

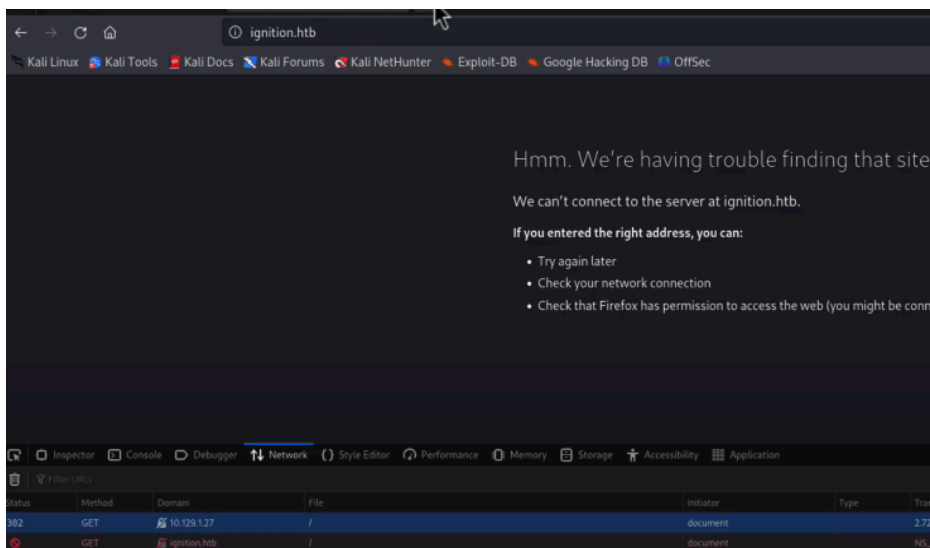
```
(root@kali)-[/home/alvadelg/Escritorio]
# openvpn starting_point_AlvaroDelgado11.ovpn
2025-01-24 16:02:59 WARNING: Compression for receiving enabled. Compression has
been used in the past to break encryption. Sent packets are not compressed
unless "allow-compression yes" is also set.
2025-01-24 16:02:59 Note: --data-ciphers-fallback with cipher 'AES-128-CBC' d
isables data channel offload.
2025-01-24 16:02:59 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO]
[...]
```

```
(root@kali)-[/mnt]
# nmap -sV -O -sS -A -p- 10.129.1.27
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-21 13:25 CET
Nmap scan report for 10.129.1.27
Host is up (0.044s 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
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.0
OS details: Linux 5.0
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   43.04 ms  10.10.14.1
2   43.36 ms  10.129.1.27

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.03 seconds
```

