Tier II Easy Offensive

This module equips learners with essential web reconnaissance skills, crucial for ethical hacking and penetration testing. It explores both active and passive techniques, including DNS enumeration, web crawling, analysis of web archives and HTTP headers, and fingerprinting web technologies.

By Saezel

Last Updated: 26 October 2024

Utilising WHOIS

Perform a WHOIS lookup against the paypal.com domain. What is the registrar Internet Assigned Numbers Authority (IANA) ID number?

Answer: 292

```
$ whois paypal.com
        Domain Name: PAYPAL.COM
        Registry Domain ID: 8017040_DOMAIN_COM-VRSN
        Registrar WHOIS Server: whois.markmonitor.com
        Registrar URL: http://www.markmonitor.com
        Updated Date: 2024-10-08T21:00:07Z
        Creation Date: 1999-07-15T05:32:11Z
        Registry Expiry Date: 2025-07-15T05:32:11Z
        Registrar: MarkMonitor Inc.
        Registrar IANA ID: 292
```

What is the admin email contact for the tesla.com domain (also in-scope for the Tesla bug bounty program)?

Answer: admin@dnstinations.com

```
$ whois tesla.com
        Domain Name: TESLA.COM
      ....
      Admin Name: Domain Administrator
      Admin Organization: DNStination Inc.
      Admin Street: 3450 Sacramento Street, Suite 405
      Admin City: San Francisco
      Admin State/Province: CA
      Admin Postal Code: 94118
      Admin Country: US
      Admin Phone: +1.4155319335
      Admin Phone Ext:
      Admin Fax: +1.4155319336
      Admin Fax Ext:
      Admin Email: admin@dnstinations.com
```

Digging DNS

Which IP address maps to inlanefreight.com?

Answer: 134.209.24.248

```
$ dig inlanefreight.com

        ;; ANSWER SECTION:

        inlanefreight.com.    300    IN    A     134.209.24.248
```

Which domain is returned when querying the PTR record for 134.209.24.248?

Answer: inlanefreight.com

```
$ dig -x 134.209.24.248

;; ANSWER SECTION:

248.24.209.134.in-addr.arpa. 1800 IN    PTR    inlanefreight.com.
```

What is the full domain returned when you query the mail records for facebook.com?

Answer: smtpin.vvv.facebook.com

```
$ dig MX facebook.com

;; ANSWER SECTION:

facebook.com.        623    IN    MX    10 smtpin.vvv.facebook.com.
```

Subdomain Bruteforcing

Using the known subdomains for inlanefreight.com (www, ns1, ns2, ns3, blog, support, customer), find any missing subdomains by brute-forcing possible domain names. Provide your answer with the complete subdomain, e.g., www.inlanefreight.com.

Answer: my.inlanefreight.com

```
$ locate seclist | grep "subdomain"
....
/usr/share/seclists/Discovery/DNS/subdomains-spanish.txt
/usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
/usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt
/usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
```

```
$ dnsenum --enum inlanefreight.com -f /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -r
Google Results:
_________________

blog.inlanefreight.com.          300    IN    A     134.209.24.248

Brute forcing with /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt:
______________________________________________________________________________________

www.inlanefreight.com.           300    IN    A     134.209.24.248
ns1.inlanefreight.com.           300    IN    A     178.128.39.165
ns2.inlanefreight.com.           300    IN    A     206.189.119.186
ns3.inlanefreight.com.           300    IN    A     134.209.24.248
support.inlanefreight.com.       300    IN    A     134.209.24.248
my.inlanefreight.com.            300    IN    A     134.209.24.248
customer.inlanefreight.com.      300    IN    A     134.209.24.248
```

Only subdomain not specified in the question

DNS Zone Transfers

After performing a zone transfer for the domain inlanefreight.htb on the target system, how many DNS records are retrieved from the target system's name server? Provide your answer as an integer, e.g, 123.

