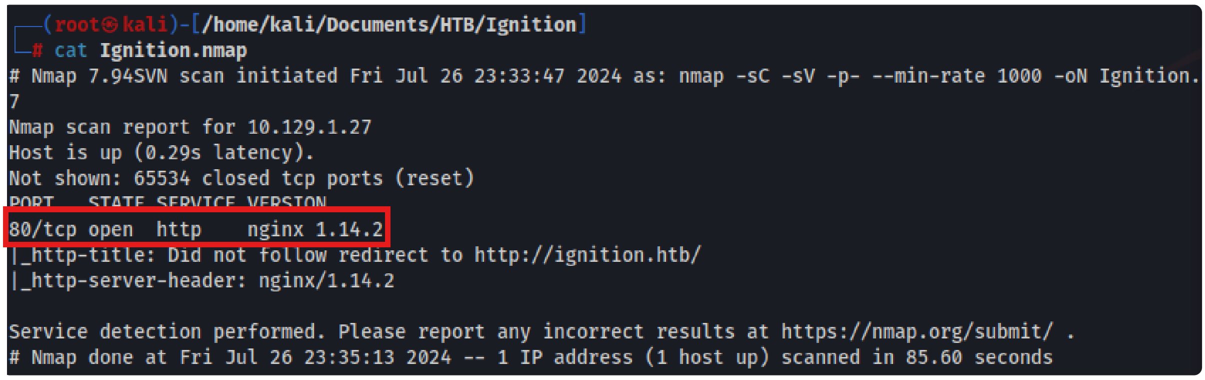
Ignition

Task 1
Which service version is found to be running on port 80?

- nginx 1.14.2

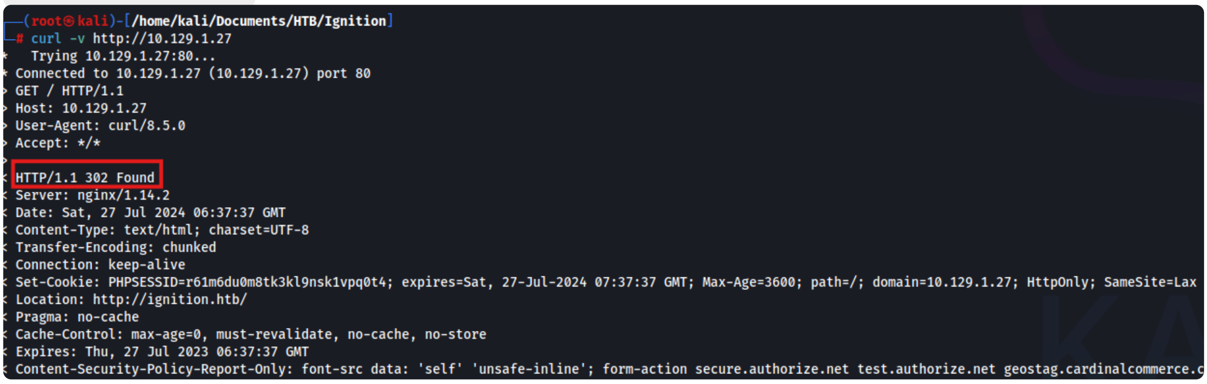


```
┌──(root㉿kali)-[/home/kali/Documents/HTB/Ignition]
└─# cat Ignition.nmap
# Nmap 7.94SVN scan initiated Fri Jul 26 23:33:47 2024 as: nmap -sC -sV -p- --min-rate 1000 -oN Ignition.
7
Nmap scan report for 10.129.1.27
Host is up (0.29s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.2
|_http-title: Did not follow redirect to http://ignition.htb/
|_http-server-header: nginx/1.14.2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jul 26 23:35:13 2024 -- 1 IP address (1 host up) scanned in 85.60 seconds
```

Task 2
What is the 3-digit HTTP status code returned when you visit http://{machine IP}/?

- 302
- `curl -v http://10.129.1.27`



```
┌──(root㉿kali)-[/home/kali/Documents/HTB/Ignition]
└─# curl -v http://10.129.1.27
*   Trying 10.129.1.27:80...
* Connected to 10.129.1.27 (10.129.1.27) port 80
> GET / HTTP/1.1
> Host: 10.129.1.27
> User-Agent: curl/8.5.0
> Accept: */*
>
< HTTP/1.1 302 Found
< Server: nginx/1.14.2
< Date: Sat, 27 Jul 2024 06:37:37 GMT
< Content-Type: text/html; charset=UTF-8
< Transfer-Encoding: chunked
< Connection: keep-alive
< Set-Cookie: PHPSESSID=r61m6du0m8tk3kl9nsk1vpq0t4; expires=Sat, 27-Jul-2024 07:37:37 GMT; Max-Age=3600; path=/; domain=10.129.1.27; HttpOnly; SameSite=Lax
< Location: http://ignition.htb/
< Pragma: no-cache
< Cache-Control: max-age=0, must-revalidate, no-cache, no-store
< Expires: Thu, 27 Jul 2023 06:37:37 GMT
< Content-Security-Policy-Report-Only: font-src data: 'self' 'unsafe-inline'; form-action secure.authorize.net test.authorize.net geostag.cardinalcommerce.c
```

