目標網站資訊蒐集實作

郭益華

資訊蒐集介紹

- 資訊蒐集是滲透測試的第一個階段，目的是蒐集目標的所有資訊，以加速後續的漏洞識別與漏洞利用。資訊蒐集分成主動情蒐與被動情蒐：

- 被動情蒐：蒐集公開在網路中可被利用的資訊，例如 WHOIS 資訊、公司資訊（聯絡人信箱、名稱）等。
- 主動情蒐：直接與目標進行存取，透過掃描工具收集資訊，例如端口掃描、服務枚舉。

工具介紹

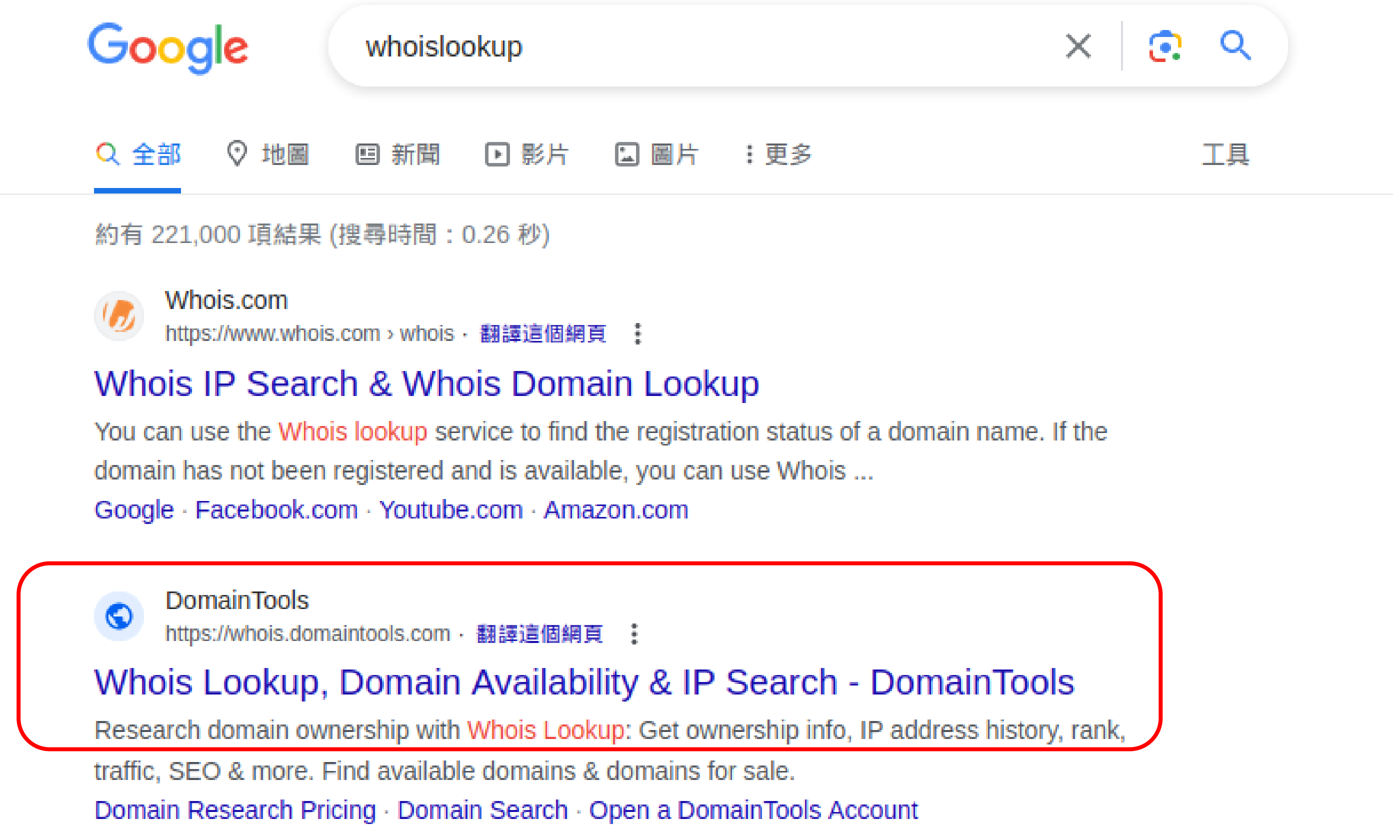
- Whois Lookup: 查詢目標網站所有者的資訊
- Netcraft Site Report: 顯示目標網站上使用的技術
- Robtex DNS: 顯示關於目標網站的全面DNS資訊
- Knock: 尋找目標網站子域名
- Dirb: 搜索目標網站的文件和目錄

目錄

1. Whois Lookup
2. Netcraft Site Report
3. Robtex DNS
4. Knock
5. Dirb

1. Whois Lookup

Google 搜尋 whoislookup



約有 221,000 項結果 (搜尋時間：0.26 秒)

Whois.com
https://www.whois.com › whois · 翻譯這個網頁

Whois IP Search & Whois Domain Lookup

You can use the Whois lookup service to find the registration status of a domain name. If the domain has not been registered and is available, you can use Whois ...

