

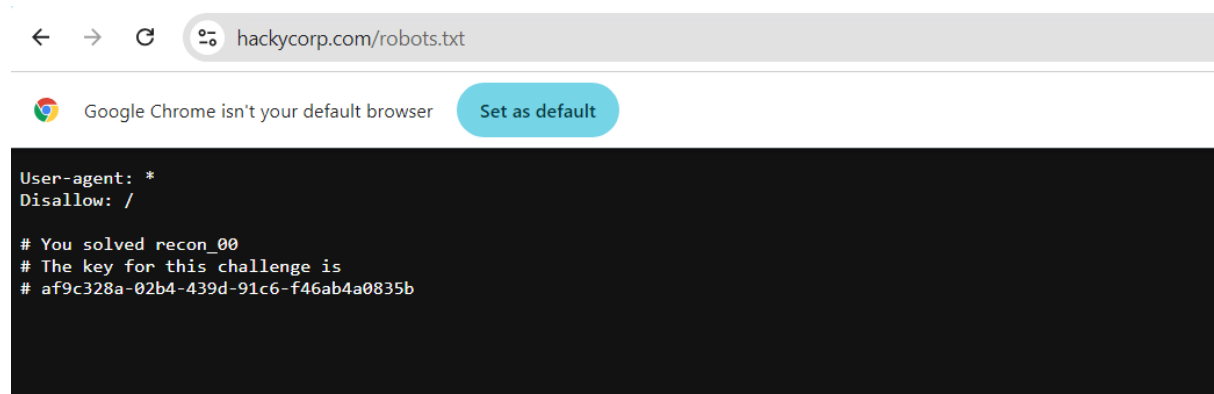
DAY-02 CyberSecurity

Challenge recon 0:

Objective

For this challenge, our goal is to retrieve the robots.txt from the main website for hackycorp.com.

Sol: For this we have to add /robots.txt at the end of main website hackycorp.com

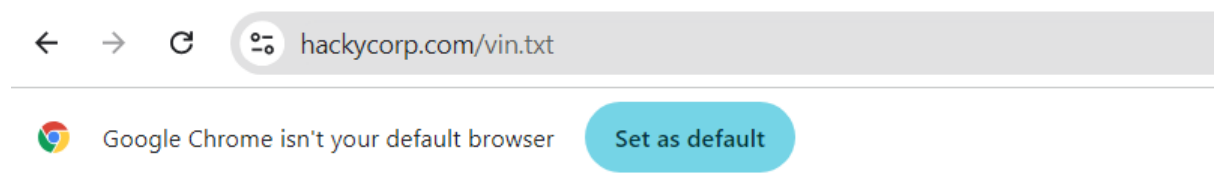


Challenge Recon 01:

Objective

For this challenge, our goal is to generate a 404/"Not Found" error on the main website for hackycorp.com.

Sol: For this we have to add /vin.txt or any name at the end of the main web site hackycorp.com



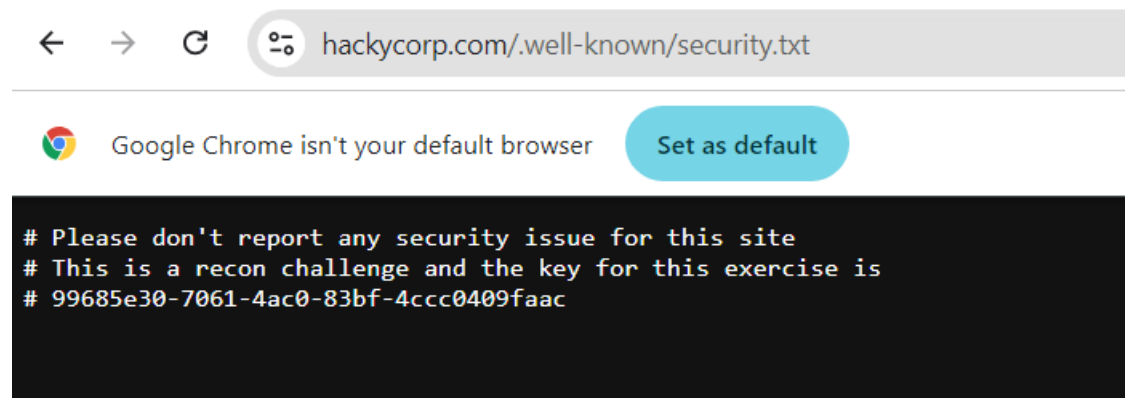
The key for this challenge is: aeae57f-2a82-41da-bc4c-d081c8cddfc8

Challenge Recon 03:

Objective

For this challenge, our goal is to retrieve the security.txt from the main website for hackycorp.com.

