FreeLancer – HackTheBox

Reconciliation finding steps –

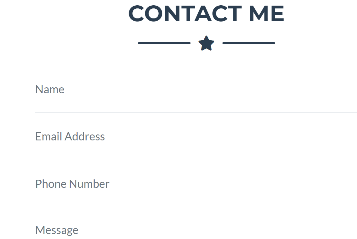
1. Comments:



2. Robots.txt: On and empty.

3. Network – Nothing interesting.

4. JavaScripts – Only one interesting point in "Contact me"

Because we can write things inside.

And there is special java-script for this action at the source directory.

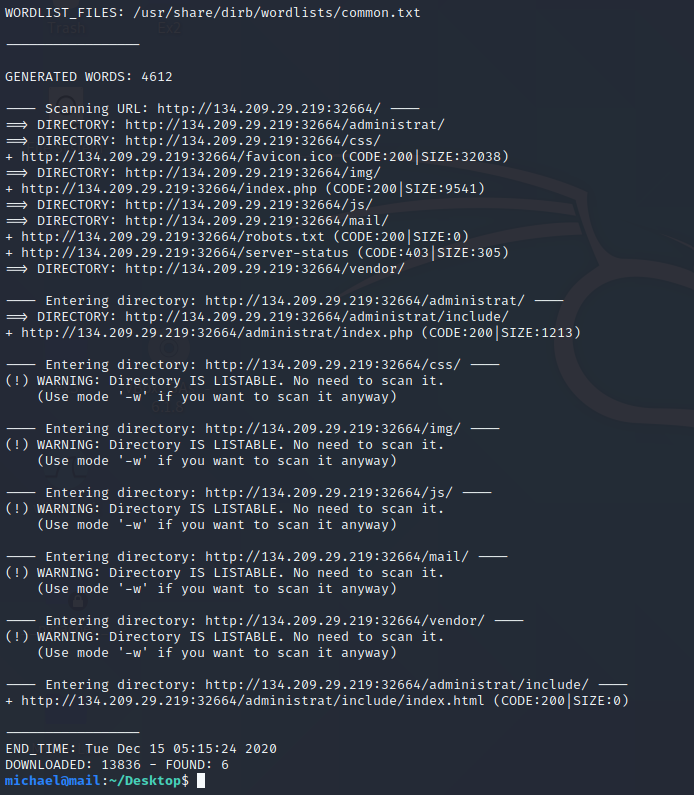
Investigate contact.js:

The website post the user input to file located in: ./.mail/contact\_me/php.

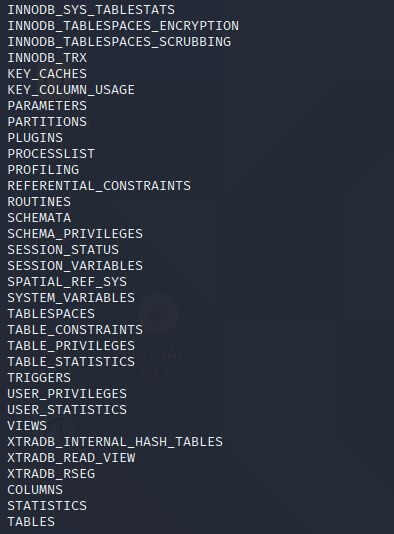
Trying file traversal !