Answer: 22

Within the zone record transferred above, find the ip address for ftp.admin.inlanefreight.htb. Respond only with the IP address, eg 127.0.0.1

Answer: 10.10.34.2

Within the same zone record, identify the largest IP address allocated within the 10.10.200 IP range. Respond with the full IP address, eg 10.10.200.1

Answer: 10.10.200.14

```
$ dig axfr inlanefreight.htb @10.129.44.226

; <<>> DiG 9.20.2-1-Debian <<>> axfr inlanefreight.htb @10.129.44.226
....
admin.inlanefreight.htb. 604800 IN      A       10.10.34.2
ftp.admin.inlanefreight.htb. 604800 IN  A       10.10.34.2
careers.inlanefreight.htb. 604800 IN    A       10.10.34.50
dc1.inlanefreight.htb.  604800  IN      A       10.10.34.16
....
test1.inlanefreight.htb. 604800 IN      A       10.10.34.101
us.inlanefreight.htb.   604800  IN      A       10.10.200.5
cluster14.us.inlanefreight.htb. 604800 IN A     10.10.200.14
messagecenter.us.inlanefreight.htb. 604800 IN A 10.10.200.10
....
;; WHEN: Fri Oct 18 22:36:05 EDT 2024
;; XFR size: 22 records (messages 1, bytes 594)
```

Virtual Hosts

Brute-force vhosts on the target system. What is the full subdomain that is prefixed with "web"? Answer using the full domain, e.g. "x.inlanefreight.htb"

Answer: web17611.inlanefreight.htb

Brute-force vhosts on the target system. What is the full subdomain that is prefixed with "vm"? Answer using the full domain, e.g. "x.inlanefreight.htb"

Answer: vm5.inlanefreight.htb

Brute-force vhosts on the target system. What is the full subdomain that is prefixed with "br"? Answer using the full domain, e.g. "x.inlanefreight.htb"

Answer: browse.inlanefreight.htb

Brute-force vhosts on the target system. What is the full subdomain that is prefixed with "a"? Answer using the full domain, e.g. "x.inlanefreight.htb"

Answer: admin.inlanefreight.htb

Brute-force vhosts on the target system. What is the full subdomain that is prefixed with "su"? Answer using the full domain, e.g. "x.inlanefreight.htb"

Answer: support.inlanefreight.htb

```
$ sudo nano /etc/hosts

ADD ENTRY:  94.237.54.229 inlanefreight.htb
```

```
$ sudo gobuster vhost -u http://inlanefreight.htb:57295 -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt --append-domain

...
Found: blog.inlanefreight.htb:57295 Status: 200 [Size: 98]
Found: support.inlanefreight.htb:57295 Status: 200 [Size: 104]
Found: forum.inlanefreight.htb:57295 Status: 200 [Size: 100]
Found: admin.inlanefreight.htb:57295 Status: 200 [Size: 100]
Found: vm5.inlanefreight.htb:57295 Status: 200 [Size: 96]
Found: browse.inlanefreight.htb:57295 Status: 200 [Size: 102]
Found: web17611.inlanefreight.htb:57295 Status: 200 [Size: 106]
...
```

Fingerprinting

Determine the Apache version running on app.inlanefreight.local on the target system. (Format: 0.0.0)

Answer: 2.4.41

Which CMS is used on app.inlanefreight.local on the target system? Respond with the name only, e.g., WordPress.

Answer: Joomla

```
$ whatweb -v -H "Host: app.inlanefreight.local" http://10.129.12.145
        WhatWeb report for http://10.129.12.145
        Status    : 200 OK
        Title     : Home
        IP        : 10.129.12.145
        Country   : RESERVED, ZZ

        Summary   : Apache[2.4.41], Bootstrap, Cookies[72af8f2b24261272e581a49f5c56de40],
        HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)],
        HttpOnly[72af8f2b24261272e581a49f5c56de40], JQuery, MetaGenerator[Joomla! -
        Open Source Content Management],
        OpenSearch[http://app.inlanefreight.local/index.php/component/search/?layout=blog&
        amp;id=9&amp;Itemid=101&amp;format=opensearch], Script,
        UncommonHeaders[permissions-policy]

        Detected Plugins:
        ...
        [ MetaGenerator ]
                This plugin identifies meta generator tags and extracts its
                value.

                String       : Joomla! - Open Source Content Management

        [ OpenSearch ]
                This plugin identifies open search and extracts the URL.
                OpenSearch is a collection of simple formats for the
                sharing of search results.
```

On which operating system is the dev.inlanefreight.local webserver running in the target system? Respond with the name only, e.g., Debian.