Sol: For this objective we have to add /.well-known/security.txt at the end of main website hackycorp.com

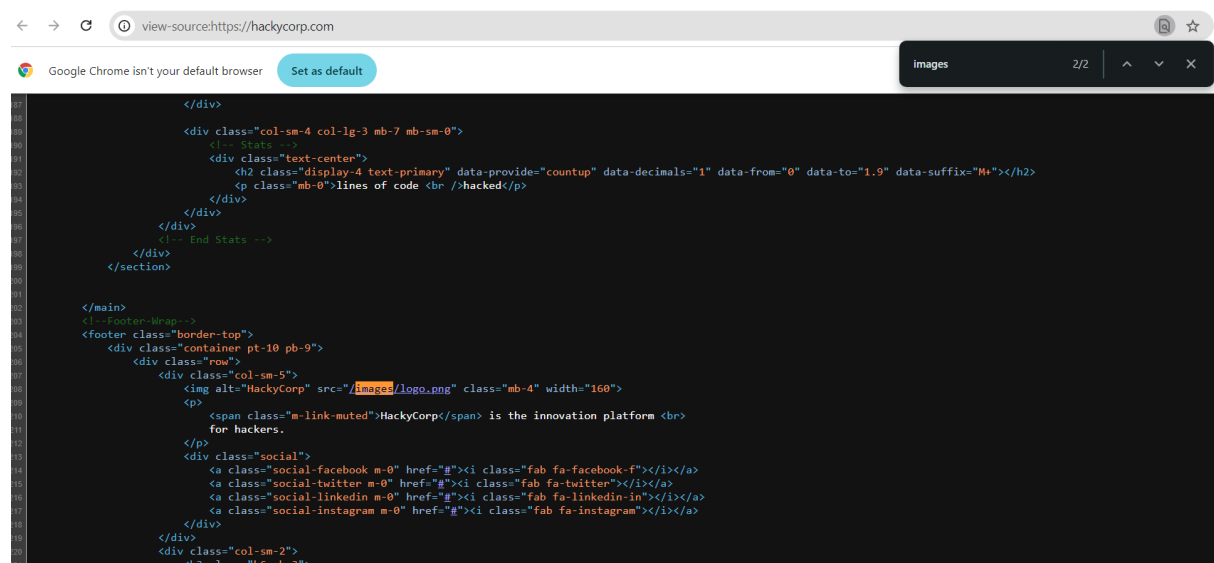


Challenge Recon 03:

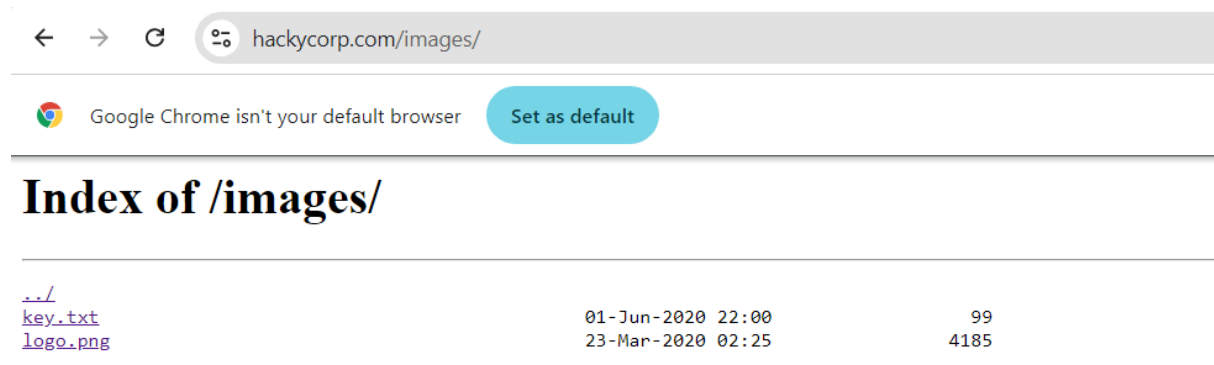
Objective

For this challenge, our goal is to find a directory with directory listing in the main website for hackycorp.com.

Sol: In main website we have to open and we have to go the view page source and in that we have to find out images.



