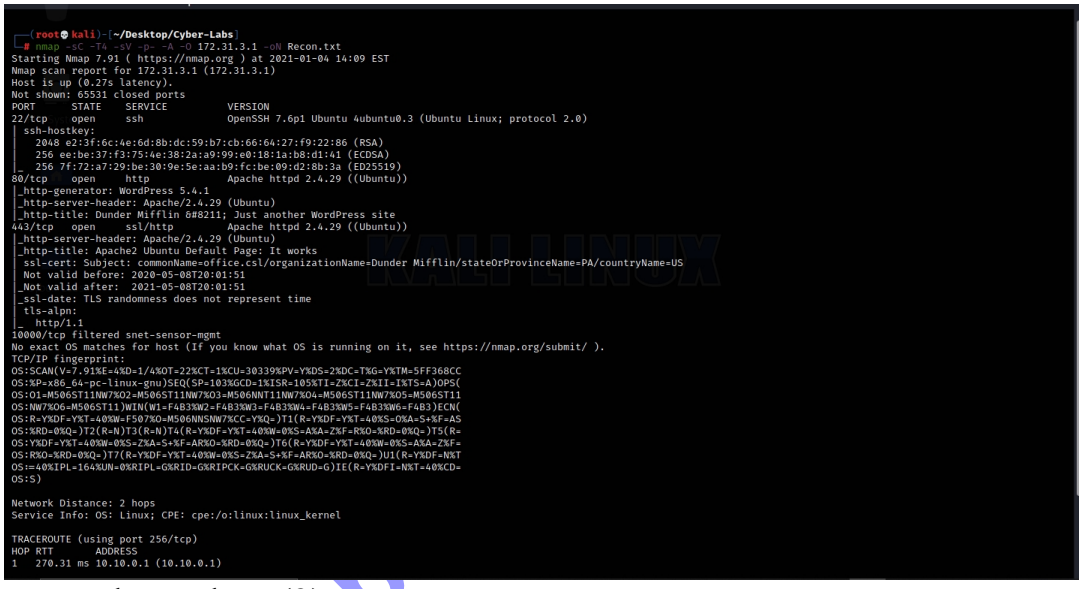
Office Lab

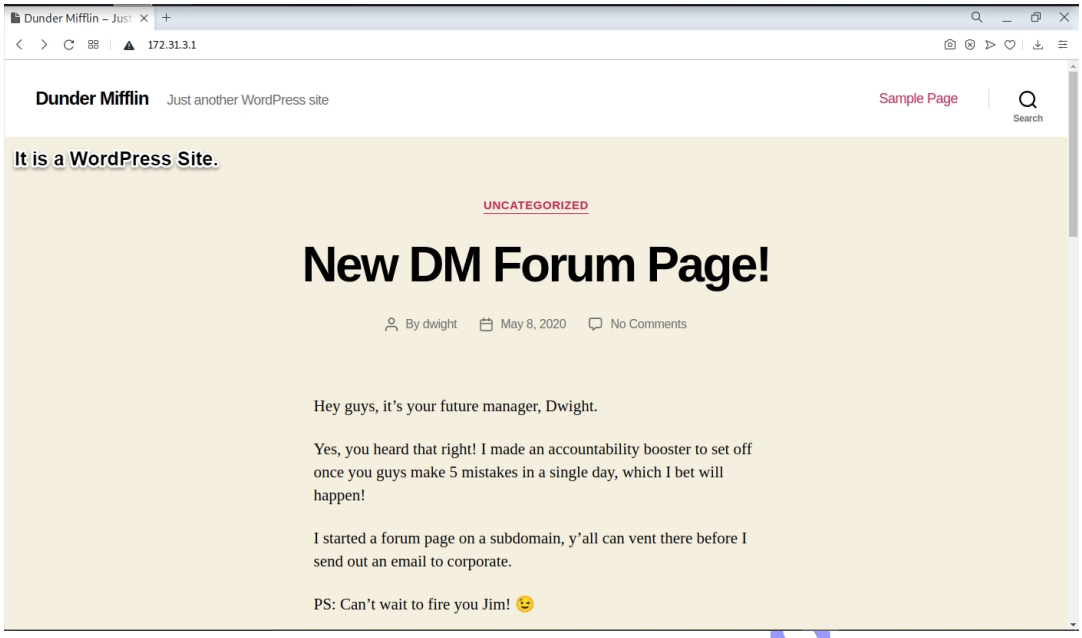
Created: *04-01-2021 19:09:30*
Updated: *10-01-2021 00:15:45*
Author: xShadowx

#Scanning And Enumeration.