Answer: Ubuntu

```
$ curl -I -H "Host: dev.inlanefreight.local" http://10.129.12.145
        HTTP/1.1 200 OK
        Date: Tue, 22 Oct 2024 02:16:32 GMT
        Server: Apache/2.4.41 (Ubuntu)
        Set-Cookie: 02a93f6429c54209e06c64b77be2180d=kbcmmdubndufaoj81t5ij1hh9n; path=/; HttpOnly
        Expires: Wed, 17 Aug 2005 00:00:00 GMT
        Last-Modified: Tue, 22 Oct 2024 02:16:32 GMT
        Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
        Pragma: no-cache
        Content-Type: text/html; charset=utf-8
```

Creepy Crawlies

After spidering inlanefreight.com, identify the location where future reports will be stored. Respond with the full domain, e.g., files.inlanefreight.com.

Answer: inlanefreight-comp133.s3.amazonaws.htb

Prepare the environment to run ReconSpider

```
$ sudo apt install python3.12-venv
$ python -m venv python-env
$ python -m venv python-env
$ sudo pip3 install scrapy
```

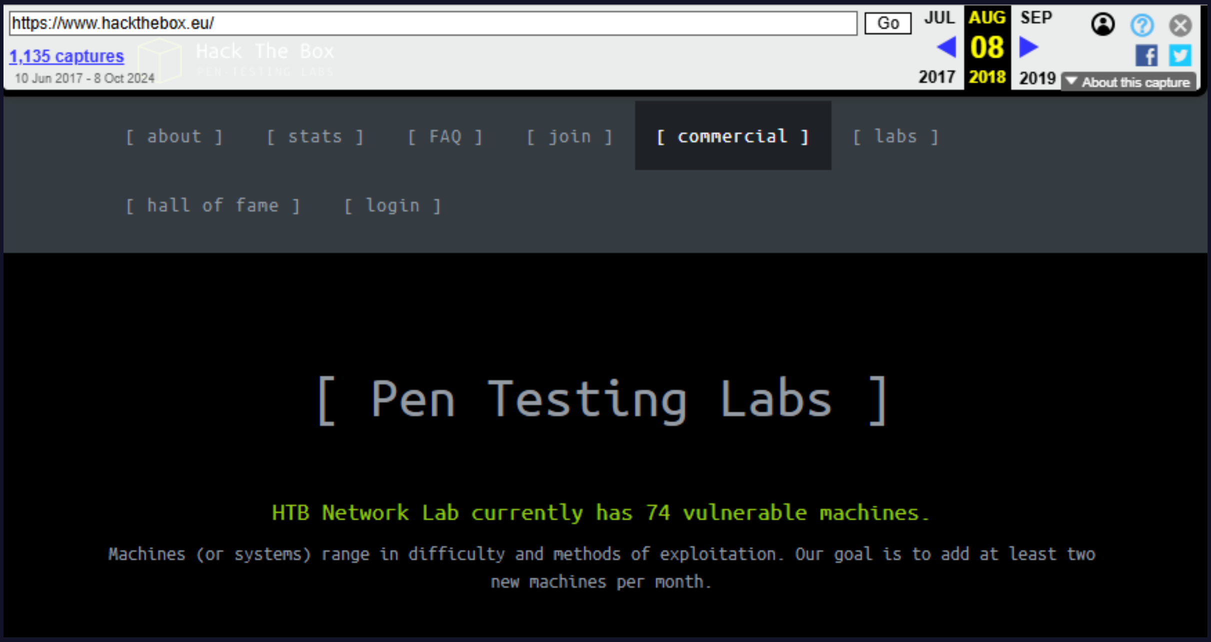
```
$ wget -O ReconSpider.zip https://academy.hackthebox.com/storage/modules/144/ReconSpider.v1.2.zip
$ unzip ReconSpider.zip
$ python3 ReconSpider.py http://inlanefreight.com
$ cat results.json
```

```
    "comments": [
        "<!--/overlay-->",
        "<!--Sidebar Area-->",
        "<!--\nSkip to content<div class=\"wrapper\">\n<header class=\"transportex-trhead\">\n\t<!--==================== Header ====================-->",
        "<!-- Right nav -->",
        "<!--==================== feature-product ====================-->",
        "<!-- /Navigation -->",
        "<!-- /Right nav -->",
        "<!-- TO-DO: change the location of future reports to inlanefreight-comp133.s3.amazonaws.htb -->",
        "<!-- /navbar-toggle -->",
        "<!-- Blog Area -->",
        "<!--==================== TOP BAR ====================-->",
        "<!-- navbar-toggle -->",
        "<!-- #secondary -->",
```

Web Archives

How many Pen Testing Labs did HackTheBox have on the 8th August 2018? Answer with an integer, eg 1234.

