Scans Output

Nmap Scan Output

```
Scan Information:
===============================================================================
=
Scan Arguments: nmap -v -p- -A -oX 10.10.156.12/output/outputNmap.xml 10.10.156.12
Scan Start Time: Tue May 30 14:01:41 2023
Scan Version: 7.93
===============================================================================
=
Host Information:
Host Address: 10.10.156.12
===============================================================================
=
Open Ports:
------------------------------------------------------------------------------------------------------------------
--
Port: 22
Protocol: tcp
Service Name: ssh
Service Product: OpenSSH
Service Version: 7.2p2 Ubuntu 4ubuntu2.6
Scripts ran:
-> ssh-hostkey:
  2048 c0de1202c5b557931feff3627b5ccf3d (RSA)
  256 3626ad2a91ba8aa09ca9433ac27276b7 (ECDSA)
  256 5efd71a5200217a887993a684c5ad125 (ED25519)
------------------------------------------------------------------------------------------------------------------
--
Port: 80
Protocol: tcp
Service Name: http
Service Product: Apache httpd
Service Version: 2.4.18
Scripts ran:
-> http-title: Rick is sup4r cool
-> http-methods:
  Supported Methods: GET HEAD POST OPTIONS
-> http-server-header: Apache/2.4.18 (Ubuntu)
------------------------------------------------------------------------------------------------------------------
```

```
--
===============================================================================
=
```

Nikto Scan Output

```
Scan Information:
===============================================================================
=
Target IP: 10.10.156.12
Target hostname: 10.10.156.12
Target port: 80
Scan start time: 2023-05-30 14:02:30
===============================================================================
=
Items:
--------------------------------------------------------------------------------------------------------------------------------------------------
--
Method: GET
Description: /: The anti-clickjacking X-Frame-Options header is not present.
URI: /
Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-
Options
--------------------------------------------------------------------------------------------------------------------------------------------------
--
Method: GET
Description: /: The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type.
URI: /
Reference: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/
missing-content-type-header/
--------------------------------------------------------------------------------------------------------------------------------------------------
--
Method: HEAD
Description: Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.54). Apache
2.2.34 is the EOL for the 2.x branch.
URI: /
Reference: Reference not available
--------------------------------------------------------------------------------------------------------------------------------------------------
--
Method: GET
Description: /: Server may leak inodes via ETags, header found with file /, inode: 426, size:
5818ccf125686, mtime: gzip.
URI: /
```

```
Reference: CVE-2003-1418
-----------------------------------------------------------------------------------------------------------------
--
Method: GET
Description: /login.php: Cookie PHPSESSID created without the httponly flag.
URI: /login.php
Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
-----------------------------------------------------------------------------------------------------------------
--
Method: OPTIONS
Description: OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
URI: /
Reference: Reference not available
-----------------------------------------------------------------------------------------------------------------
--
Method: GET
Description: /icons/README: Apache default file found.
URI: /icons/README
Reference: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
-----------------------------------------------------------------------------------------------------------------
--
Method: GET
Description: /login.php: Admin login page/section found.
URI: /login.php
Reference: Reference not available
-----------------------------------------------------------------------------------------------------------------
--
=========================================================================
=
```

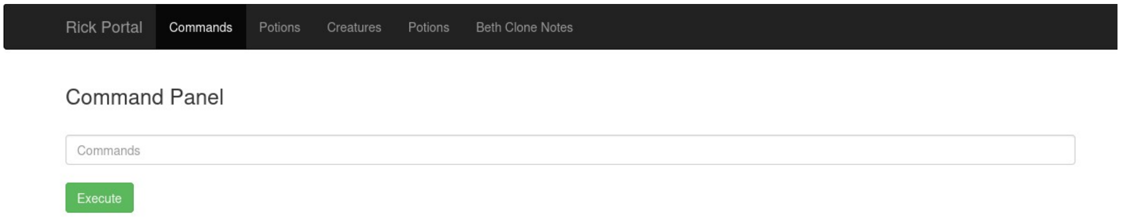
Dirbuster Scan Output

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: 10.10.156.12/output/outputDirb.txt
START_TIME: Tue May 30 14:06:53 2023
URL_BASE: http://10.10.156.12/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------
```

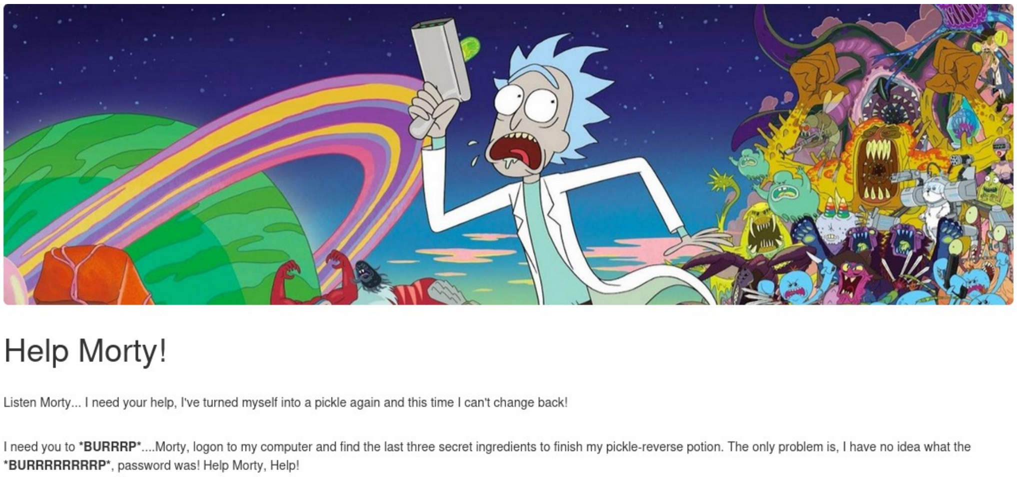
```
GENERATED WORDS: 4612