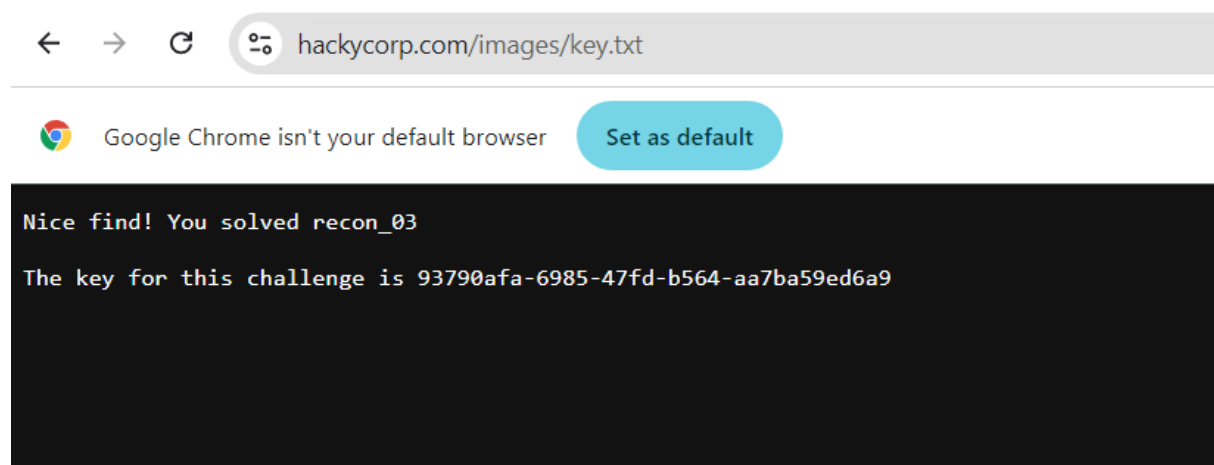
And we have to go images directory there we get the key.txt file and next we have to open that key.txt and we solved the challenge.



The screenshot shows a web browser with the address bar at `hackycorp.com/images/`. Below the browser interface, a directory listing is displayed with the title "Index of /images/". The listing contains three entries: `../`, `key.txt`, and `logo.png`. The `key.txt` entry shows a modification date of "01-Jun-2020 22:00" and a size of "99". The `logo.png` entry shows a modification date of "23-Mar-2020 02:25" and a size of "4185".

../		
key.txt	01-Jun-2020 22:00	99
logo.png	23-Mar-2020 02:25	4185

The below image is after selecting key.txt



Challenge Recon 04:


Objective

For this challenge, our goal is to find a directory that is commonly used to manage applications.

Sol: My goal was to locate such a directory on hackycorp.com.

I entered this URL in the browser:

- <http://hackycorp.com/admin/>

← → ↻  hackycorp.com/admin/



Google Chrome isn't your default browser

Set as default

Well done! You solved recon_04

The key for this exercise is: ad1d44d6-ab73-4640-8291-c5bf2343e2a5

Challenge Recon 05:

Objective:

Find a directory that is not directly accessible on the main website for hackycorp.com.