Answer: 74



https://www.hackthebox.eu/ Go JUL AUG SEP 08 2017 2018 2019

1,135 captures
10 Jun 2017 - 8 Oct 2024

[about] [stats] [FAQ] [join] [commercial] [labs] [hall of fame] [login]

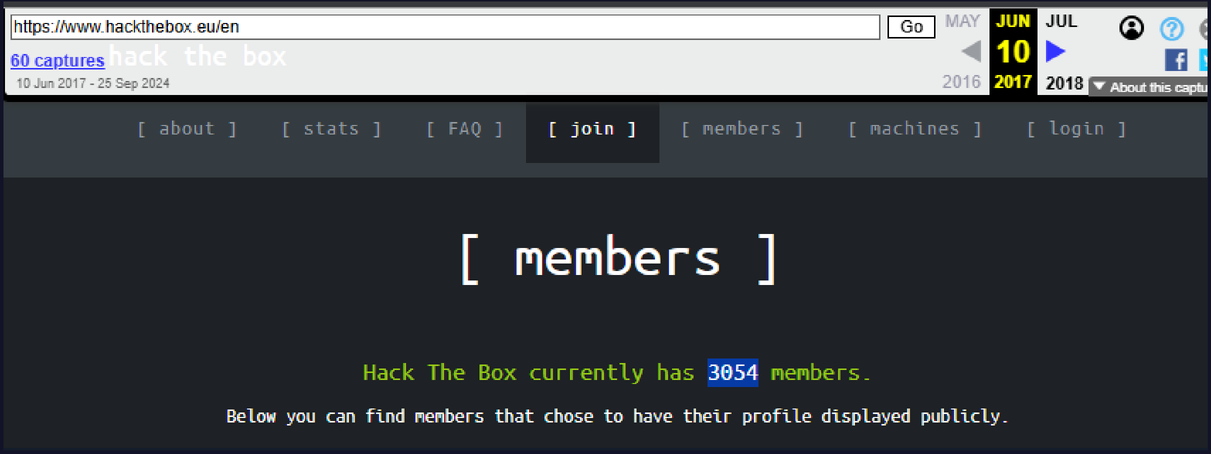
[Pen Testing Labs]

HTB Network Lab currently has 74 vulnerable machines.

Machines (or systems) range in difficulty and methods of exploitation. Our goal is to add at least two new machines per month.

How many members did HackTheBox have on the 10th June 2017? Answer with an integer, eg 1234.

Answer: 3054



https://www.hackthebox.eu/en Go MAY JUN JUL 10 2016 2017 2018

60 captures
10 Jun 2017 - 25 Sep 2024

[about] [stats] [FAQ] [join] [members] [machines] [login]

[members]

Hack The Box currently has 3054 members.