Which service version is found to be running on port 80?  
nginx 1.14.2



Status	Method	Domain
302	GET	10.129.1.27
🚫	GET	ignition.htb

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

302

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`

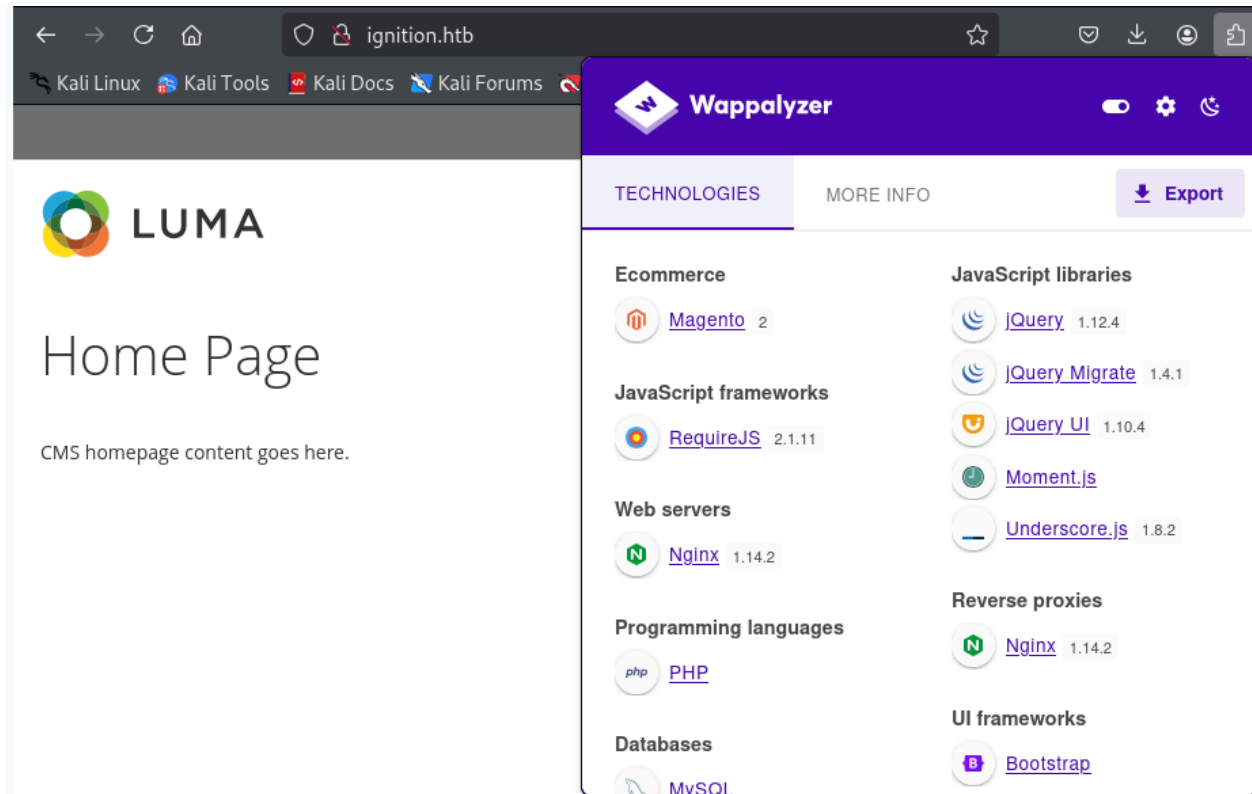
```
(root@kali)-[/mnt]
# nano /etc/hosts

GNU nano 8.2 /etc/hosts
127.0.0.1    localhost
127.0.1.1    kali

# The following lines are desirable for IPv6 capable hosts
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
10.129.1.27 ignition.htb
```

