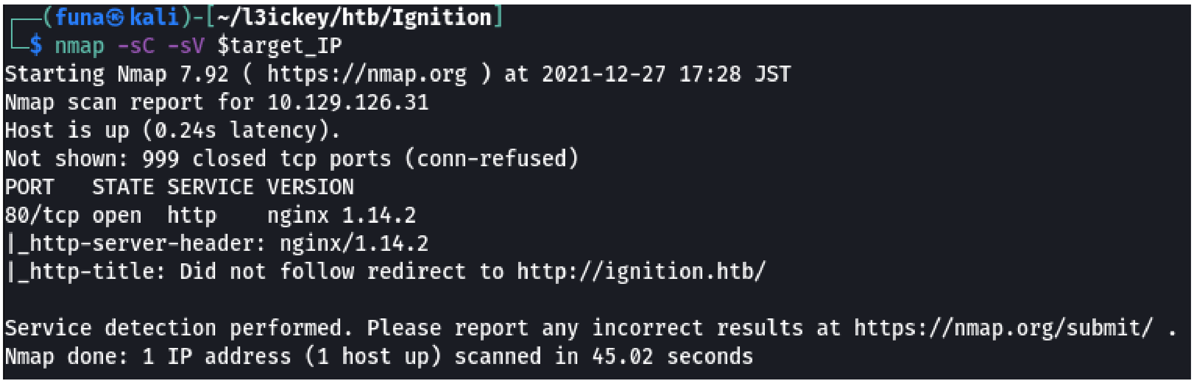
Ignition

Enumeration

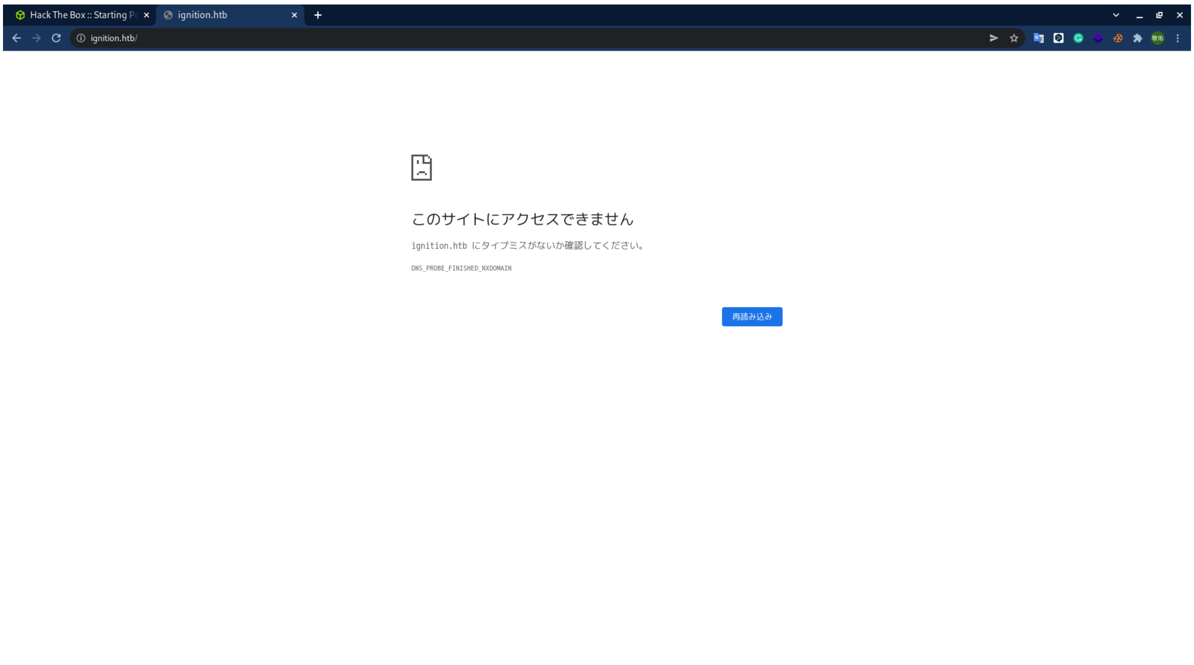
Starting off with an nmpa scan, we select the `-sC` and `-sV` switches to trigger default script scanning and version detection.



```
┌──(funa㉿kali)-[~/l3ickey/htb/Ignition]
└─$ nmap -sC -sV $target_IP
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-27 17:28 JST
Nmap scan report for 10.129.126.31
Host is up (0.24s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Did not follow redirect to http://ignition.htb/

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 45.02 seconds
```

Upon attempting to access the webpage through a browser window, we are presented with the following error.