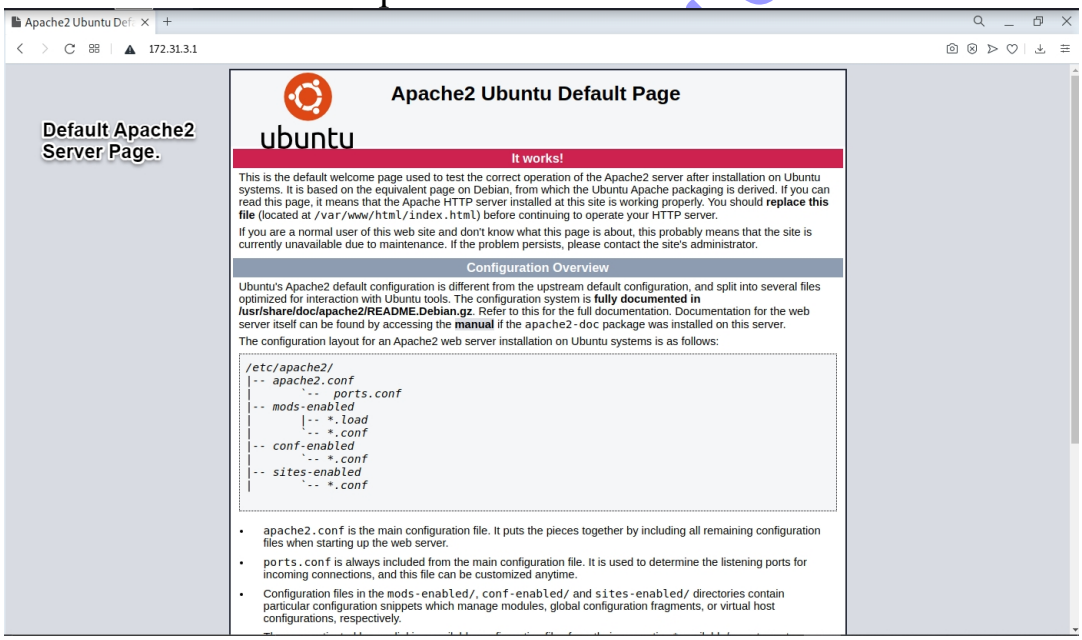


So we have three(3) ports open
1. An ssh port on 22
2. A web server running on 80.
3. A web server(secure) on 443.