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

`ignition.htb`



Now with this extension we can see that the programming language is PhP and Js

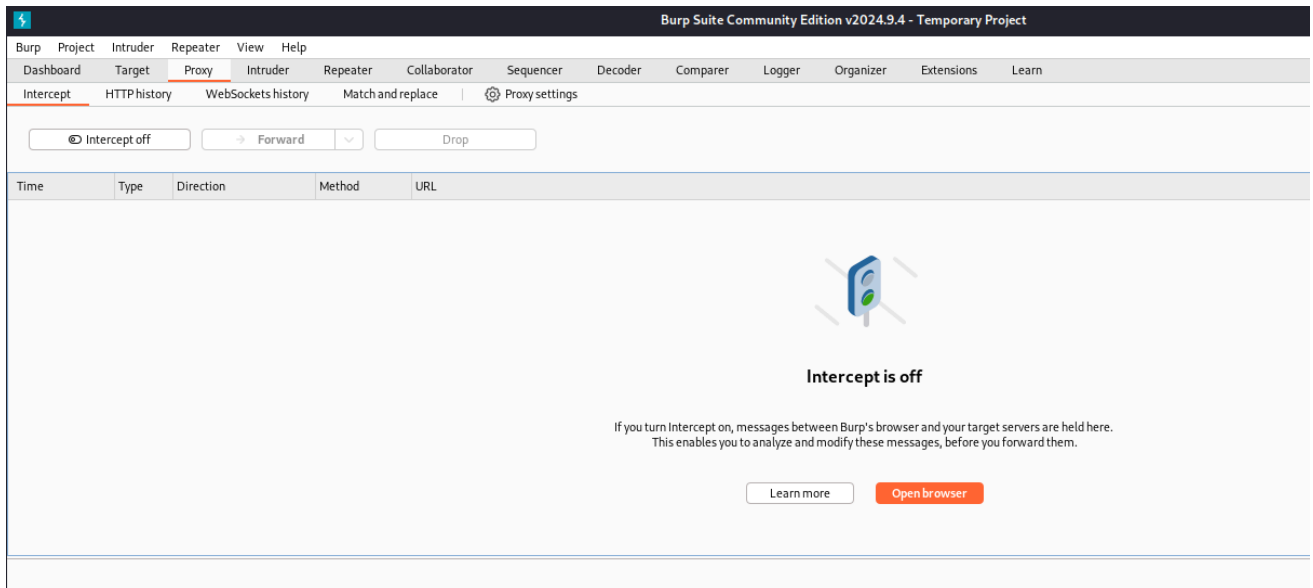
Use a tool to brute force directories on the web server. What is the full URL to the Magento login page?

```
(root@kali)-[/mnt]
# gobuster dir -u http://ignition.htb -w /usr/share/dirb/wordlists/common.txt -x php,js

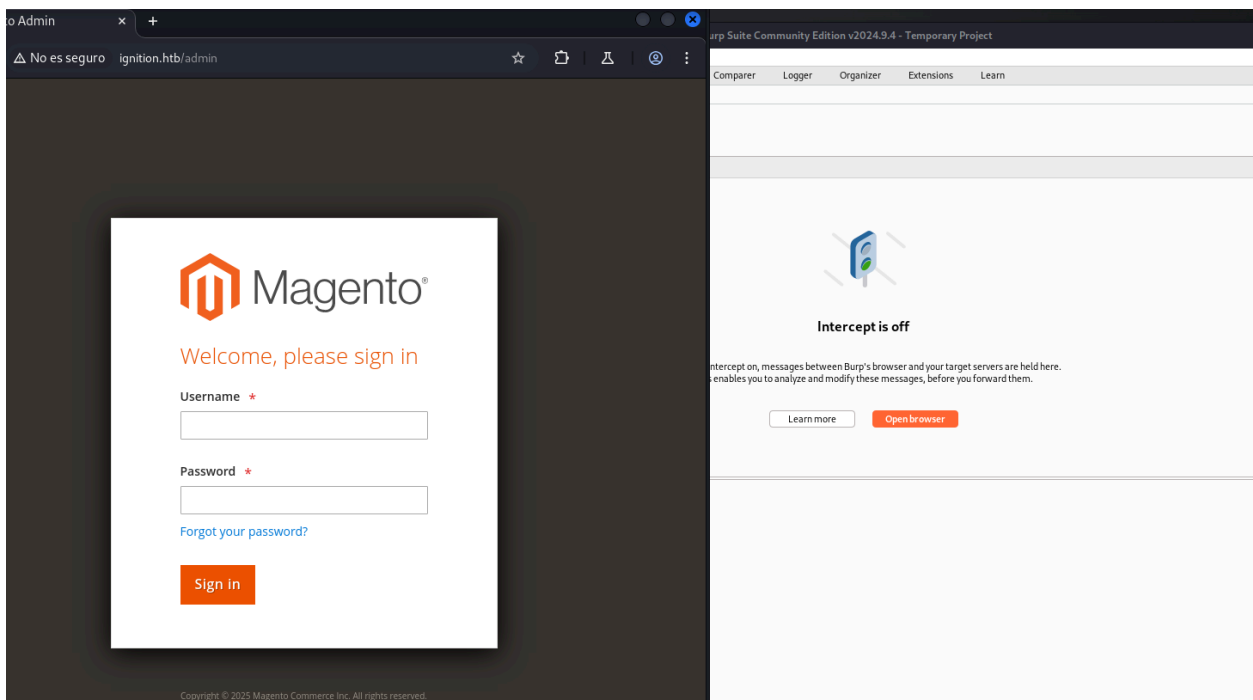
Starting gobuster in directory enumeration mode

/0 (Status: 200) [Size: 25803]
/admin (Status: 200) [Size: 7092]
/catalog (Status: 302) [Size: 0] [→ http://ignition.htb/]
```