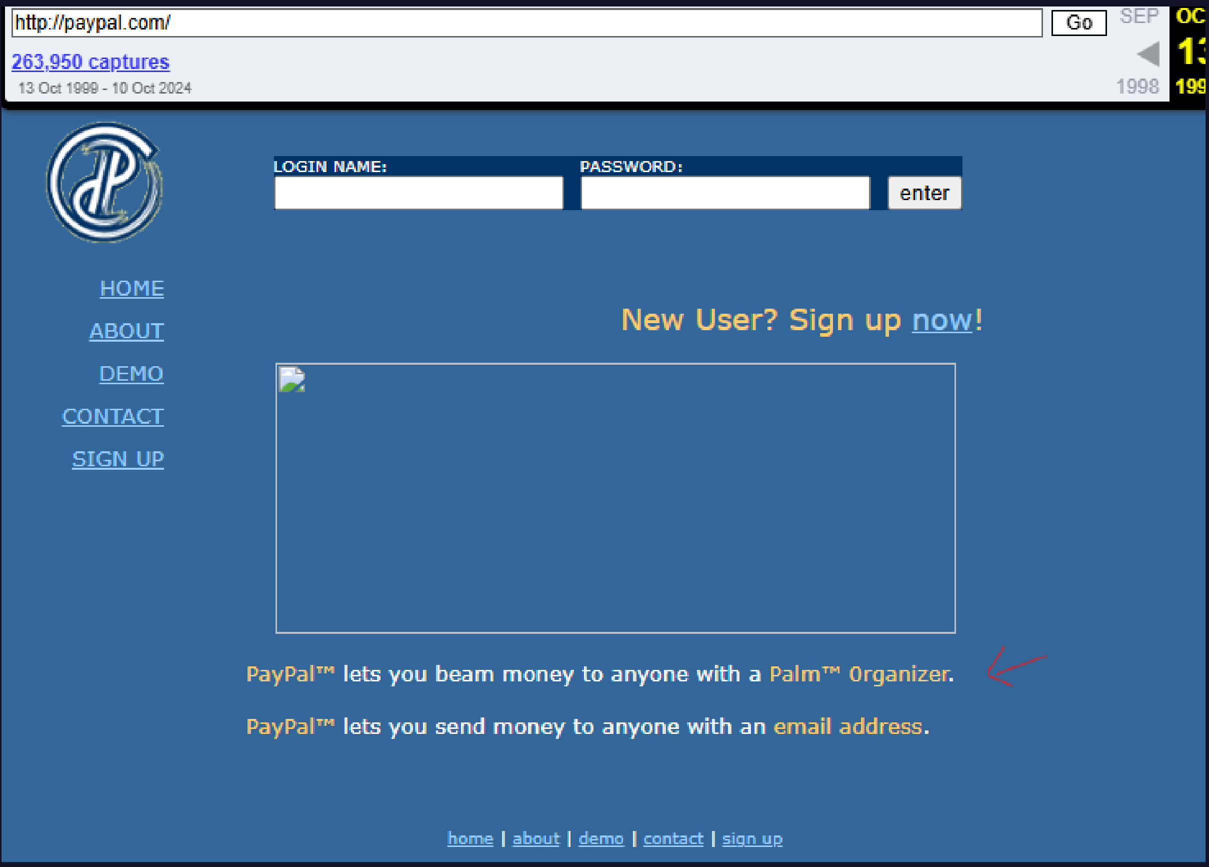
Below you can find members that chose to have their profile displayed publicly.

Going back to March 2002, what website did the facebook.com domain redirect too? Answer with the full domain, eg http://www.facebook.com/

Answer: http://site.aboutface.com/

According to the paypal.com website in October 1999, what could you use to "beam money to anyone"? Answer with the product name, eg My Device, remove the ™ from your answer.

Answer: Palm Organizer



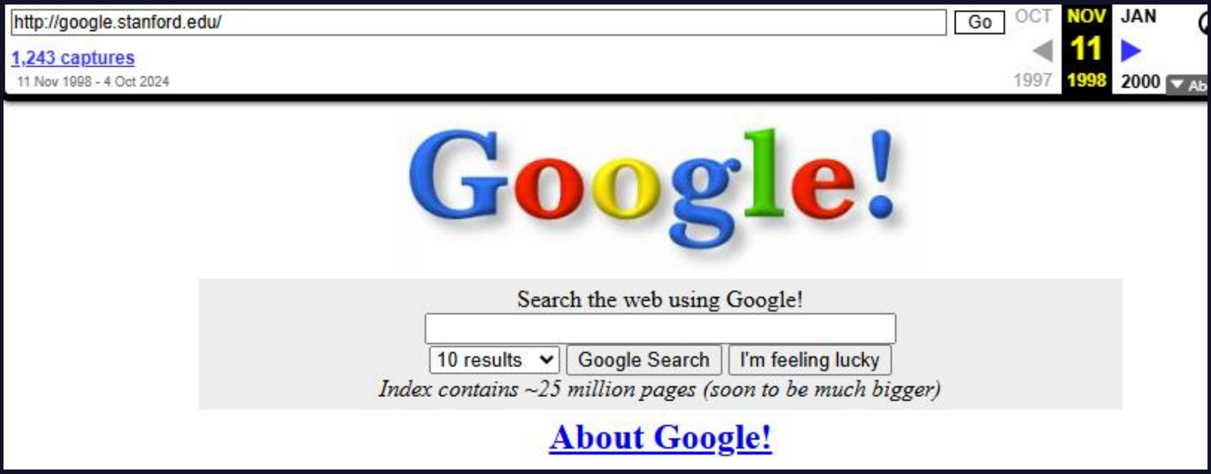
New User? Sign up now!