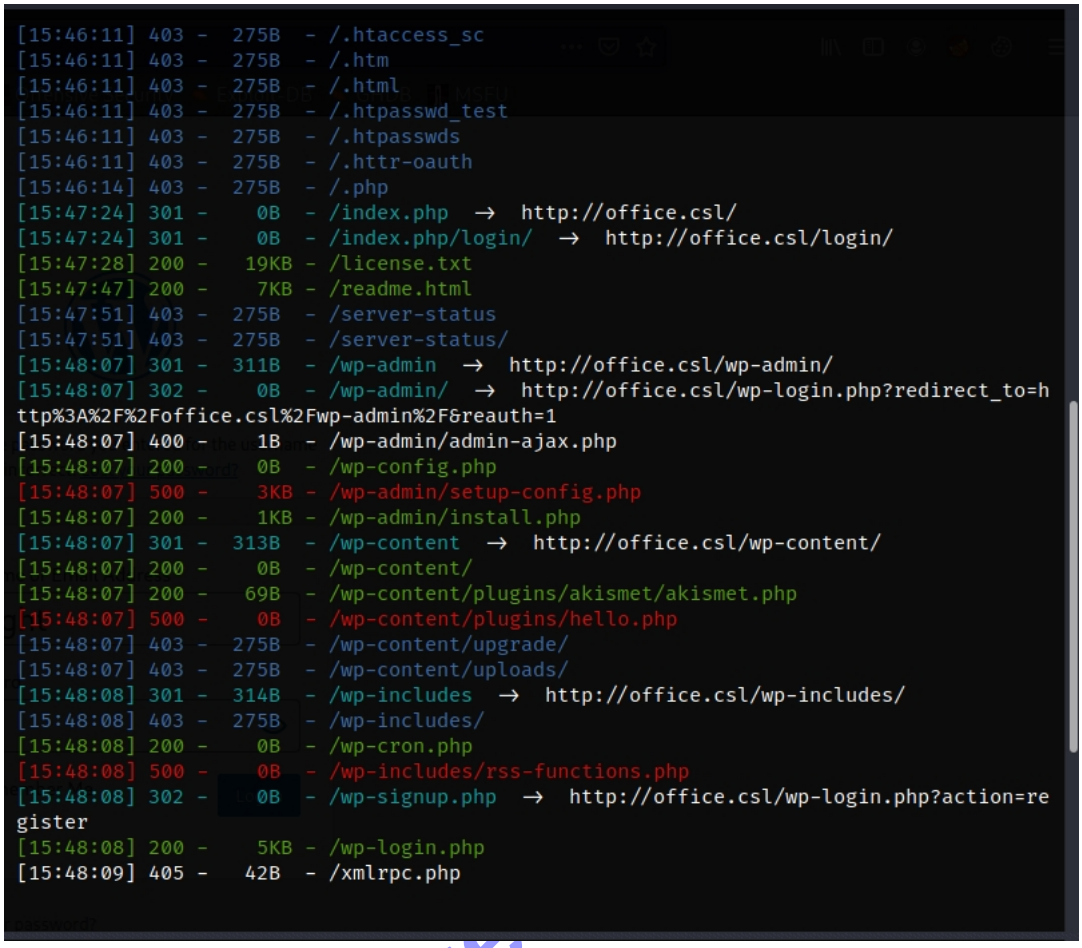
#Web without secure strip



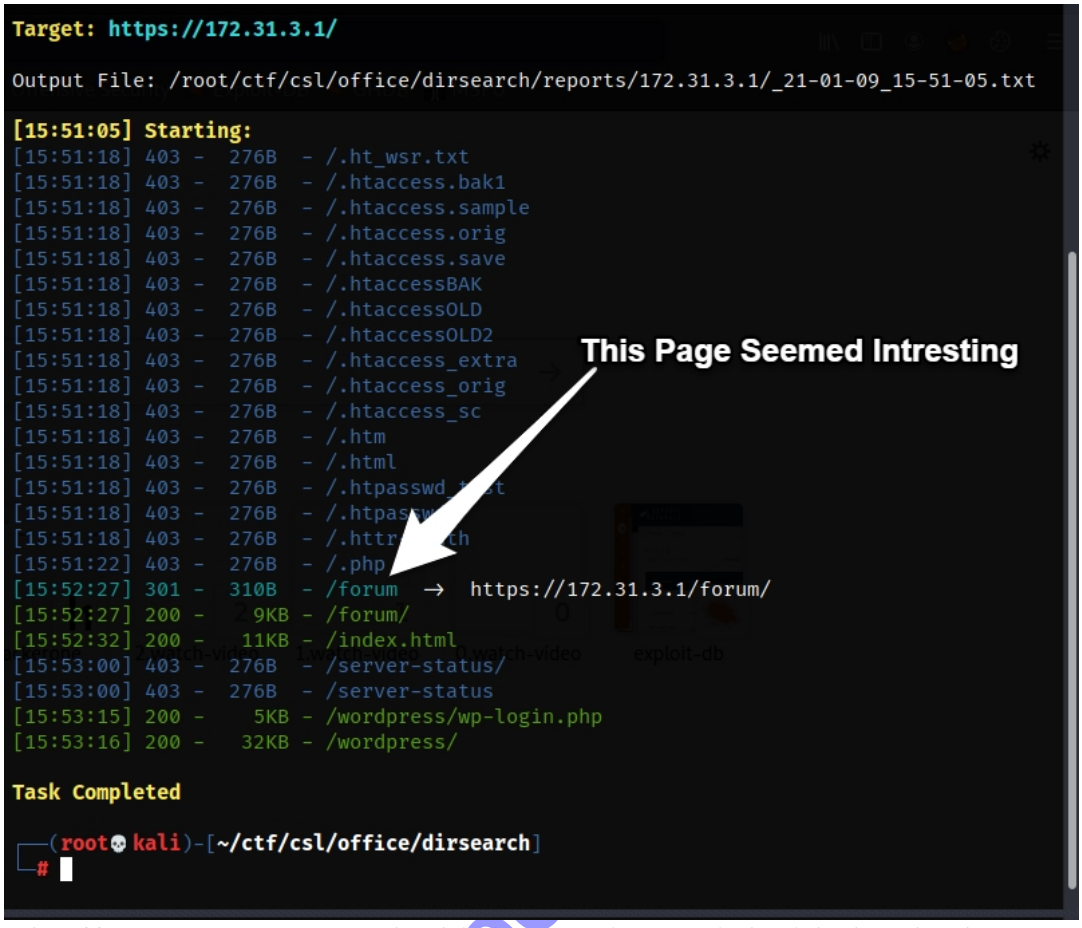
Web With Secure Strip



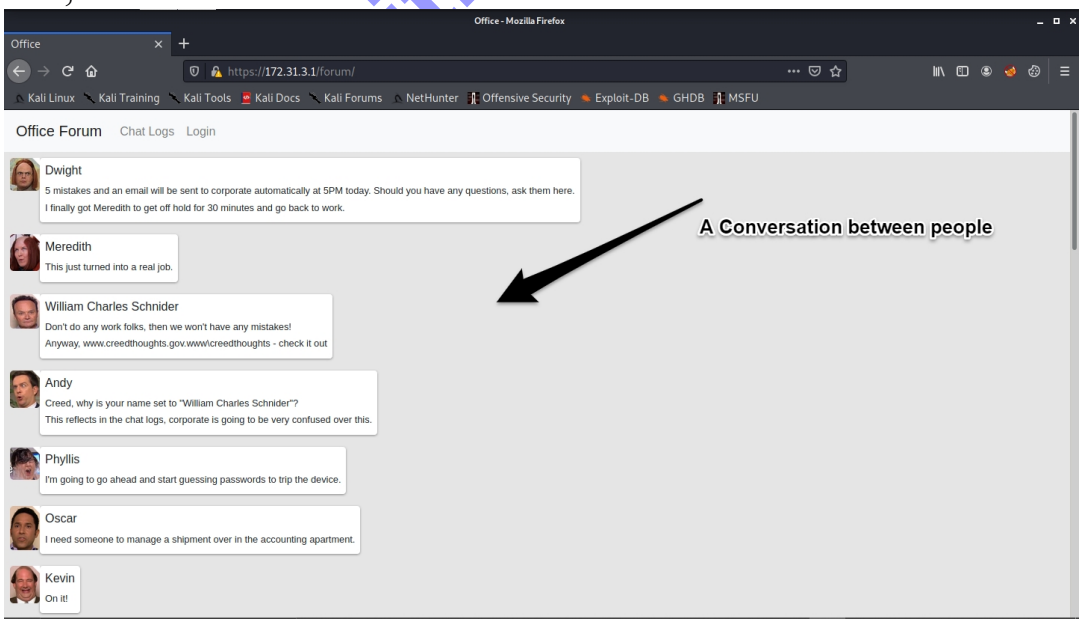
#Directories Found By dir-search