Google · Facebook.com · Youtube.com · Amazon.com

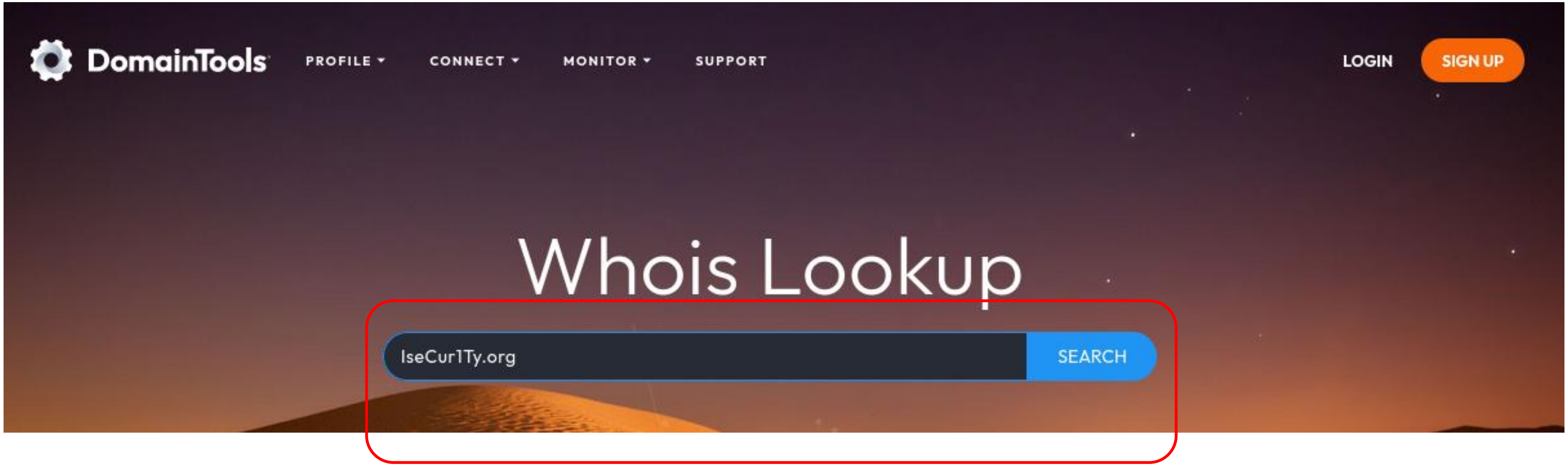
DomainTools
https://whois.domaintools.com · 翻譯這個網頁

Whois Lookup, Domain Availability & IP Search - DomainTools

Research domain ownership with Whois Lookup: Get ownership info, IP address history, rank, traffic, SEO & more. Find available domains & domains for sale.

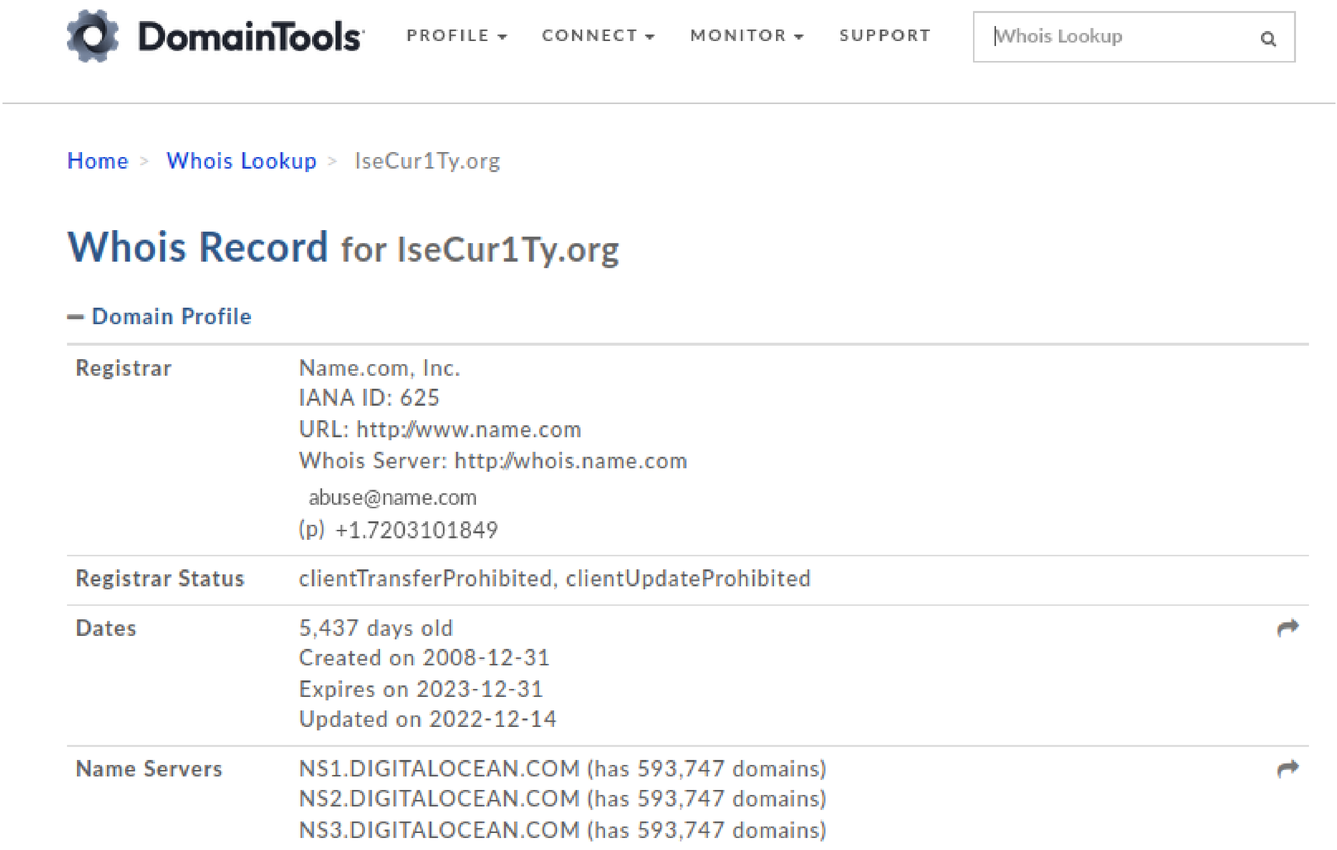
Domain Research Pricing · Domain Search · Open a DomainTools Account