PayPal™ lets you beam money to anyone with a Palm™ Organizer.

PayPal™ lets you send money to anyone with an email address.

Going back to November 1998 on google.com, what address hosted the non-alpha "Google Search Engine Prototype" of Google? Answer with the full address, eg http://google.com

Answer: http://google.stanford.edu/



http://google.stanford.edu/

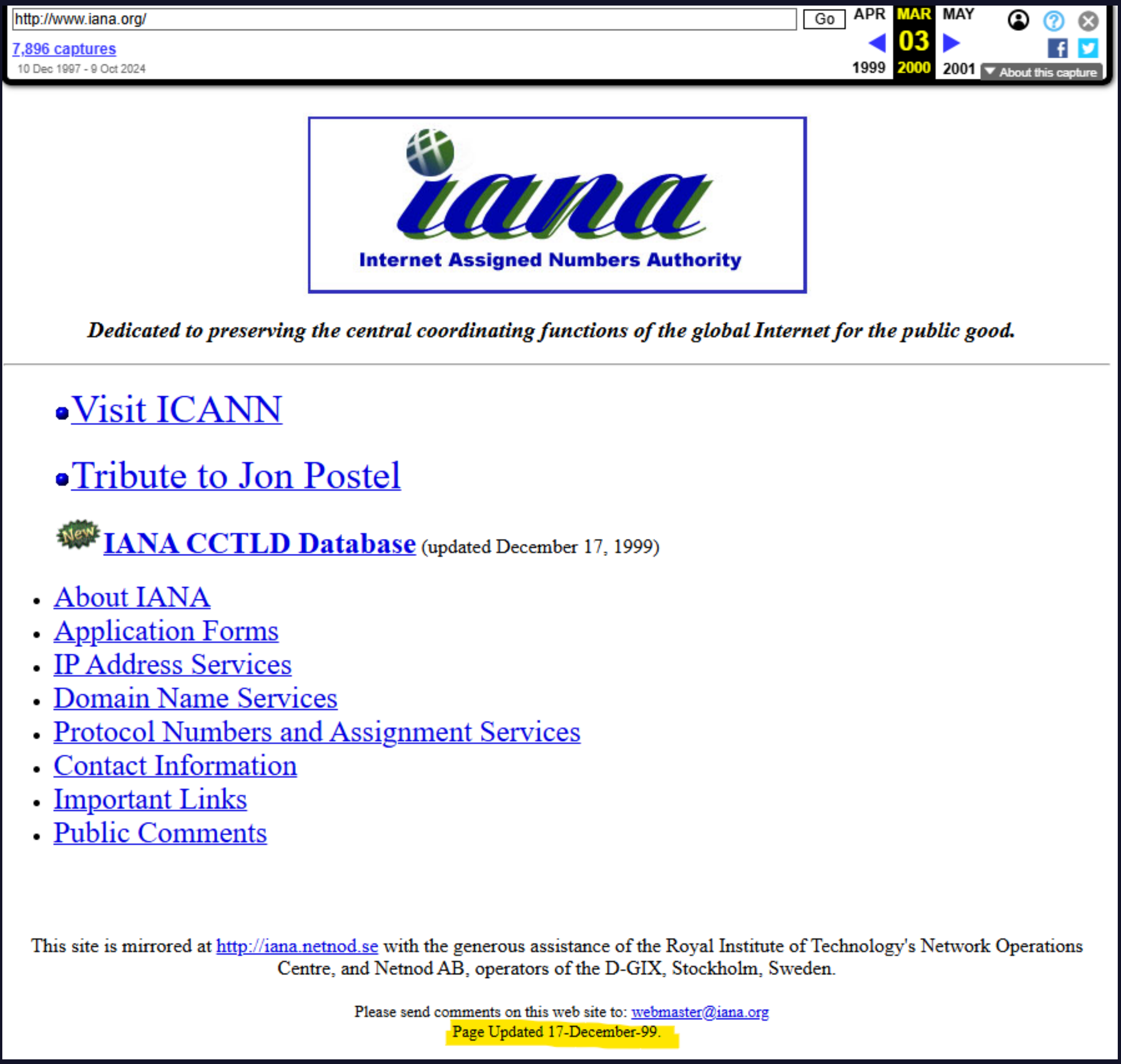
Search the web using Google!