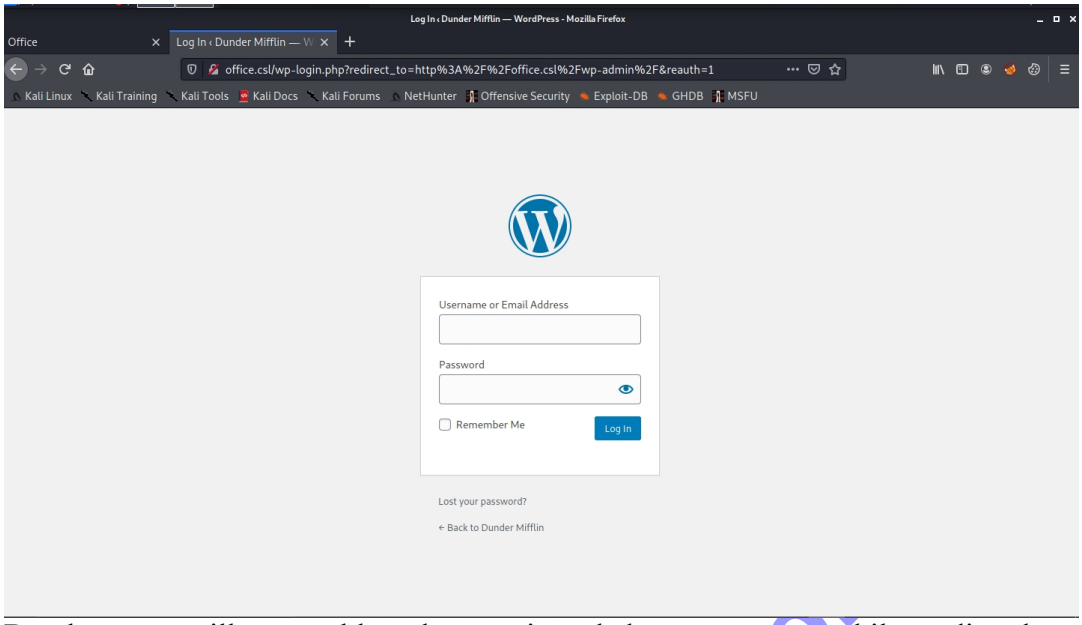
So Before going and checking every single directory in here i decided to hunt directories for the other server too(the secure one with the default page)