輸入目標網站的domain



IseCur1Ty.org

即可獲得目標網站相關資訊(1/2)



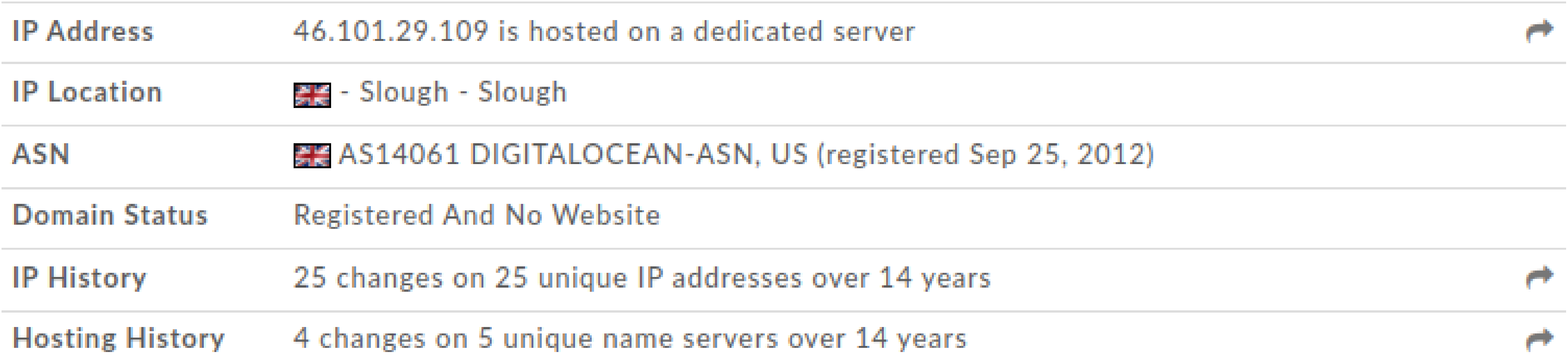
Home > Whois Lookup > IseCur1Ty.org

Whois Record for IseCur1Ty.org

— Domain Profile

Registrar	Name.com, Inc. IANA ID: 625 URL: http://www.name.com Whois Server: http://whois.name.com abuse@name.com (p) +1.7203101849
Registrar Status	clientTransferProhibited, clientUpdateProhibited
Dates	5,437 days old Created on 2008-12-31 Expires on 2023-12-31 Updated on 2022-12-14
Name Servers	NS1.DIGITALOCEAN.COM (has 593,747 domains) NS2.DIGITALOCEAN.COM (has 593,747 domains) NS3.DIGITALOCEAN.COM (has 593,747 domains)