Sol: In kali linux :search for dirbuster

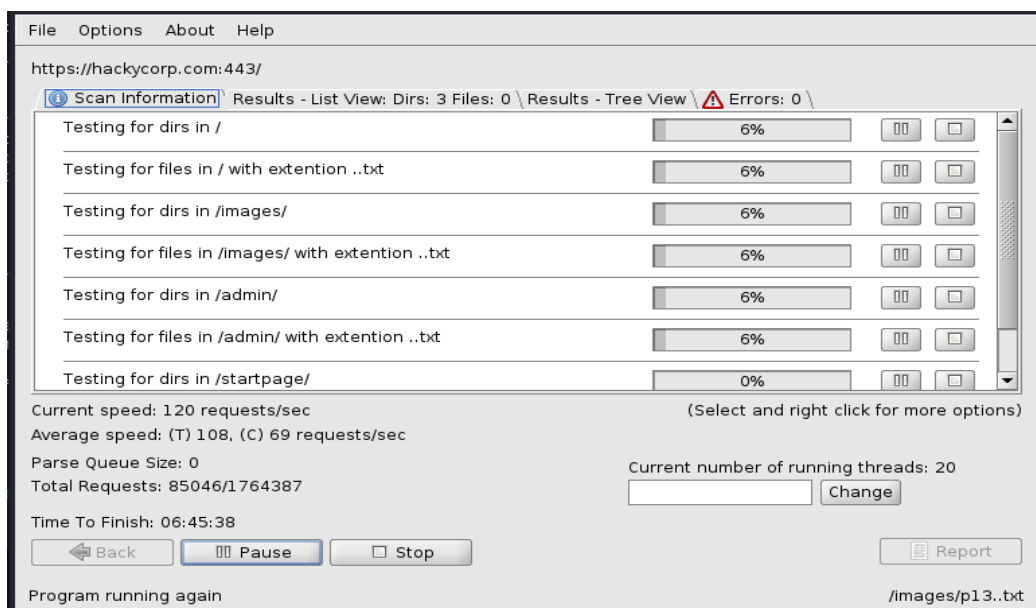
Type url: <http://hackycorp.com/>

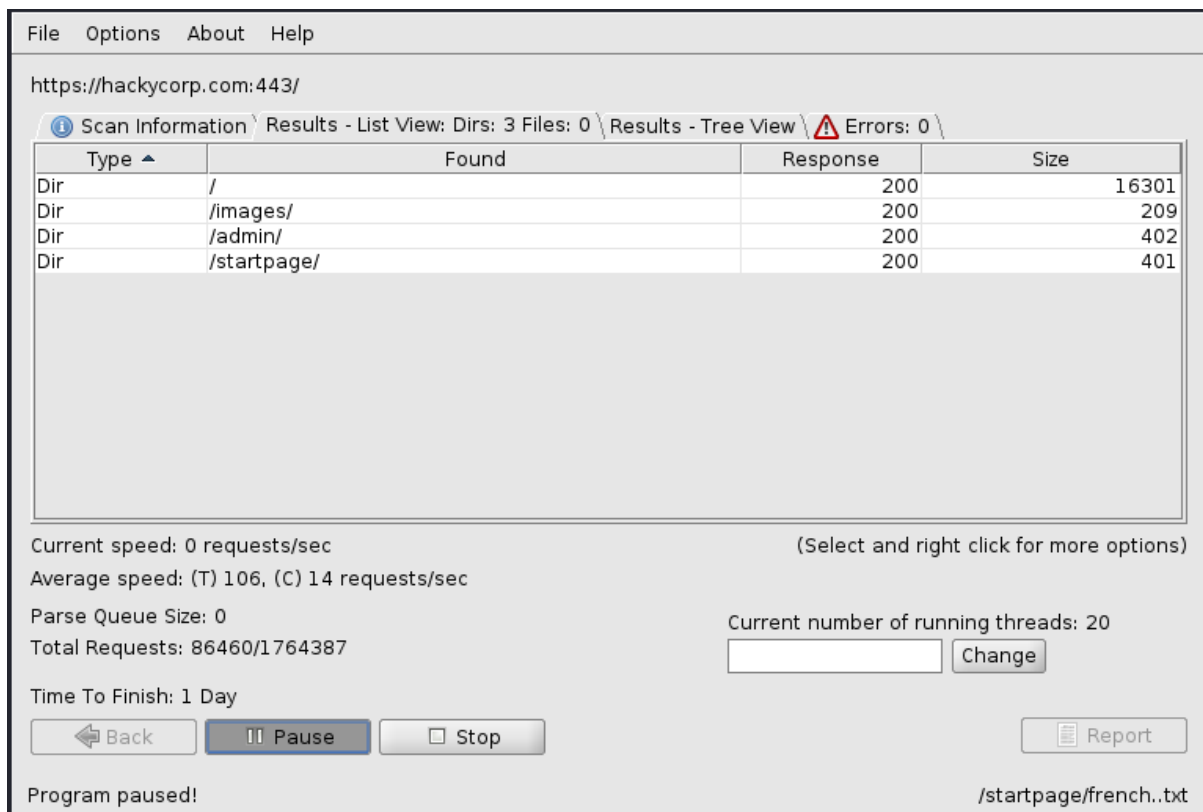
Remove extension Uncheck brute force files

Check brute force dirs.