<http://ignition.htb/admin>



Open browser



<div> <span>Intercept on</span> <span>→ Forward</span> <span>Drop</span> </div>				
Time	Type	Direction	Method	URL
14:06:27 21 feb...	HTTP	→ Request	POST	http://ignition.htb/admin

## Request

	Pretty	Raw	Hex
1	POST /admin HTTP/1.1		
2	Host: ignition.htb		
3	Content-Length: 77		
4	Cache-Control: max-age=0		
5	Accept-Language: es-ES,es;q=0.9		
6	Origin: http://ignition.htb		
7	Content-Type: application/x-www-form-urlencoded		
8	Upgrade-Insecure-Requests: 1		
9	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36		
10	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7		
11	Referer: http://ignition.htb/admin		
12	Accept-Encoding: gzip, deflate, br		
13	Cookie: admin=pljfktpgm10pqongba3g0v1b0		
14	Connection: keep-alive		
15			
16	form_key=sRsIcMnoyjfNveyS&login%5Busername%5D=admin&login%5Bpassword%5D=admin		

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward Drop

Time	Type	Direction	Method	URL
14:07:13 21 Feb ...	HTTP	→ Request	POST	http://ignition.htb/admin

Request

Pretty Raw

```

1 POST /admin HTTP/1.1
2 Host: ignition.htb
3 Content-Length: 80
4 Cache-Control: max-age=0
5 Accept-Language: es-ES,es;q=0.9
6 Origin: http://ignition.htb
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://ignition.htb/admin
12 Accept-Encoding: gzip, deflate, br
13 Cookie: admin=pljftjpgm10pqongba3g0v1b0
14 Connection: keep-alive
15
16 form_key=sRsIcMnoyjfNveyS&login%5Busername%5D=admin&login%5Bpassword%5D=admin

```

Scan

- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Send to Organizer Ctrl+O
- Insert Collaborator payload
- Request in browser >
- Engagement tools [Pro version only] >

Change request method

Change body encoding

- Copy Ctrl+C
- Copy URL
- Copy as curl command (bash)
- Copy to file
- Paste from file
- Save item