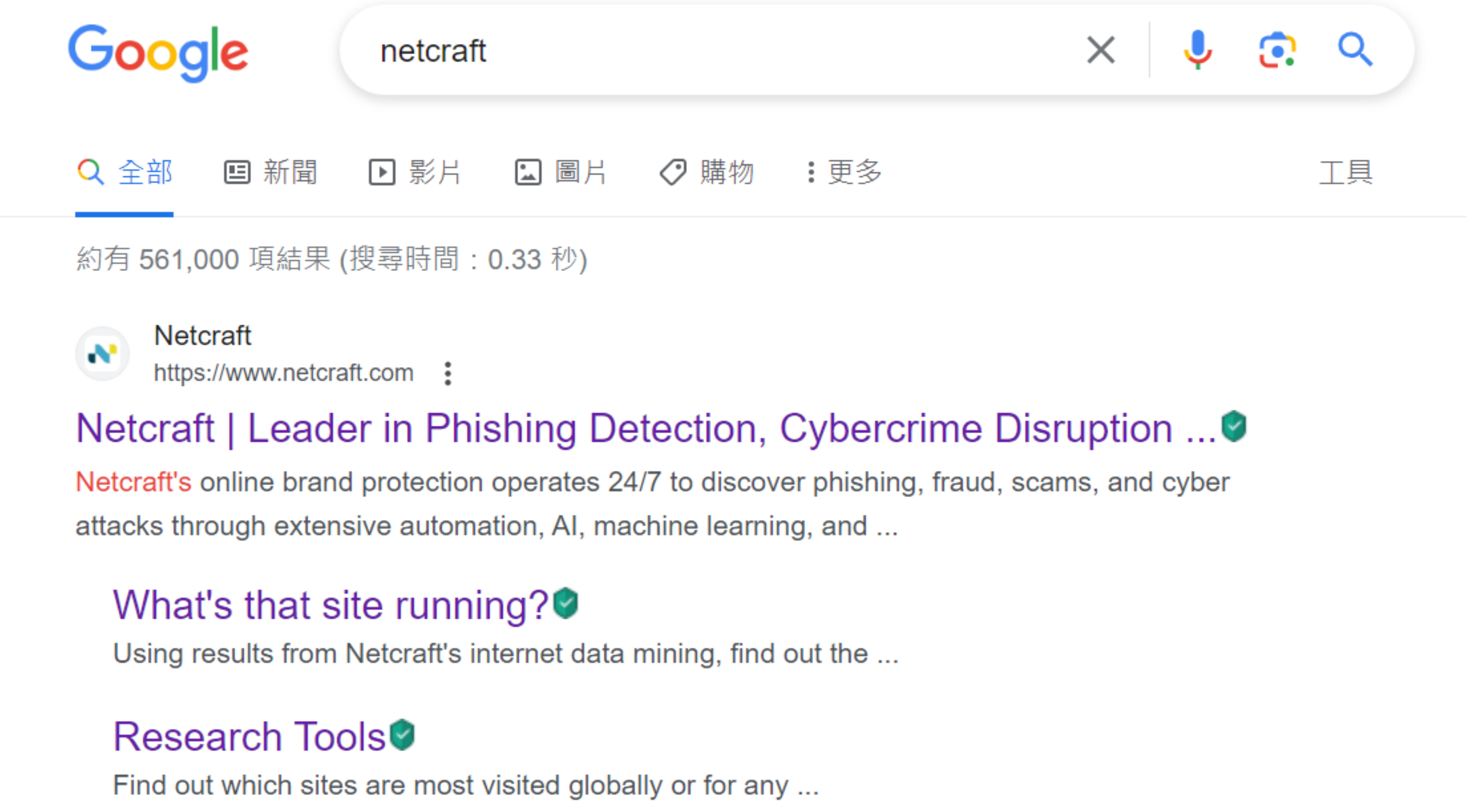
即可獲得目標網站相關資訊(2/2)



IP Address	46.101.29.109 is hosted on a dedicated server
IP Location	🇬🇧 - Slough - Slough
ASN	🇬🇧 AS14061 DIGITALOCEAN-ASN, US (registered Sep 25, 2012)
Domain Status	Registered And No Website
IP History	25 changes on 25 unique IP addresses over 14 years
Hosting History	4 changes on 5 unique name servers over 14 years

2. Netcraft Site Report

Google 搜尋 netctaft



約有 561,000 項結果 (搜尋時間：0.33 秒)

Netcraft
https://www.netcraft.com

Netcraft | Leader in Phishing Detection, Cybercrime Disruption ...

Netcraft's online brand protection operates 24/7 to discover phishing, fraud, scams, and cyber attacks through extensive automation, AI, machine learning, and ...