Index contains ~25 million pages (soon to be much bigger)

About Google!

Going back to March 2000 on www.iana.org, when exacty was the site last updated? Answer with the date in the footer, eg 11-March-99

Answer: 17-December-99



Dedicated to preserving the central coordinating functions of the global Internet for the public good.

- Visit ICANN
- Tribute to Jon Postel

IANA CCTLD Database (updated December 17, 1999)

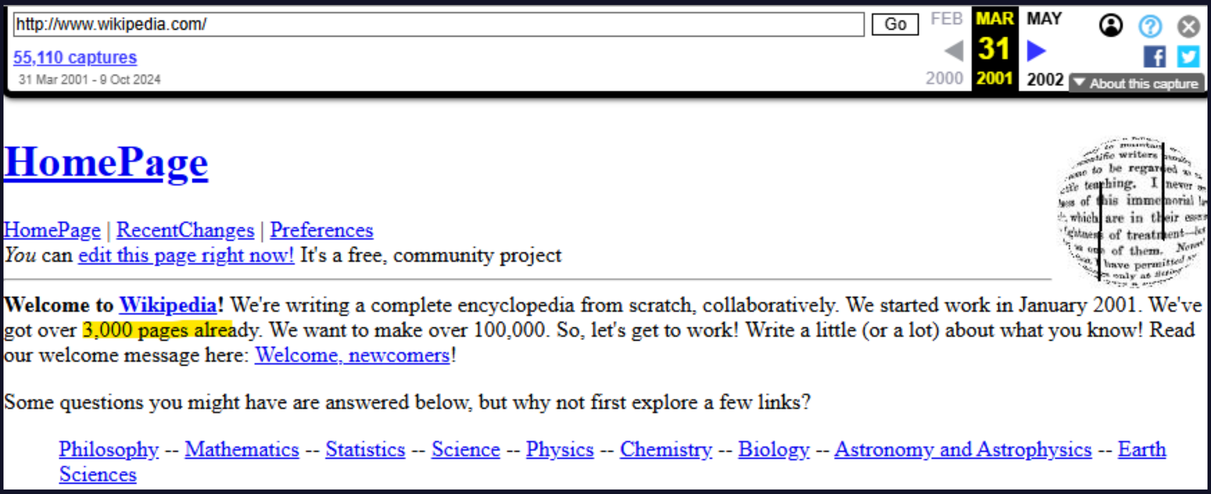
- About IANA
- Application Forms
- IP Address Services
- Domain Name Services
- Protocol Numbers and Assignment Services
- Contact Information
- Important Links
- Public Comments

This site is mirrored at http://iana.netnod.se with the generous assistance of the Royal Institute of Technology's Network Operations Centre, and Netnod AB, operators of the D-GIX, Stockholm, Sweden.

Please send comments on this web site to: webmaster@iana.org
Page Updated 17-December-99.

According to the wikipedia.com snapshot taken in March 2001, how many pages did they have over? Answer with the number they state without any commas, eg 2000 not 2,000

Answer: 3000



HomePage

HomePage | RecentChanges | Preferences
You can edit this page right now! It's a free, community project

Welcome to Wikipedia! We're writing a complete encyclopedia from scratch, collaboratively. We started work in January 2001. We've got over 3,000 pages already. We want to make over 100,000. So, let's get to work! Write a little (or a lot) about what you know! Read our welcome message here: Welcome, newcomers!

Some questions you might have are answered below, but why not first explore a few links?