The /forum page seemed a bit interesting so i decided to look at that, and...

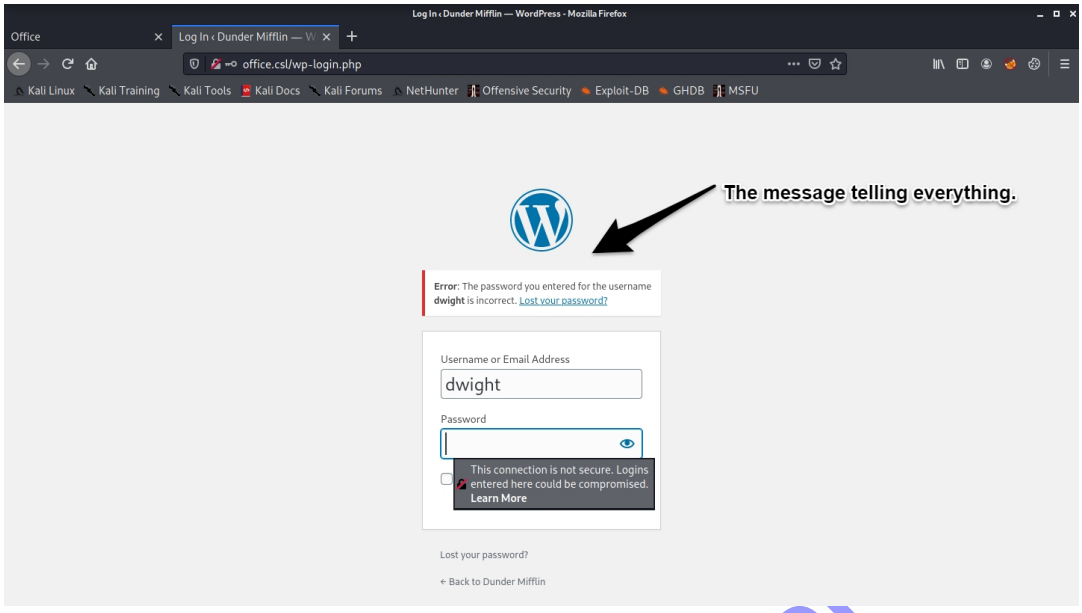


This page got my eye as previously i found a word-press login page

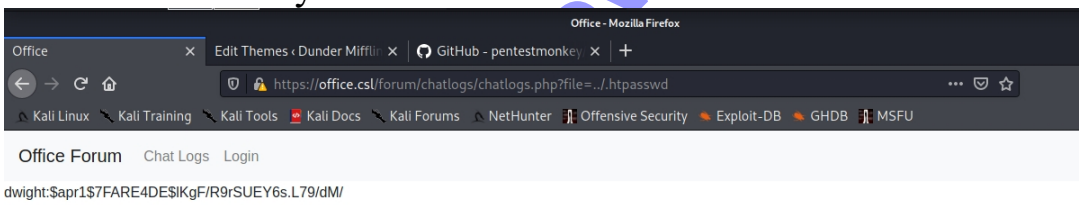


But there was still one problem that was i needed a username so while reading the conversation i found this

So from here i thought checking any available username for person d-w-i-g-h-t and i got lucky.