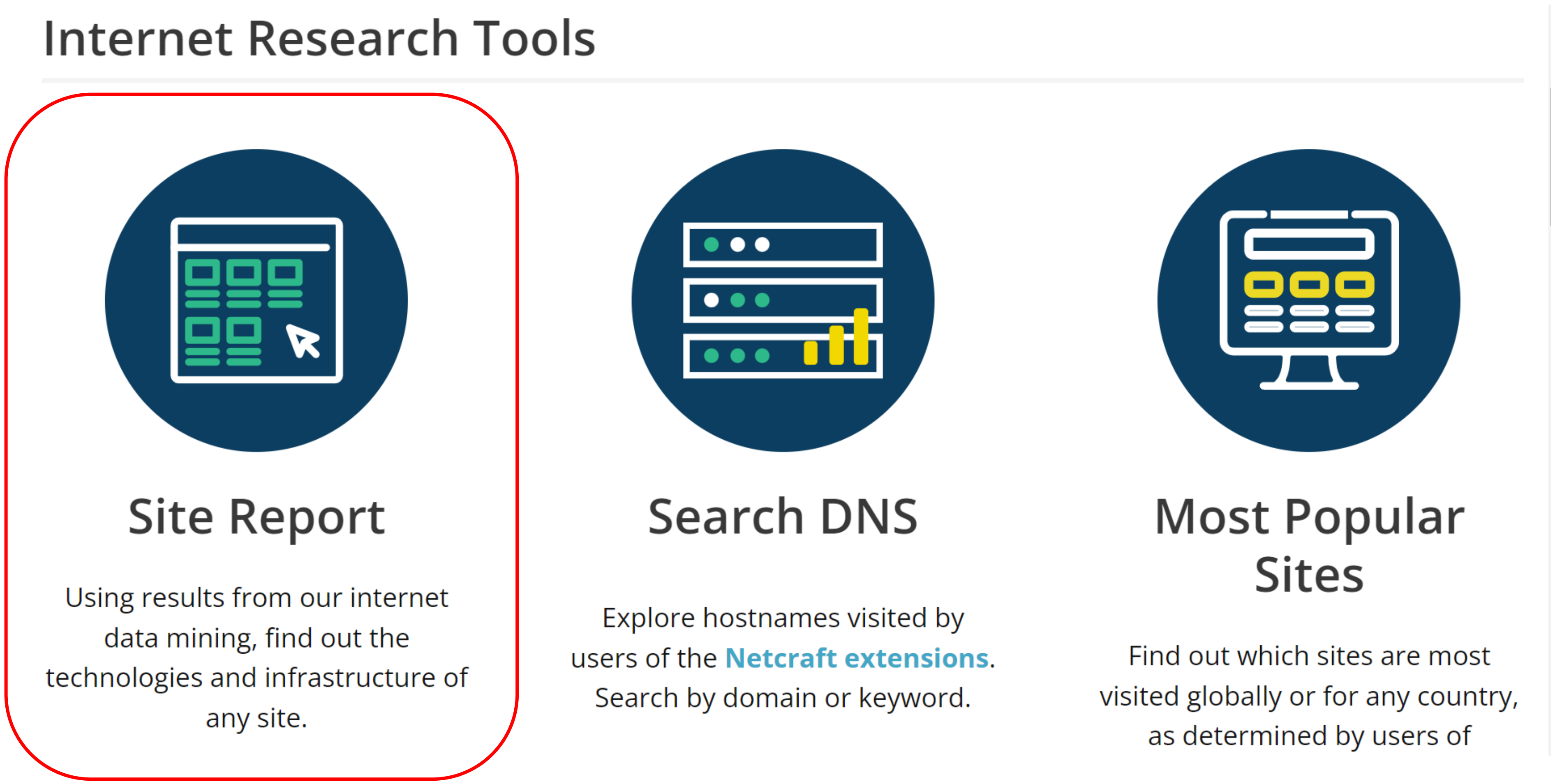
What's that site running?

Using results from Netcraft's internet data mining, find out the ...

Research Tools

Find out which sites are most visited globally or for any ...

選取 Site Report



Internet Research Tools

Site Report

Using results from our internet data mining, find out the technologies and infrastructure of any site.

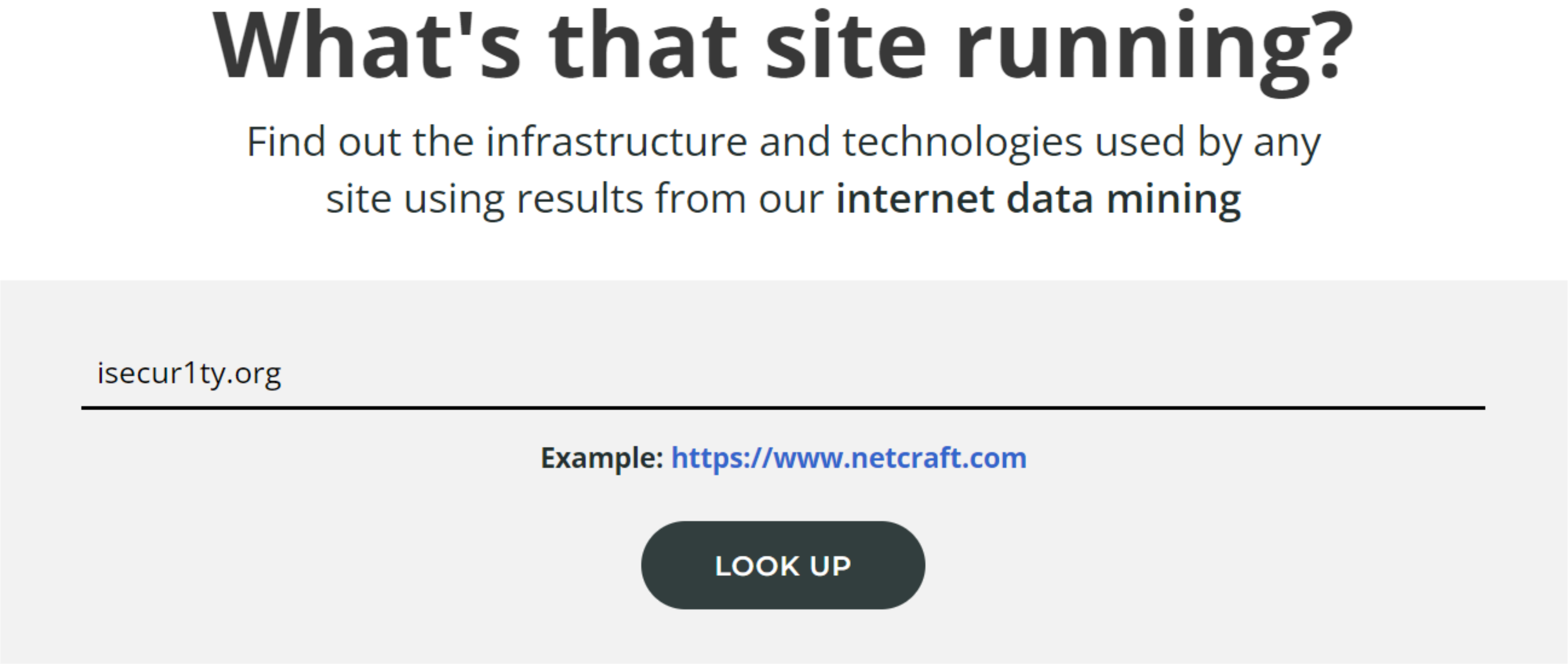
Search DNS

Explore hostnames visited by users of the Netcraft extensions. Search by domain or keyword.