Don't intercept requests >

Do intercept >

Convert selection >

URL-encode as you type

- Cut Ctrl+X
- Copy Ctrl+C
- Paste Ctrl+V

## Sent to intruder

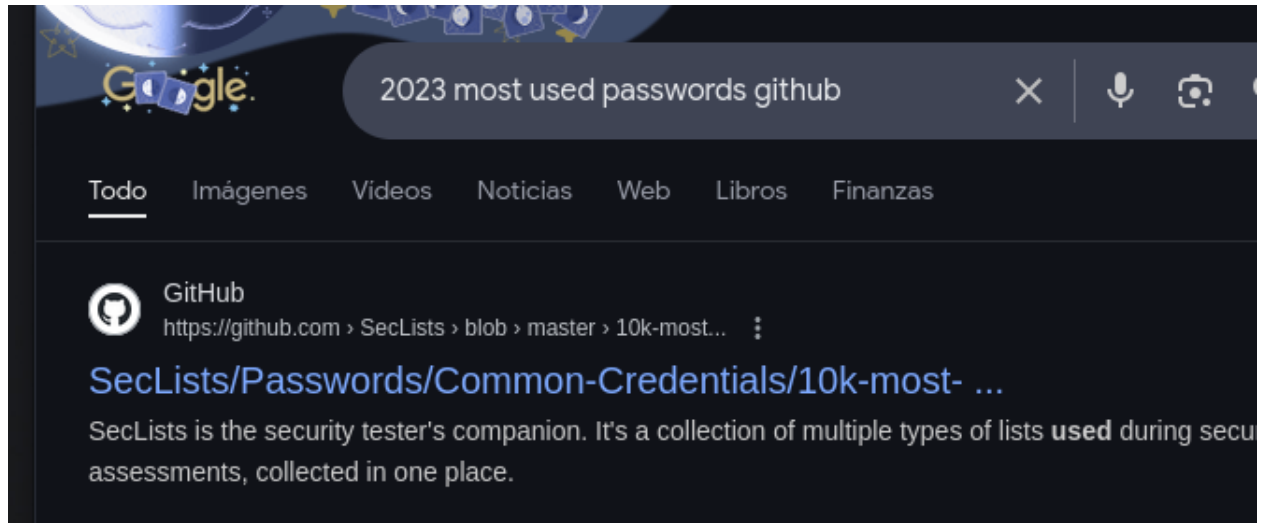
```

1 POST /admin HTTP/1.1
2 Host: ignition.htb
3 Content-Length: 80
4 Cache-Control: max-age=0
5 Accept-Language: es-ES,es;q=0.9
6 Origin: http://ignition.htb
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://ignition.htb/admin
12 Accept-Encoding: gzip, deflate, br
13 Cookie: admin=pljftjpgm10pqongba3g0v1b0
14 Connection: keep-alive
15
16 form_key=sRsIcMnoyjfNveyS&login%5Busername%5D=admin&login%5Bpassword%5D=$passwords

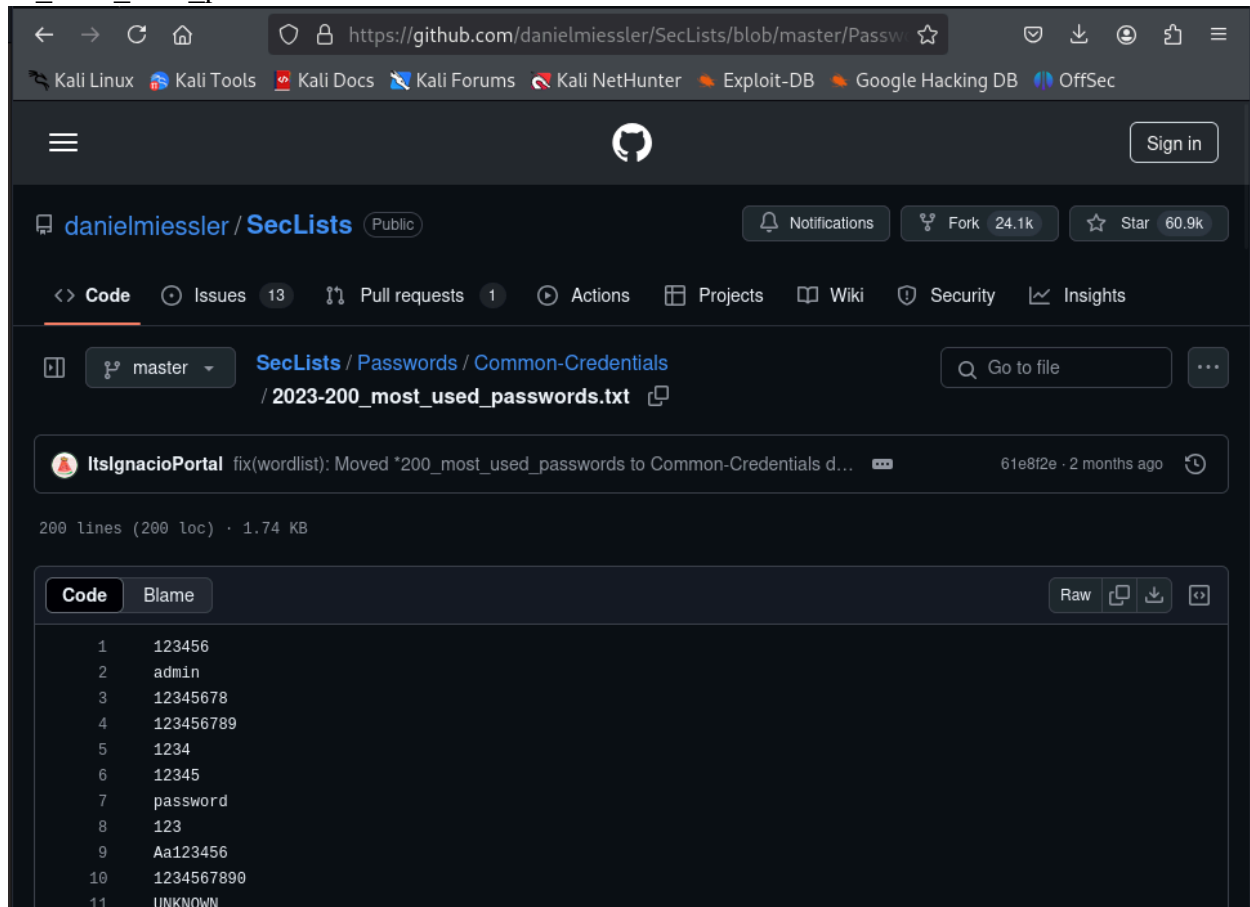
```

```
form_key=sRsIcMnoyjfNveyS&login%5Busername%5D=admin&login%5Bpassword%5D=$passwords
```