So this message by the server has confirmed everything - there is a user named d-w-i-g-h-t on word-press but we don't have the password yet so in the scan results the word-press version was 5.4.1 so lets search for any exploit against that before spending hours on dictionary attacks.

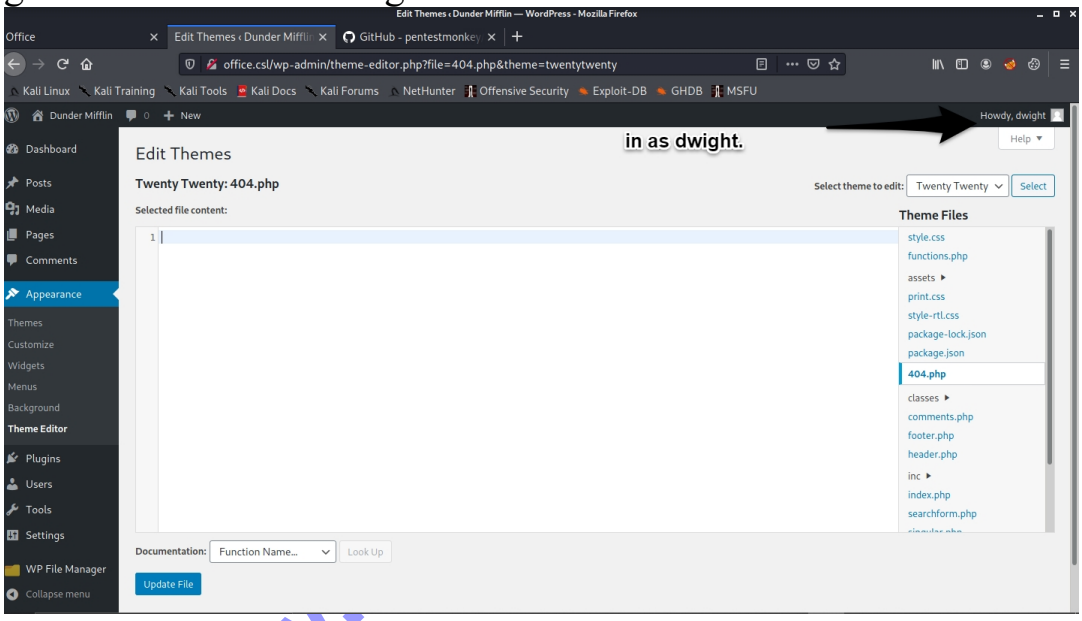


So i found out that the web service is vulnerable to a L.F.I{ Local File Inclusion } so i decided to take a word list full of these random payload and w fuzz that out

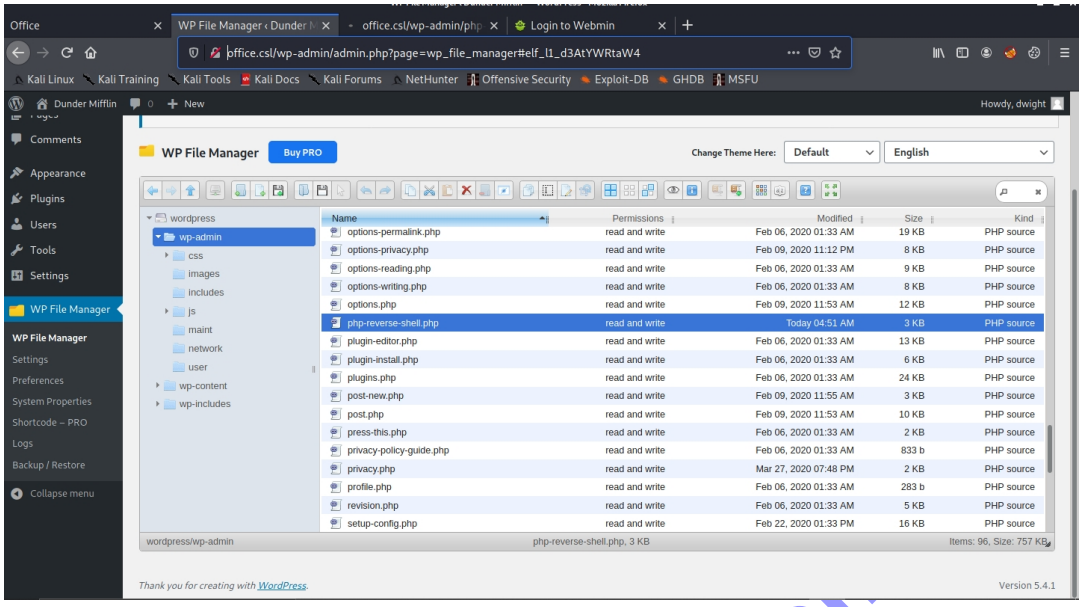
i will always look out for the ht password file as this contains passwords

so i found the password and cracked it using john.