Philosophy -- Mathematics -- Statistics -- Science -- Physics -- Chemistry -- Biology -- Astronomy and Astrophysics -- Earth Sciences

Skills Assessment

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

Answer: 468

```
$ whois inlanefreight.com

        Domain Name: INLANEFREIGHT.COM
          Registry Domain ID: 2420436757_DOMAIN_COM-VRSN
          Registrar WHOIS Server: whois.registrar.amazon.com
          Registrar URL: http://registrar.amazon.com
          Updated Date: 2024-07-02T22:07:11Z
          Creation Date: 2019-08-05T22:43:09Z
          Registry Expiry Date: 2025-08-05T22:43:09Z
          Registrar: Amazon Registrar, Inc.
          Registrar IANA ID: 468
```

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.

Answer: nginx

```
$ whatweb http://83.136.254.47:31018

        http://83.136.254.47:31018 [200 OK] Country[FINLAND][FI], HTML5,
        HTTPServer[nginx/1.26.1], IP[83.136.254.47], Title[inlanefreight], nginx[1.26.1]
```

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

Answer: e963d863ee0e82ba7080fbf558ca0d3f

```
$ sudo nano /etc/hosts
        83.136.254.47 web1337.inlanefreight.htb


$ gobuster vhost -u http://inlanefreight.htb:31018 -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt --append-domain


        Found: web1337.inlanefreight.htb:31018 Status: 200 [Size: 104]
```

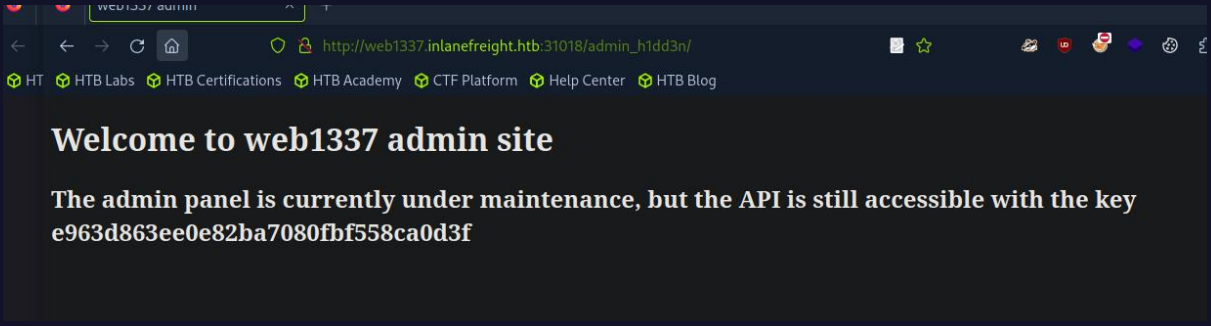
```
$ ffuf -recursion -recursion-depth 1 -u http://web1337.inlanefreight.htb:31018/FUZZ -w
/opt/useful/seclists/Discovery/Web-Content/common.txt

        Found robots.txt

$ curl http://web1337.inlanefreight.htb:31018/robots.txt

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


$ curl http://web1337.inlanefreight.htb:31018/admin_h1dd3n/
<!DOCTYPE html><html><head><title>web1337 admin</title></head><body><h1>Welcome to
web1337 admin site</h1><h2>The admin panel is currently under maintenance, but the API is
still accessible with the key e963d863ee0e82ba7080fbf558ca0d3f</h2></body></html>
```



Welcome to web1337 admin site

The admin panel is currently under maintenance, but the API is still accessible with the key e963d863ee0e82ba7080fbf558ca0d3f

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.

Answer: 1337testing@inlanefreight.htb

What is the API key the inlanefreight.htb developers will be changing too?

Answer: ba988b835be4aa97d068941dc852ff33

```
$ gobuster vhost -u http://web1337.inlanefreight.htb:31018 -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt --append-domain

        Found: dev.web1337.inlanefreight.htb:PORT Status: 200

$ sudo nano /etc/hosts
        83.136.254.47 dev.web1337.inlanefreight.htb

$ pip3 install scrapy
$ wget -O ReconSpider.zip
https://academy.hackthebox.com/storage/modules/144/ReconSpider.v1.2.zip

$ unzip ReconSpider.zip
```

```
$ python3 ReconSpider.py http://dev.web1337.inlanefreight.htb:31018/
$ cat results.json
{
  "emails": [
    "1337testing@inlanefreight.htb"
  ],

.....
"comments": [
    "<!-- Remember to change the API key to ba988b835be4aa97d068941dc852ff33 -->"
```