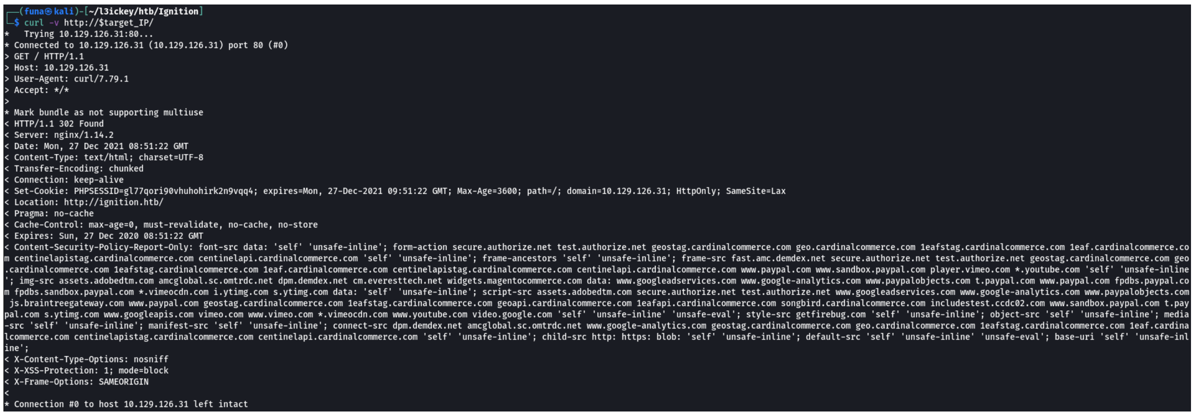


このサイトにアクセスできません

ignition.htb にタイプミスがないか確認してください。

DNS_PROBE_FINISHED_NXDOMAIN

`cURL` will allow us to manipulate HTTP requests make to a server and receive the responses directly in the terminal, without the latter being interpreted by our browser as generic error messages such as in the example above.



```
┌──(funa㉿kali)-[~/l3ickey/htb/Ignition]
└─$ curl -v http://$target_IP/
*   Trying 10.129.126.31:80...
* Connected to 10.129.126.31 (10.129.126.31) port 80 (#0)
> GET / HTTP/1.1
> Host: 10.129.126.31
> User-Agent: curl/7.79.1
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 302 Found
< Server: nginx/1.14.2
< Date: Mon, 27 Dec 2021 08:51:22 GMT
< Content-Type: text/html; charset=UTF-8
< Transfer-Encoding: chunked
< Connection: keep-alive
< Set-Cookie: PHPSESSID=gl77qori90vhuhohirk2n9vqq4; expires=Mon, 27-Dec-2021 09:51:22 GMT; Max-Age=3600; path=/; domain=10.129.126.31; HttpOnly; SameSite=Lax
< Location: http://ignition.htb/
< Pragma: no-cache
< Cache-Control: max-age=0, must-revalidate, no-cache, no-store
< Expires: Sun, 27 Dec 2020 08:51:22 GMT
< Content-Security-Policy-Report-Only: font-src data: 'self' 'unsafe-inline'; form-action secure.authorize.net test.authorize.net geostag.cardinalcommerce.com geo.cardinalcommerce.com 1eafstag.cardinalcommerce.com 1eaf.cardinalcommerce.co
m centinelapistag.cardinalcommerce.com centinelapi.cardinalcommerce.com 'self' 'unsafe-inline'; frame-ancestors 'self' 'unsafe-inline'; frame-src fast.amc.demdex.net secure.authorize.net test.authorize.net geostag.cardinalcommerce.com geo
.cardinalcommerce.com 1eafstag.cardinalcommerce.com 1eaf.cardinalcommerce.com centinelapistag.cardinalcommerce.com centinelapi.cardinalcommerce.com www.paypal.com www.sandbox.paypal.com player.vimeo.com *.youtube.com 'self' 'unsafe-inline
'; img-src assets.adobedtm.com amcglobal.sc.omtrdc.net dpm.demdex.net cm.everesttech.net widgets.magentocommerce.com data: www.googleadservices.com www.google-analytics.com www.paypalobjects.com t.paypal.com www.paypal.com fpdbs.paypal.co
m fpdbs.sandbox.paypal.com *.vimeocdn.com i.ytimg.com s.ytimg.com data: 'self' 'unsafe-inline'; script-src assets.adobedtm.com secure.authorize.net test.authorize.net www.googleadservices.com www.google-analytics.com www.paypalobjects.com
 js.braintreegateway.com www.paypal.com geostag.cardinalcommerce.com 1eafstag.cardinalcommerce.com geoapi.cardinalcommerce.com 1eafapi.cardinalcommerce.com songbird.cardinalcommerce.com includestest.ccdc02.com www.sandbox.paypal.com t.pay
pal.com s.ytimg.com www.googleapis.com vimeo.com www.vimeo.com *.vimeocdn.com www.youtube.com video.google.com 'self' 'unsafe-inline' 'unsafe-eval'; style-src getfirebug.com 'self' 'unsafe-inline'; object-src 'self' 'unsafe-inline'; media
-src 'self' 'unsafe-inline'; manifest-src 'self' 'unsafe-inline'; connect-src dpm.demdex.net amcglobal.sc.omtrdc.net www.google-analytics.com geostag.cardinalcommerce.com geo.cardinalcommerce.com 1eafstag.cardinalcommerce.com 1eaf.cardina
lcommerce.com centinelapistag.cardinalcommerce.com centinelapi.cardinalcommerce.com 'self' 'unsafe-inline'; child-src http: https: blob: 'self' 'unsafe-inline'; default-src 'self' 'unsafe-inline' 'unsafe-eval'; base-uri 'self' 'unsafe-inl
ine';
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< X-Frame-Options: SAMEORIGIN
<
* Connection #0 to host 10.129.126.31 left intact
```