Browse /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Start it and wait for completion Then check results ...stop



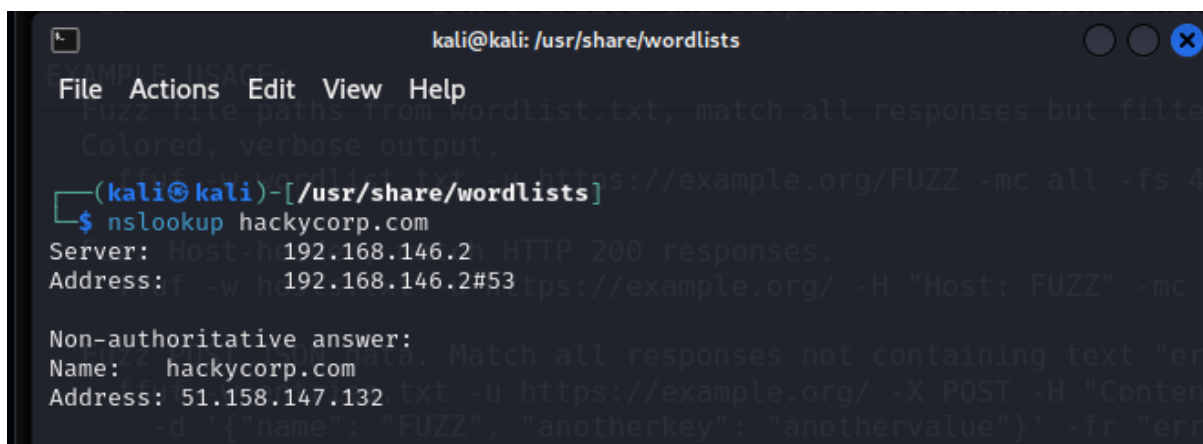


Challenge Recon 06:

Objective

For this challenge, our goal is to access the default virtual host ("vhost").

Sol:



```
(kali㉿kali)-[/usr/share/wordlists]
$ curl http://51.158.147.132
<h1>Well done! You solved recon_06 </h1>
More information and examples: https://github.com/ffuf/ffuf
The key for this exercise is 5cf83b5d-eb6c-4eee-af6c-945f9aed8dfd
```

Challenge Recon 07:

Objective

For this challenge, our goal is to access the default virtual host ("vhost") over TLS.

Sol: `curl -v -k https://51.158.147.132`

```
kali@kali: /usr/share/wordlists
File Actions Edit View Help

(kali㉿kali)-[/usr/share/wordlists]
$ curl -v -k https://51.158.147.132

* Trying 51.158.147.132:443 ...
* Connected to 51.158.147.132 (51.158.147.132) port 443
* GnuTLS ciphers: NORMAL:-ARCFOUR-128:-CTYPE-ALL:+CTYPE-X509:-VERS-SSL3.0
* SSL connection using TLS1.2 / ECDHE_RSA_CHACHA20_POLY1305
* server certificate verification SKIPPED
* server certificate status verification SKIPPED
* common name: hackycorp.com (does not match '51.158.147.132')
* server certificate expiration date OK
* server certificate activation date OK
* certificate public key: RSA
* certificate version: #3
* subject: CN=hackycorp.com
* start date: Sun, 08 Sep 2024 16:33:59 GMT
* expire date: Sat, 07 Dec 2024 16:33:58 GMT
* issuer: C=US,O=Let's Encrypt,CN=R11
* ALPN: server accepted http/1.1
* using HTTP/1.x
> GET / HTTP/1.1
> Host: 51.158.147.132
> User-Agent: curl/8.8.0
> Accept: */*
>
* Request completely sent off
```

```
kali@kali: /usr/share/wordlists
File Actions Edit View Help
* issuer: C=US,O=Let's Encrypt,CN=R11
* ALPN: server accepted http/1.1
* using HTTP/1.x
> GET / HTTP/1.1
> Host: 51.158.147.132
> User-Agent: curl/8.8.0
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Server: nginx
< Date: Tue, 24 Sep 2024 09:36:57 GMT
< Content-Type: text/html
< Content-Length: 107
< Last-Modified: Wed, 01 Apr 2020 03:25:09 GMT
< Connection: keep-alive
< ETag: "5e840995-6b"
< pentesterlab_recon_09: 99d0738b-1e52-4a00-8885-b15894b2c79e
< Accept-Ranges: bytes
<
<h1>Well done! You solved recon_07</h1>

The key for this exercise is 23eafa56-6d55-4b78-8307-24e7dc2ce5e6
* Connection #0 to host 51.158.147.132 left intact

(kali@kali)-[/usr/share/wordlists]
$
```

Challenge Recon 08:

Objective

For this challenge, our goal is to access the alternative names in the certificate.