ord%5D=\$password\$



[https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/2023-200\\_most\\_used\\_passwords.txt](https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/2023-200_most_used_passwords.txt)



Copy and paste here in burpsuite:

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	123456
Load...	admin
Remove	12345678
Clear	123456789
Deduplicate	1234
	12345
	password
	123
	Aa123456
	1234567890
Add	Enter a new item

Add from list... [Pro version only]

```

1 POST /admin HTTP/1.1
2 Host: ignition.htb
3 Content-Length: 80
4 Cache-Control: max-age=0
5 Accept-Language: es-ES,es;q=0.9
6 Origin: http://ignition.htb
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
1 Referer: http://ignition.htb/admin
2 Accept-Encoding: gzip, deflate, br
3 Cookie: admin=plj9ktj9gnl0qongba3y0vlbo
4 Connection: keep-alive
5
6 form_keysRaIch9oyjftfwey5&llogin5&username5D=admin&llogin5&password5D=password

```

Request count: 0

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	password
Load...	123456
Remove	12345678
Clear	1234
Deduplicate	qwerty
	12345
	dragon
	pussy
	baseball
	football
Add	Enter a new item
Add from list...	[Pro version only]



Start attack

And then we are going to hit start attack:

4. Intruder attack of http://ignition.htb

Attack Save

4. Intruder attack of http://ignition.htb

Attack Save

Results Positions

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	156			10154	
1	123456	200	160			10154	
2	admin	200	151			10154	
3	12345678	200	154			10154	
4	123456789	200	161			10154	
5	1234	200	155			10154	
6	12345	200	162			10154	
7	password	200	158			10154	
8	123	200	165			10154	
9	Aa123456	200	168			10154	

Now we are searching the status code 302:

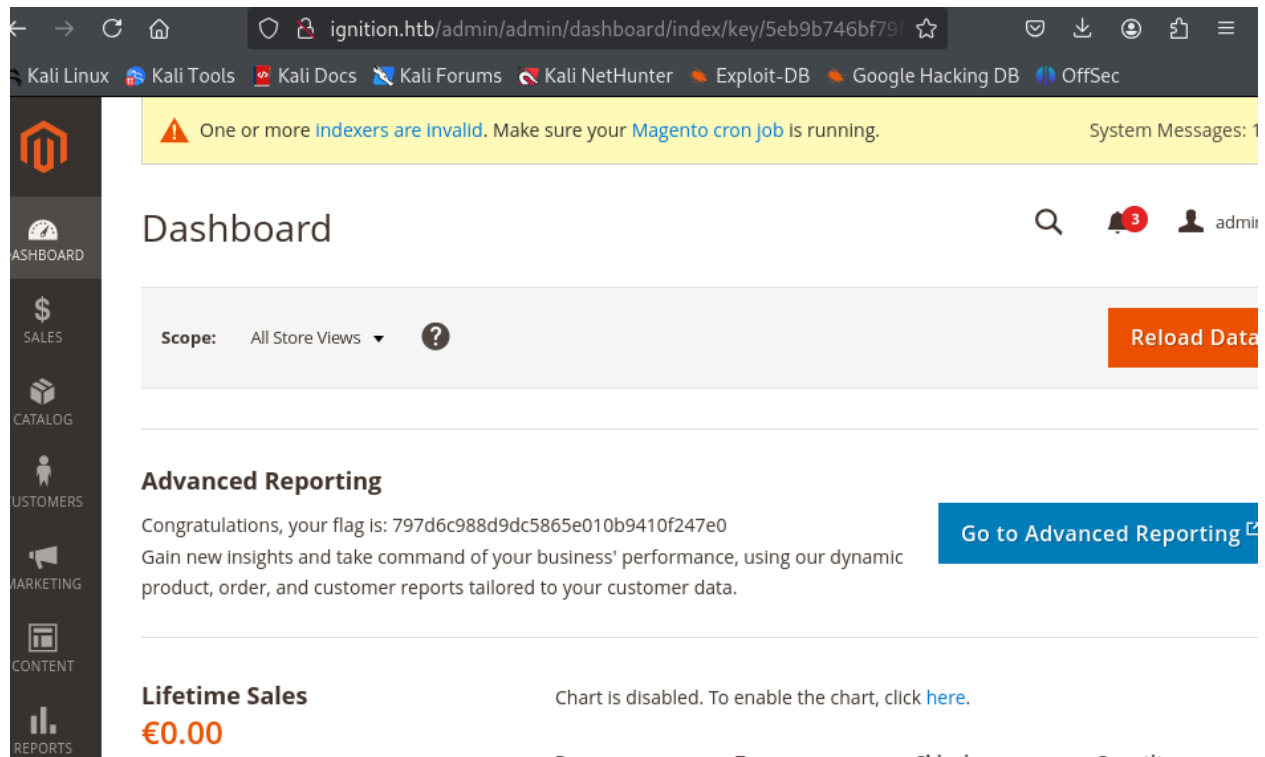
46	qwerty123	302	2
----	-----------	-----	---

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



Now we stop the attack and we are going to log in



The screenshot shows the Magento 2 Admin Dashboard in a web browser. The address bar displays the URL: `ignition.htb/admin/admin/dashboard/index/key/5eb9b746bf79`. The browser's bookmark bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. A yellow system message banner at the top states: "One or more **Indexers** are **Invalid**. Make sure your **Magento cron job** is running." The dashboard header includes a search icon, a notification bell with 3 alerts, and the user profile "admin". The left sidebar contains navigation links: DASHBOARD, SALES, CATALOG, CUSTOMERS, MARKETING, CONTENT, and REPORTS. The main content area features a "Scope" dropdown set to "All Store Views" and a "Reload Data" button. Below this is the "Advanced Reporting" section, which displays a congratulatory message: "Congratulations, your flag is: 797d6c988d9dc5865e010b9410f247e0" and a button to "Go to Advanced Reporting". The "Lifetime Sales" section shows a value of "€0.00" and a note that the chart is disabled, with a link to enable it.

And there we have 😊