Most Popular Sites

Find out which sites are most visited globally or for any country, as determined by users of

輸入目標網站domain



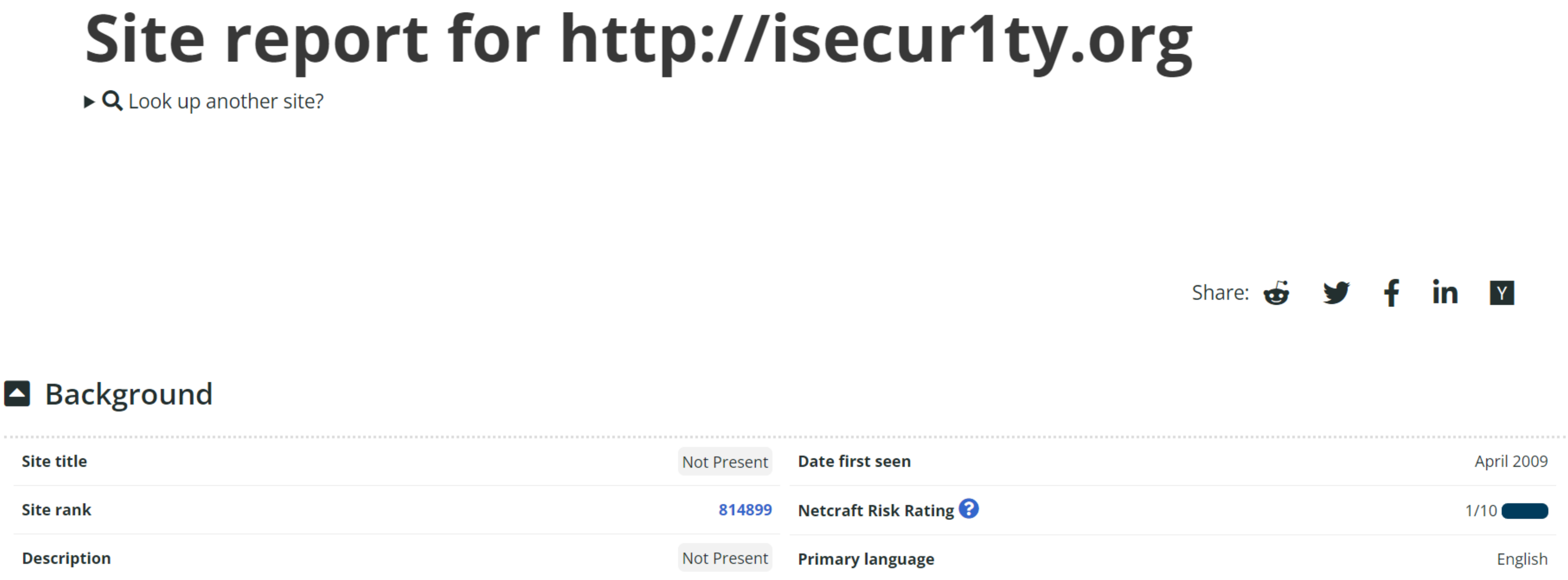
What's that site running?

Find out the infrastructure and technologies used by any site using results from our **internet data mining**

isecur1ty.org

Example: https://www.netcraft.com

即可獲得目標網站相關資訊(1/3)