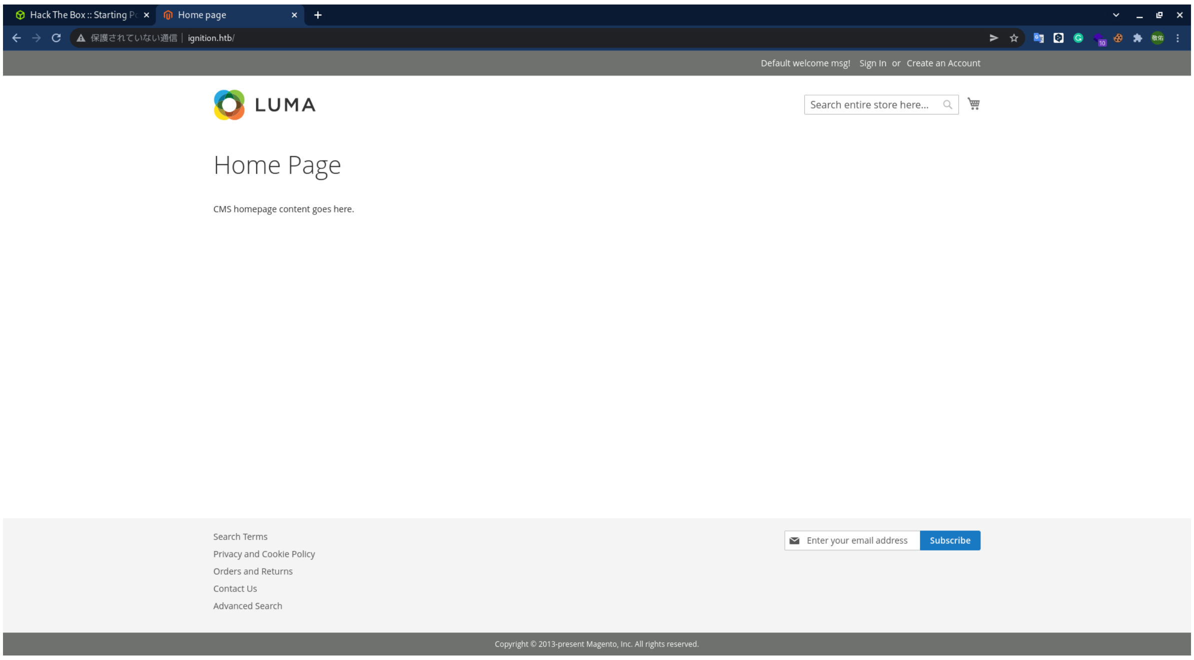
As observed from the screenshot above, our request contains a `Host` field which is home to the target's IP address instead of the hostname. The `302 Found` response, together with the `Location` header, indicates that the resource we requested (`/`) has been (temporarily) moved to `http://ignition.htb/`.

To solve the issue we are currently facing here, we will modify our local DNS file named `hosts` located in the `/etc` directory.

```
$ echo "{target_IP} ignition.htb" | sudo tee -a /etc/hosts
$ cat /etc/hosts
{target_IP} ignition.htb
```

Reading the `/etc/hosts` file of your Linux system should return an entry for `ignition.htb` with the associated target IP address.