- curl -v
  - **Request Headers**: Details about the headers being sent in the request.
  - **Response Headers**: Information about the headers received in the response.
  - **Connection Information**: Details about the connection process.
  - **Body Data**: The content of the response body (e.g., HTML, JSON).

Task 3
What is the virtual host name the webpage expects to be accessed by?

- ignition.htb

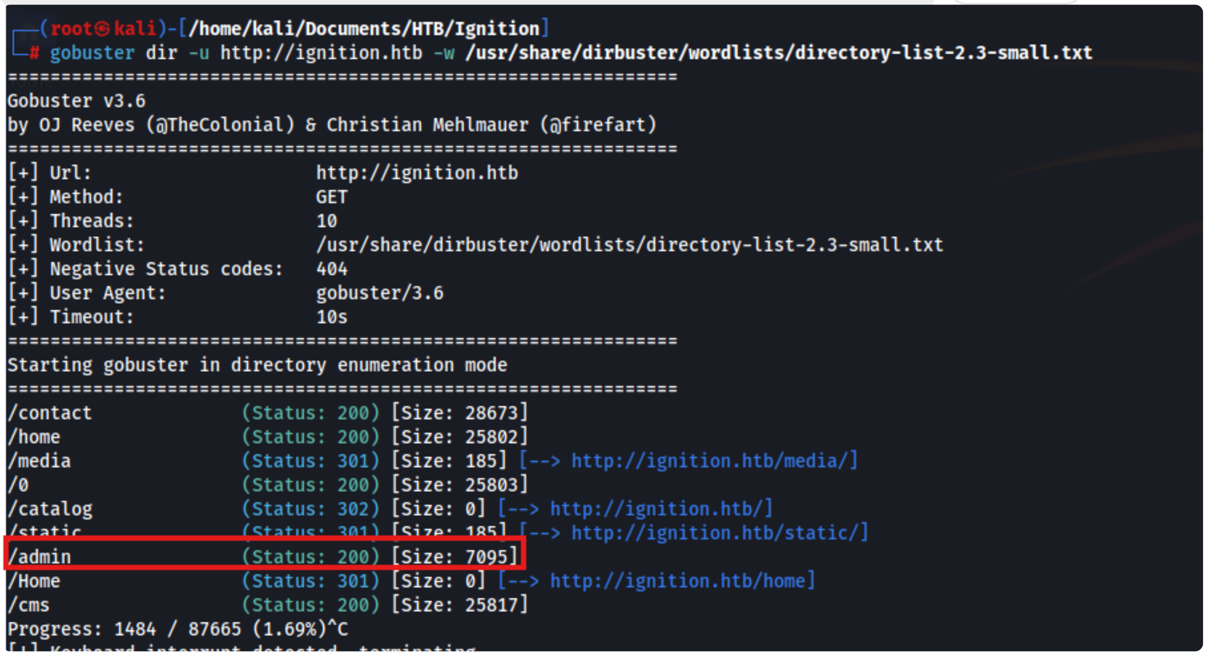
Task 4
What is the full path to the file on a Linux computer that holds a local list of domain name to IP address pairs?

- /etc/hosts

Task 5

Use a tool to brute force directories on the webserver. What is the full URL to the Magento login page?

- http://ignition.htb/admin
- `gobuster dir -u http://ignition.htb -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt` #gobuster



```
┌──(root㉿kali)-[/home/kali/Documents/HTB/Ignition]
└─# gobuster dir -u http://ignition.htb -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://ignition.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/contact              (Status: 200) [Size: 28673]
/home                 (Status: 200) [Size: 25802]
/media                (Status: 301) [Size: 185] [--> http://ignition.htb/media/]
/0                    (Status: 200) [Size: 25803]
/catalog              (Status: 302) [Size: 0] [--> http://ignition.htb/]
/static               (Status: 301) [Size: 185] [--> http://ignition.htb/static/]
/admin                (Status: 200) [Size: 7095]
/Home                 (Status: 301) [Size: 0] [--> http://ignition.htb/home]
/cms                  (Status: 200) [Size: 25817]
Progress: 1484 / 87665 (1.69%)^C
[!] Keyboard interrupt detected, terminating.
```