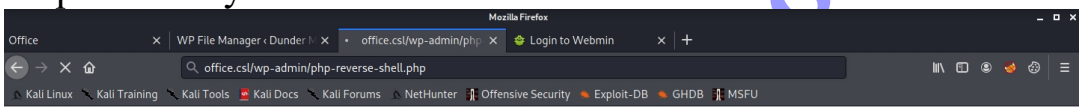
Then i decided to login to word-press using these credentials and i got in as the user d-w-i-g-h-t.



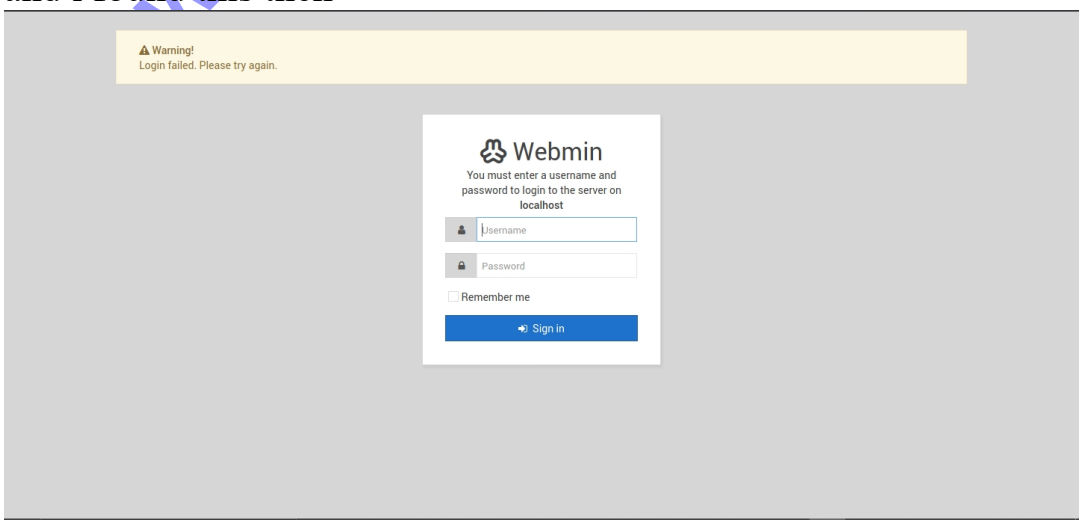
Now i will edit the 404 page the error page and access the page from other u-r-l to get a reverse shell.
unfortunately this did not worked for some reason and after some time searching here and there i found this



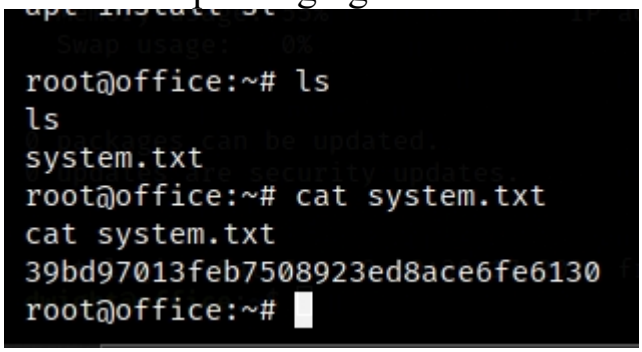
I Uploaded my file here and then access from other url.



Got shell but as web and got user access and the access flag.
now we needed root so i ran lin-peas and discovered a port open on 10000 and decided to forward it to my localhost using ssh (with -L localhost:10000:localhost name@office.csl)
and i found this then



The web-min framework was very vulnerable so i found a matching exploit for it(credits to m-e-t-a-s-p-l-o-i-t)
and after exploiting i got a shell as root.



And also the system flag and pwned the machine.
Awesome.