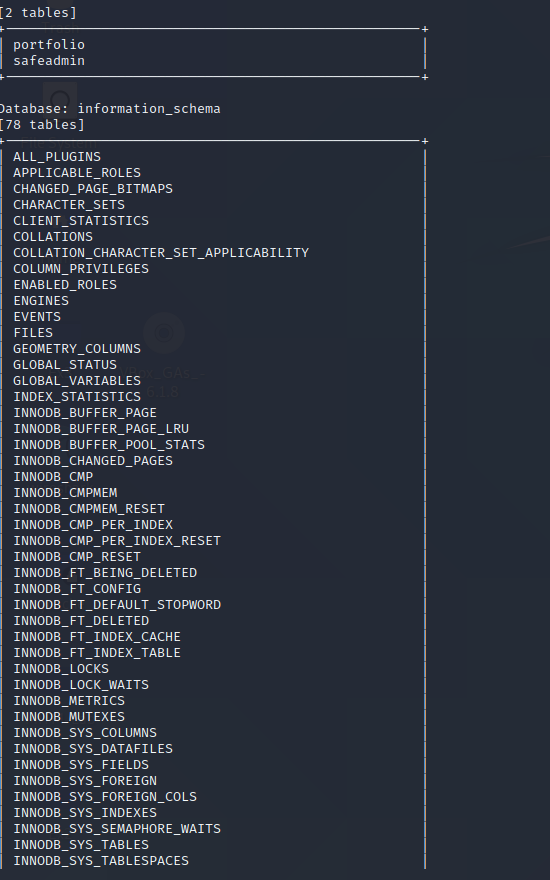
But contact\_me.php is not reachable.

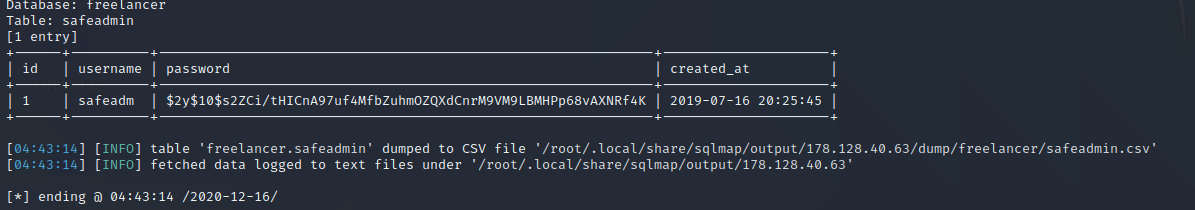
Ok… We can access robots.txt and some directories that not appear in the source directory hence we will use penetration tools to find more!

DireB search result:

Running SQLmap with –forms –crawl=2 flag on the base url website and its show us that in <http://178.128.40.63:32510/portfolio.php?id=1> there is sql injection .

So we run: sqlmap -u <http://178.128.40.63:32510/portfolio.php?id=1> --tables --dump and it mapped us the DB's:

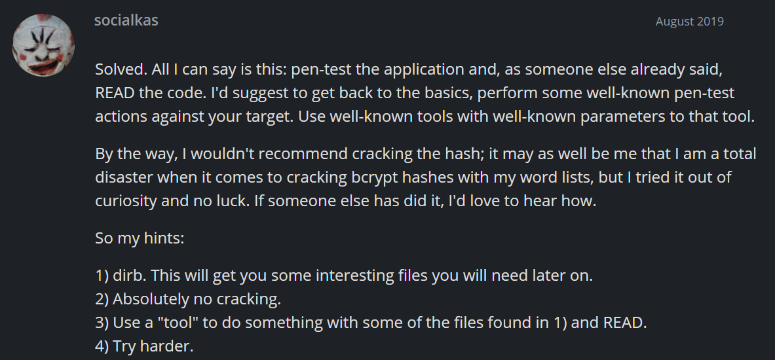


Trying to dump the safeadmin content because all others shows nothing.

But the password is hash so we cant reverse the function.