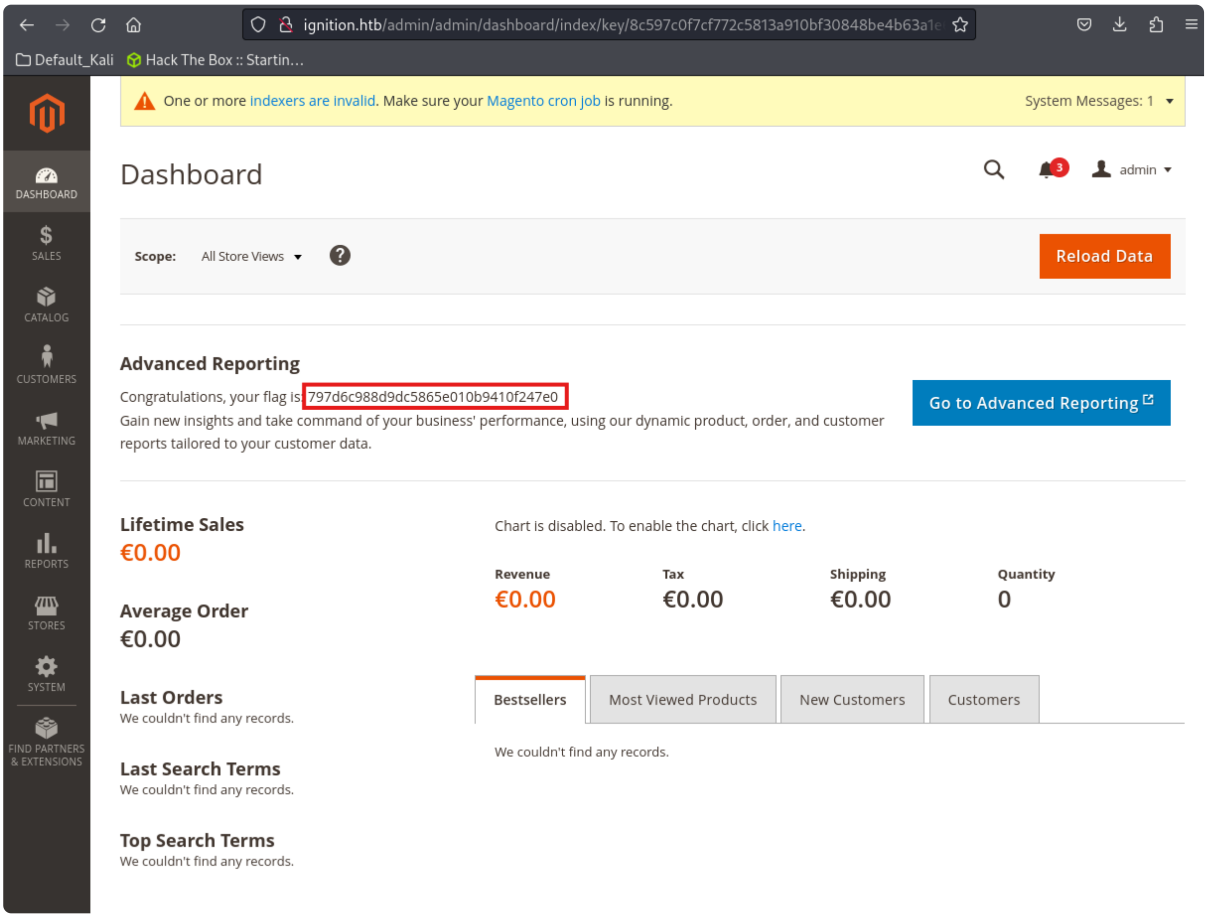
Task 6

Look up the password requirements for Magento and also try searching for the most common passwords of 2023. Which password provides access to the admin account?

- qwerty123

Submit Flag

- Login to the account and get the flag
  - admin
  - qwerty123



One or more indexers are invalid. Make sure your Magento cron job is running.

System Messages: 1

Dashboard

Scope: All Store Views

Advanced Reporting

Congratulations, your flag is: 797d6c988d9dc5865e010b9410f247e0

Gain new insights and take command of your business' performance, using our dynamic product, order, and customer reports tailored to your customer data.

Lifetime Sales
€0.00

Average Order
€0.00

Last Orders
We couldn't find any records.

Last Search Terms
We couldn't find any records.

Top Search Terms
We couldn't find any records.

Chart is disabled. To enable the chart, click here.

Revenue	Tax	Shipping	Quantity
€0.00	€0.00	€0.00	0

We couldn't find any records.