Once this configuration is complete, we can proceed to reload the target's webpage and verify if it loads successfully.


Hack The Box :: Starting P
Home page
保護されていない通信 | ignition.htb/
Default welcome msg! Sign In or Create an Account
LUMA
Search entire store here...

Home Page

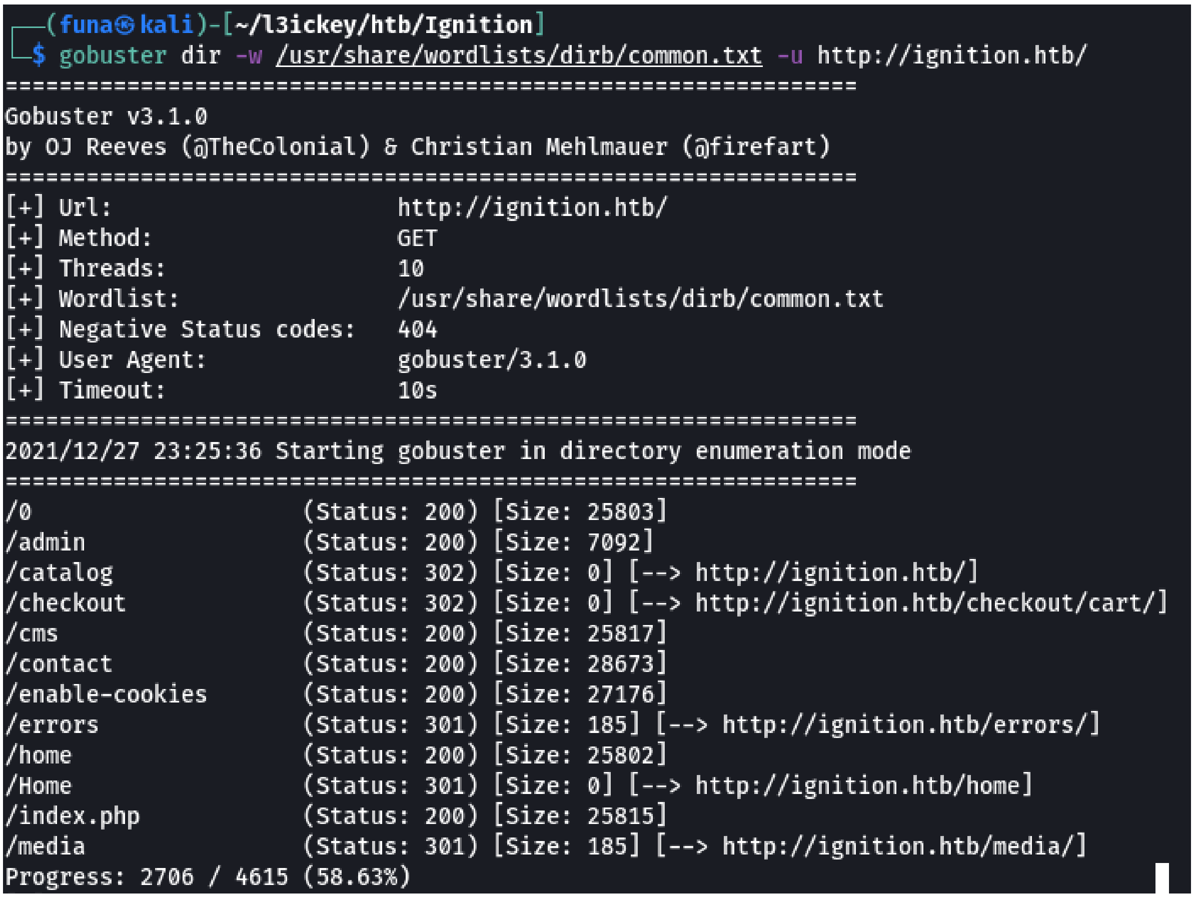
CMS homepage content goes here.

Search Terms
Privacy and Cookie Policy
Orders and Returns
Contact Us
Advanced Search
Enter your email address
Subscribe

Copyright © 2013-present Magento, Inc. All rights reserved.