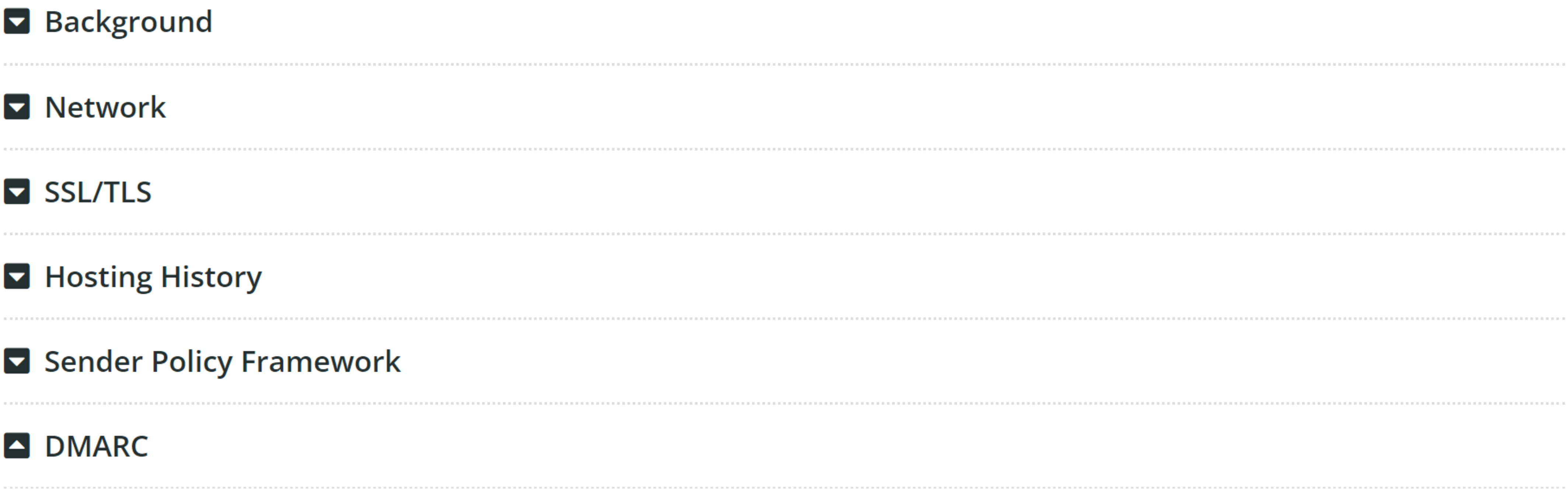
Site report for http://isecur1ty.org

▸ 🔍 Look up another site?

Background

Site title	Not Present	**Date first seen**	April 2009
Site rank	814899	**Netcraft Risk Rating** ?	1/10
Description	Not Present	**Primary language**	English

即可獲得目標網站相關資訊(2/3)



▼ Background

▼ Network

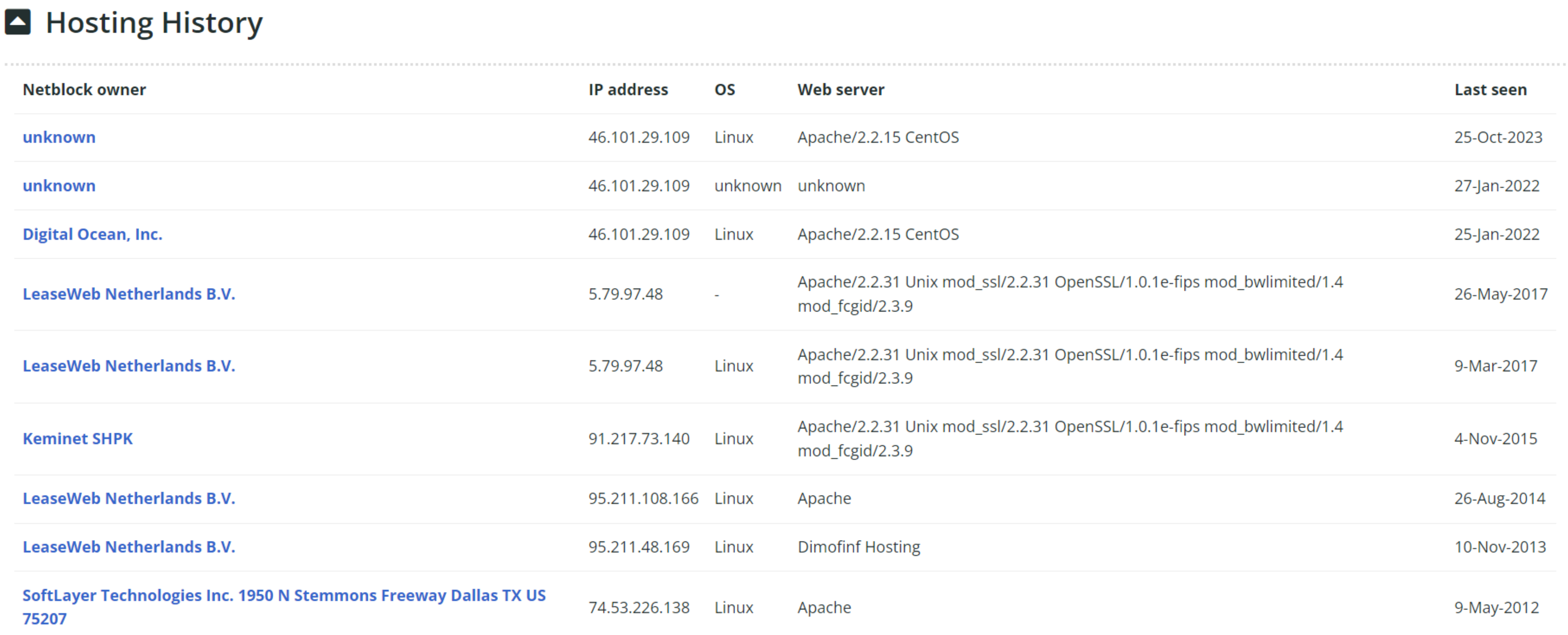
▼ SSL/TLS

▼ Hosting History

▼ Sender Policy Framework

▲ DMARC

即可獲得目標網站相關資訊(3/3)