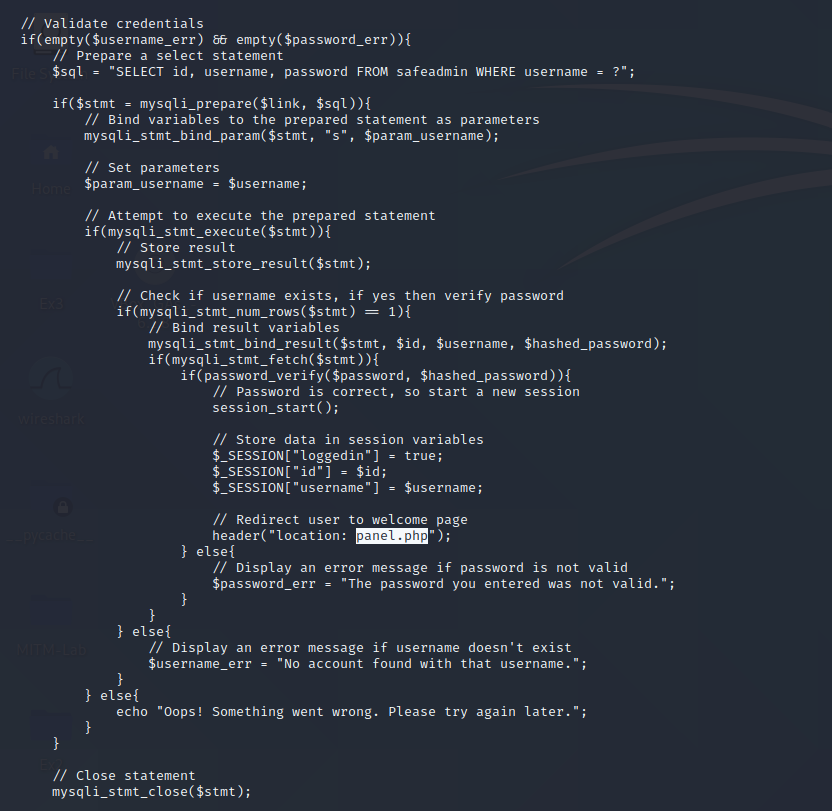
Trying another way..

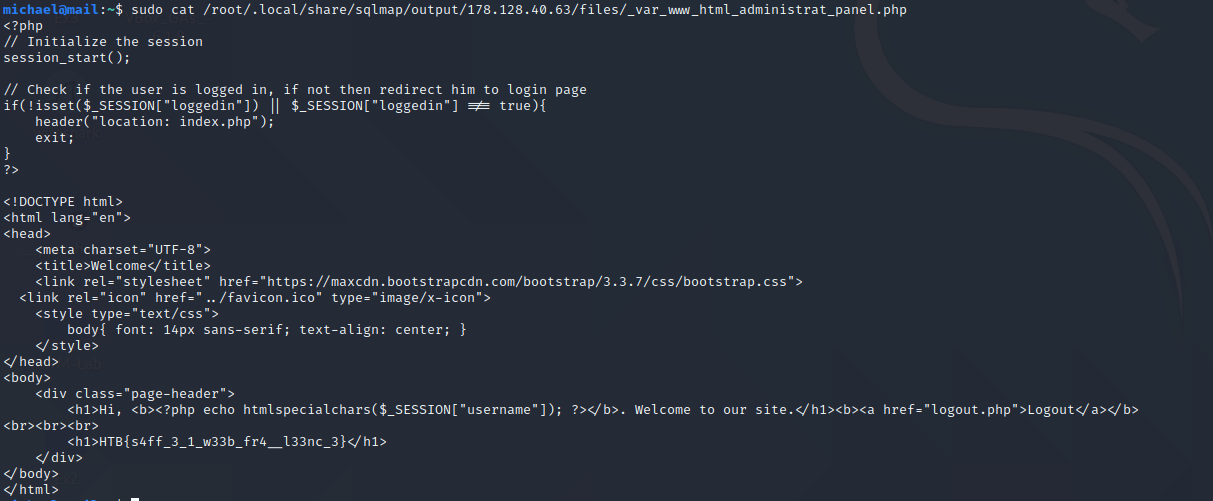
As I tried almost everything I entered HackTheBox forum to see some hint and I find my angel!

So I find a way to READ the file

Index.php that we cant see in the client side with flag:

--file-read**=/var/www/html/**administrat/index.php





Flag: HTB{s4ff\_3\_1\_w33b\_fr4\_\_l33nc\_3}