200 OK (text/html)	
2354	45.497219441	127.0.0.1	127.0.0.1	HTTP	896	POST /1/loginforperus/index.php HTTP/1.1 (application/x-www-form-urle...	
2356	45.497866670	127.0.0.1	127.0.0.1	HTTP	1060	HTTP/1.1 200 OK (text/html)	

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?}**