

Web Information Gather HTB

vHosts needed for these questions:

- inlanefreight.htb

+ 1

What is the IANA ID of the registrar of the inlanefreight.com domain?

- to find this what we can do is run `whois`

```
whois inlanefreight.com | grep "IANA ID"
```

```
[us-academy-4]-[10.10.15.112]-[htb-ac-1326293@htb-emddjjl2bv]-[~]
-- [★]$ whois inlanefreight.com | grep "IANA ID"
Registrar IANA ID: 132
Registrar IANA ID: 132
```

+ 1

What http server software is powering the inlanefreight.htb site on the target system? Respond with the name of the software, not the version, e.g., Apache.

Submit your answer here...

- to complete this we can use a tool like `whatweb`

```
[us-academy-4]-[10.10.15.112]-[htb-ac-1326293@htb-emddjjl2bv]-[~]
-- [★]$ whatweb http://inlanefreight.htb:32546/
```

```
[us-academy-4]-[10.10.15.112]-[htb-ac-1326293@htb-emddjjl2bv]-[~]
-- [★]$ whatweb http://inlanefreight.htb:32546/
http://inlanefreight.htb:32546/ [200 OK] Country[FINLAND][FI], HTML5, HTTPServer
[94.237.48.12], IP[94.237.48.12], Title[inlanefreight], [94.237.48.12]
```

+ 1

What is the API key in the hidden admin directory that you have discovered on the target system?

- Run VHOST Scan:

```
gobuster vhost -u http://inlanefreight.htb:32546 -w subdomains-top1million-110000.txt --append-domain
```

```
[+] Append Domain: true
=====
Starting gobuster in VHOST enumeration mode
=====
Found: web inlanefreight.htb:32546 Status: 200 [Size: 104]
Progress: 114441 / 114442 (100.00%)
=====
Finished
```

USE Curl to Navigate and Check The Site:

```
—[us-academy-4]—[10.10.15.112]—[htb-ac-1326293@htb-8mfc7imjzh]—[/root]
└── [★]$ curl -i http://web1337.inlanefreight.htb:32546/robots.txt
```

- Check if Robots.txt has anything.

```
User-agent: *
Allow: /index.html
Allow: /index-2.html
Allow: /index-3.html
Disallow: /admin_h1dd3n
```

+ 4 📦

After crawling the inlanefreight.htb domain on the target system, what is the email address you have found? Respond with the full email, e.g., mail@inlanefreight.htb.

- we will need to use the python webcrawler `scrapy`

```
—[us-academy-4]—[10.10.15.112]—[htb-ac-1326293@htb-8mfc7imjzh]—[~]
└── [★]$ pip3 install scrapy

—[us-academy-4]—[10.10.15.112]—[htb-ac-1326293@htb-8mfc7imjzh]—[~]
└── [★]$ wget -O ReconSpider.zip https://academy.hackthebox.com/storage/modules/144/ReconSpider.v1.2.zip
--2025-05-07 14:38:50-- https://academy.hackthebox.com/storage/modules/144/ReconSpider.v1.2.zip
Resolving academy.hackthebox.com (academy.hackthebox.com)... 109.176.239.69, 109.176.239.70
Connecting to academy.hackthebox.com (academy.hackthebox.com)|109.176.239.69|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1706 (1.7K) [application/zip]
Saving to: 'ReconSpider.zip'

ReconSpider.zip      100%[=====
======>]  1.67K  --.-KB/s   in 0s

2025-05-07 14:38:51 (17.4 MB/s) - 'ReconSpider.zip' saved [1706/1706]

└── [us-academy-4]—[10.10.15.112]—[htb-ac-1326293@htb-8mfc7imjzh]—[~]
└── [★]$ unzip ReconSpider.zip
Archive: ReconSpider.zip
  inflating: ReconSpider.py
```

```
—[us-academy-4]—[10.10.15.112]—[htb-ac-1326293@htb-8mfc7imjzh]—[/usr/share/wordlists/seclists/Discover
y/DNS]
└── [★]$ gobuster vhost -u http://web1337.inlanefreight.htb:32546 -w subdomains-top1million-110000.txt -
-append-domain

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====

[+] Url:      http://web1337.inlanefreight.htb:32546
[+] Method:   GET
[+] Threads:  10
```

```
[+] Wordlist:      subdomains-top1million-110000.txt
[+] User Agent:   gobuster/3.6
[+] Timeout:     10s
[+] Append Domain: true

=====
Starting gobuster in VHOST enumeration mode
=====
Found: XXX.webXXXX.inlanefreight.htb:32546 Status: 200 [Size: 123]
Progress: 488 / 114442 (0.43%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 525 / 114442 (0.46%)

=====
Finished
=====
```

- using this result we can again curl the site and vist it.

```
tb-ac-1326293@htb-8mfc7imjzh]—[/usr/share/wordlists/seclists/Discovery/DNS]
└─ [★]$ curl -i http://dev.web1337.inlanefreight.htb:32546/robots.txt
```

- noticed a werid hyperlink:

```
Content-Length: 123
Last-Modified: Thu, 01 Aug 2024 09:35:23 GMT
Connection: keep-alive
ETag: "66ab56db-7b"
Accept-Ranges: bytes

<!DOCTYPE html><html><head><title>Page 1</title></head><body><h1>Page 1</h1><a href="index-334.html">Next</a>
tb-ac-1326293@htb-8mfc7imjzh]—[/usr/share/wordlists/seclists/Discovery/DNS]
```

- lets visit that endpoint
- it was like never ending loop so lets let the recon spider do it's thing.
 - from this i could solve last to lab with it.