---- Scanning URL: http://10.10.156.12/ ----
==> DIRECTORY: http://10.10.156.12/assets/
+ http://10.10.156.12/index.html (CODE:200|SIZE:1062)
+ http://10.10.156.12/robots.txt (CODE:200|SIZE:17)
+ http://10.10.156.12/server-status (CODE:403|SIZE:300)

---- Entering directory: http://10.10.156.12/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Tue May 30 14:09:16 2023
DOWNLOADED: 4612 - FOUND: 3
```

Captured Screenshots

Screenshot: 10.10.156.12/screenshots/10.10.156.12.login.php.png



Screenshot: 10.10.156.12/screenshots/http...10.10.156.12.index.html.png

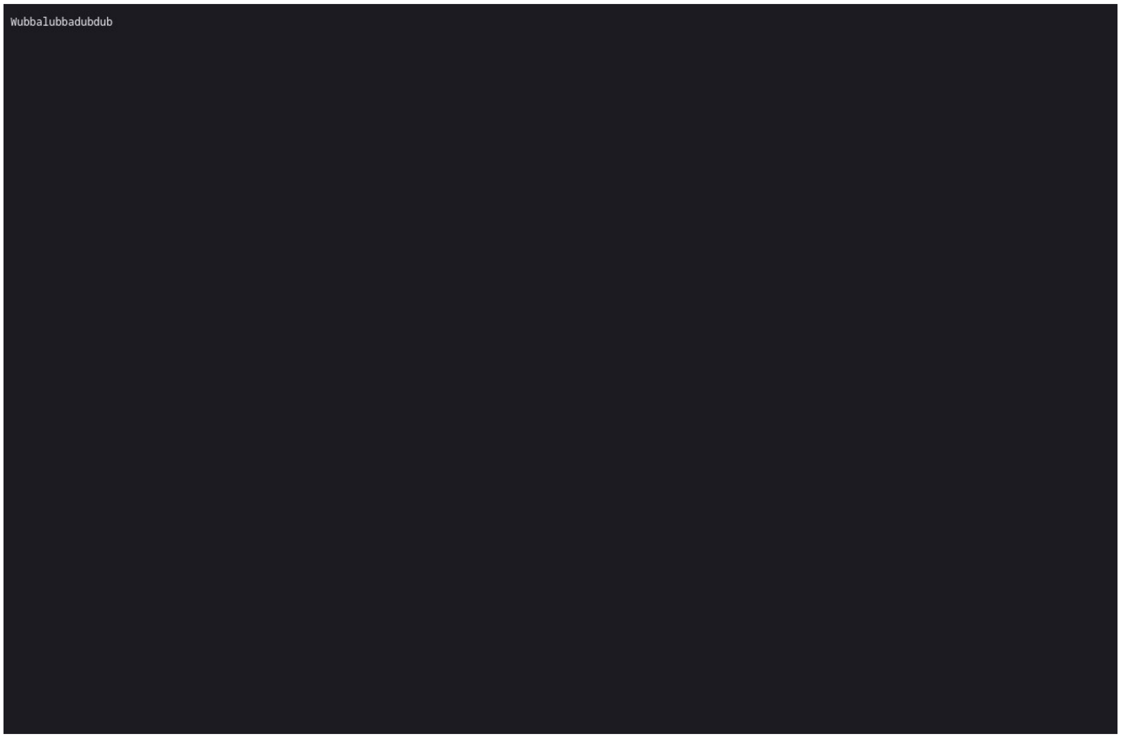


Help Morty!

Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!

I need you to ***BURRRP***....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is, I have no idea what the ***BURRRRRRRRP***, password was! Help Morty, Help!

Screenshot: 10.10.156.12/screenshots/http...10.10.156.12.robots.txt.png



```
Wubbalubbadubdub
```

Created wordlist

```
Note
to
self
remember
username
Username
R1ckRul3s
Rick
is
sup4r
cool
Help
Morty
Listen
Morty
I
need
```

your
help
Ive
turned
myself
into
a
pickle
again
and
this
time
I
cant
change
back
I
need
you
to
BURRRPMorty
logon
to
my
computer
and
find
the
last
three
secret
ingredients
to
finish
my
picklereverse
potion
The
only
problem
is
I
have
no

idea
what
the
BURRRRRRRRP
password
was
Help
Morty
Help
Wubbalubbadubdub

Discovered credentials

R1ckRul3s:Wubbalubbadubdub