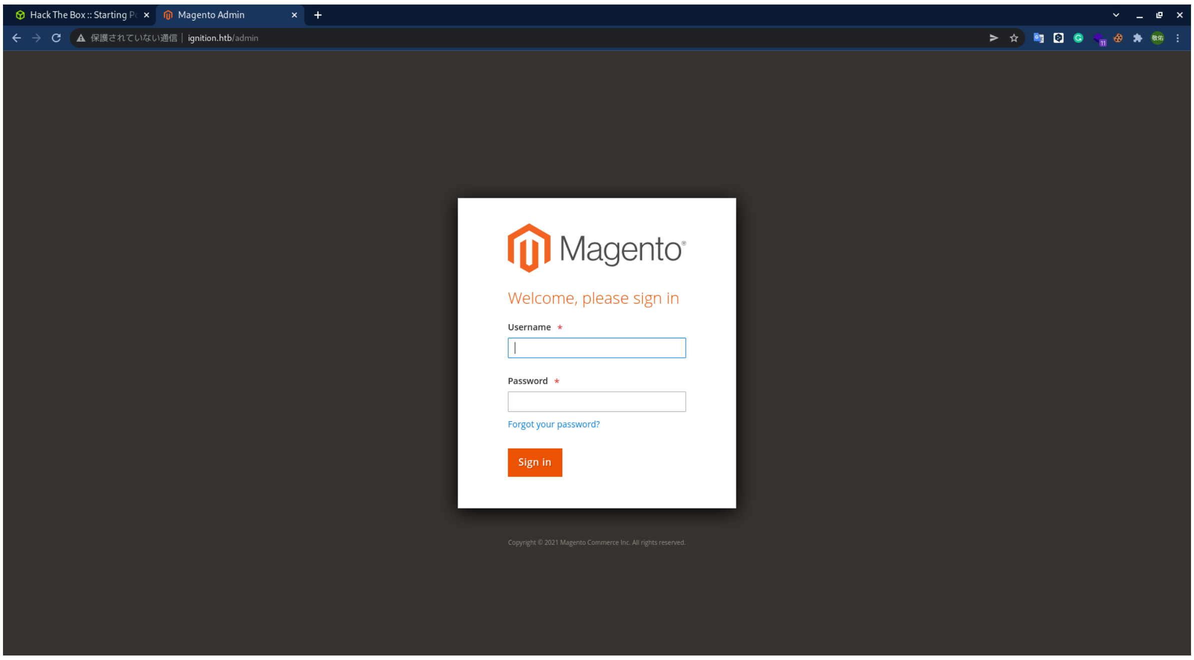
Foothold

After exploring the landing page for a short period of time, we can deduce that nothing helpful can be leveraged here. The only option of exploring the website further is using gobuster.



```
┌──(funa㉿kali)-[~/l3ickey/htb/Ignition]
└─$ gobuster dir -w /usr/share/wordlists/dirb/common.txt -u http://ignition.htb/
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://ignition.htb/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/12/27 23:25:36 Starting gobuster in directory enumeration mode
===============================================================
/0                    (Status: 200) [Size: 25803]
/admin                (Status: 200) [Size: 7092]
/catalog              (Status: 302) [Size: 0] [--> http://ignition.htb/]
/checkout             (Status: 302) [Size: 0] [--> http://ignition.htb/checkout/cart/]
/cms                  (Status: 200) [Size: 25817]
/contact              (Status: 200) [Size: 28673]
/enable-cookies       (Status: 200) [Size: 27176]
/errors               (Status: 301) [Size: 185] [--> http://ignition.htb/errors/]
/home                 (Status: 200) [Size: 25802]
/Home                 (Status: 301) [Size: 0] [--> http://ignition.htb/home]
/index.php            (Status: 200) [Size: 25815]
/media                (Status: 301) [Size: 185] [--> http://ignition.htb/media/]
Progress: 2706 / 4615 (58.63%)
```

From the output of our gobuster script, we find our target. The `/admin` page returns a 200 response code, signalling its' availability. We can navigate to it by appending it to the end of the URL: `http://ignition.htb/admin`.



Hack The Box :: Starting P
Magento Admin
保護されていない通信 | ignition.htb/admin
Magento

Welcome, please sign in

Username *

Password *

Forgot your password?
Sign in

Copyright © 2021 Magento Commerce Inc. All rights reserved.

According to the documentation, we should not attempt to brute force this login form because it has antibruteforce measures implemented, we will need to guess the password. Since the password must be seven or more characters long & to include both letters ad numbers, we can attempt to use the most common passwords of the year 2021 as well as a common username, such as `admin`. From the [list](), only the following password fulfils the requirements.

```
admin admin123
admin root123
admin password1
admin administrator1
admin changeme1
admin password123
admin qwerty123
admin administrator123
admin changeme123
```

After manually attempting a number of these credentials, we land on a successful login. The correct combinationis : `admin:qwerty123`.

Congratulations!