Sol: Get the SANs using openssl

Then curl one of the SANs and 3 DNS under one SSL certificate

66177e3f25e3ea0713807b1dc5f0b9df .hackycorp.com 51.158.147.132

```
kali@kali: /usr/share/wordlists
File Actions Edit View Help
<h1>Well done! You solved recon_07</h1>

The key for this exercise is 23eafa56-6d55-4b78-8307-24e7dc2ce5e6
* Connection #0 to host 51.158.147.132 left intact

(kali@kali)-[/usr/share/wordlists]
$ openssl s_client -connect 51.158.147.132:443 </dev/null | openssl x509 -t
ext | grep -A 1 "Subject Alternative Name"
Connecting to 51.158.147.132
Can't use SSL_get_servername
depth=2 C=US, O=Internet Security Research Group, CN=ISRG Root X1
verify return:1
depth=1 C=US, O=Let's Encrypt, CN=R11
verify return:1
depth=0 CN=hackycorp.com
verify return:1
DONE
```

```
kali@kali: /usr/share/wordlists
File Actions Edit View Help

(kali@kali)-[/usr/share/wordlists]
$ curl -k https://66177e3f25e3ea0713807b1dc5f0b9df.hackycorp.com -v
* Host 66177e3f25e3ea0713807b1dc5f0b9df.hackycorp.com:443 was resolved.
* IPv6: (none)
* IPv4: 51.158.147.132
* Trying 51.158.147.132:443 ...
* Connected to 66177e3f25e3ea0713807b1dc5f0b9df.hackycorp.com (51.158.147.132)
  port 443
* GnuTLS ciphers: NORMAL:-ARCFOUR-128:-CTYPE-ALL:+CTYPE-X509:-VERS-SSL3.0
* SSL connection using TLS1.2 / ECDHE_RSA_CHACHA20_POLY1305
*  server certificate verification SKIPPED
*  server certificate status verification SKIPPED
*  common name: hackycorp.com (matched)
*  server certificate expiration date OK
*  server certificate activation date OK
*  certificate public key: RSA
*  certificate version: #3
*  subject: CN=hackycorp.com
*  start date: Sun, 08 Sep 2024 16:33:59 GMT
*  expire date: Sat, 07 Dec 2024 16:33:58 GMT
*  issuer: C=US,O=Let's Encrypt,CN=R11
* ALPN: server accepted http/1.1
* using HTTP/1.x
> GET / HTTP/1.1
> Host: 66177e3f25e3ea0713807b1dc5f0b9df.hackycorp.com
> User-Agent: curl/8.8.0
> Accept: */*
```



```
kali@kali: /usr/share/wordlists
File Actions Edit View Help
* ALPN: server accepted http/1.1
* using HTTP/1.x
> GET / HTTP/1.1
> Host: 66177e3f25e3ea0713807b1dc5f0b9df.hackycorp.com -showcerts
> User-Agent: curl/8.8.0
> Accept: */*
>
* Request completely sent off to the server and displays the SSL certificate chain, including
< HTTP/1.1 200 OK
< Server: nginx
< Date: Tue, 24 Sep 2024 09:56:35 GMT
< Content-Type: text/html
< Content-Length: 110
< Last-Modified: Wed, 01 Apr 2020 02:56:32 GMT
< Connection: keep-alive
< ETag: "5e8402e0-6e"
< pentesterlab_recon_09: 99d0738b-1e52-4a00-8885-b15894b2c79e
< Accept-Ranges: bytes
<
<h1>Well done! You solved recon_08</h1>

The key for this exercise is: 1763ec4f-8467-47f7-9a80-6de93a1a2253. Let me know
* Connection #0 to host 66177e3f25e3ea0713807b1dc5f0b9df.hackycorp.com left intact

(kali@kali)-[/usr/share/wordlists]
$
```

Challenge Recon 09:

Objective

For this challenge, our goal is to access the headers from responses.

Sol: curl <https://hackycorp.com> -I

```
kali@kali: ~
File Actions Edit View Help
js"></script>

<script src="//assets.hackycorp.com/js/other.js"></script>
<script src="//assets.hackycorp.com/js/page.js"></script>
<script src="//assets.hackycorp.com/js/script.js"></script>

<!-- Theme Custom -->
<script src="//assets.hackycorp.com/js/custom.js"></script>
</body>
</html>

(kali@kali)-[~]
$ curl https://hackycorp.com -I
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 24 Sep 2024 10:31:37 GMT
Content-Type: text/html
Content-Length: 16011
Last-Modified: Tue, 31 Mar 2020 03:12:16 GMT
Connection: keep-alive
ETag: "5e82b510-3e8b"
pentesterlab_recon_09: 99d0738b-1e52-4a00-8885-b15894b2c79e
Accept-Ranges: bytes

(kali@kali)-[~]
$
```