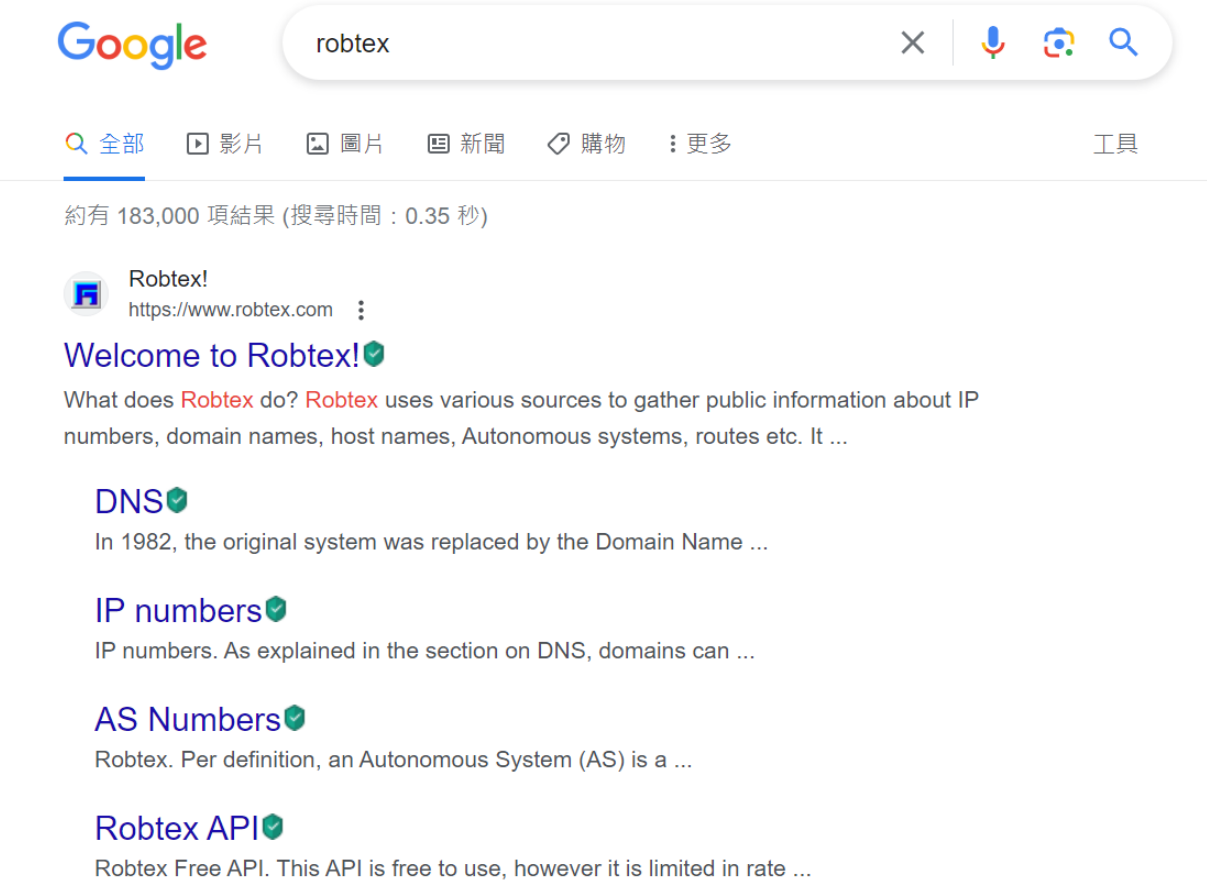


Hosting History

Netblock owner	IP address	OS	Web server	Last seen
unknown	46.101.29.109	Linux	Apache/2.2.15 CentOS	25-Oct-2023
unknown	46.101.29.109	unknown	unknown	27-Jan-2022
Digital Ocean, Inc.	46.101.29.109	Linux	Apache/2.2.15 CentOS	25-Jan-2022
LeaseWeb Netherlands B.V.	5.79.97.48	-	Apache/2.2.31 Unix mod_ssl/2.2.31 OpenSSL/1.0.1e-fips mod_bwlimited/1.4 mod_fcgid/2.3.9	26-May-2017
LeaseWeb Netherlands B.V.	5.79.97.48	Linux	Apache/2.2.31 Unix mod_ssl/2.2.31 OpenSSL/1.0.1e-fips mod_bwlimited/1.4 mod_fcgid/2.3.9	9-Mar-2017
Keminet SHPK	91.217.73.140	Linux	Apache/2.2.31 Unix mod_ssl/2.2.31 OpenSSL/1.0.1e-fips mod_bwlimited/1.4 mod_fcgid/2.3.9	4-Nov-2015
LeaseWeb Netherlands B.V.	95.211.108.166	Linux	Apache	26-Aug-2014
LeaseWeb Netherlands B.V.	95.211.48.169	Linux	Dimofinf Hosting	10-Nov-2013
SoftLayer Technologies Inc. 1950 N Stemmons Freeway Dallas TX US 75207	74.53.226.138	Linux	Apache	9-May-2012

3. Robtex DNS

Google 搜尋 robtex



約有 183,000 項結果 (搜尋時間：0.35 秒)

Robtex!
https://www.robtex.com

Welcome to Robtex!

What does Robtex do? Robtex uses various sources to gather public information about IP numbers, domain names, host names, Autonomous systems, routes etc. It ...

DNS

In 1982, the original system was replaced by the Domain Name ...

IP numbers

IP numbers. As explained in the section on DNS, domains can ...

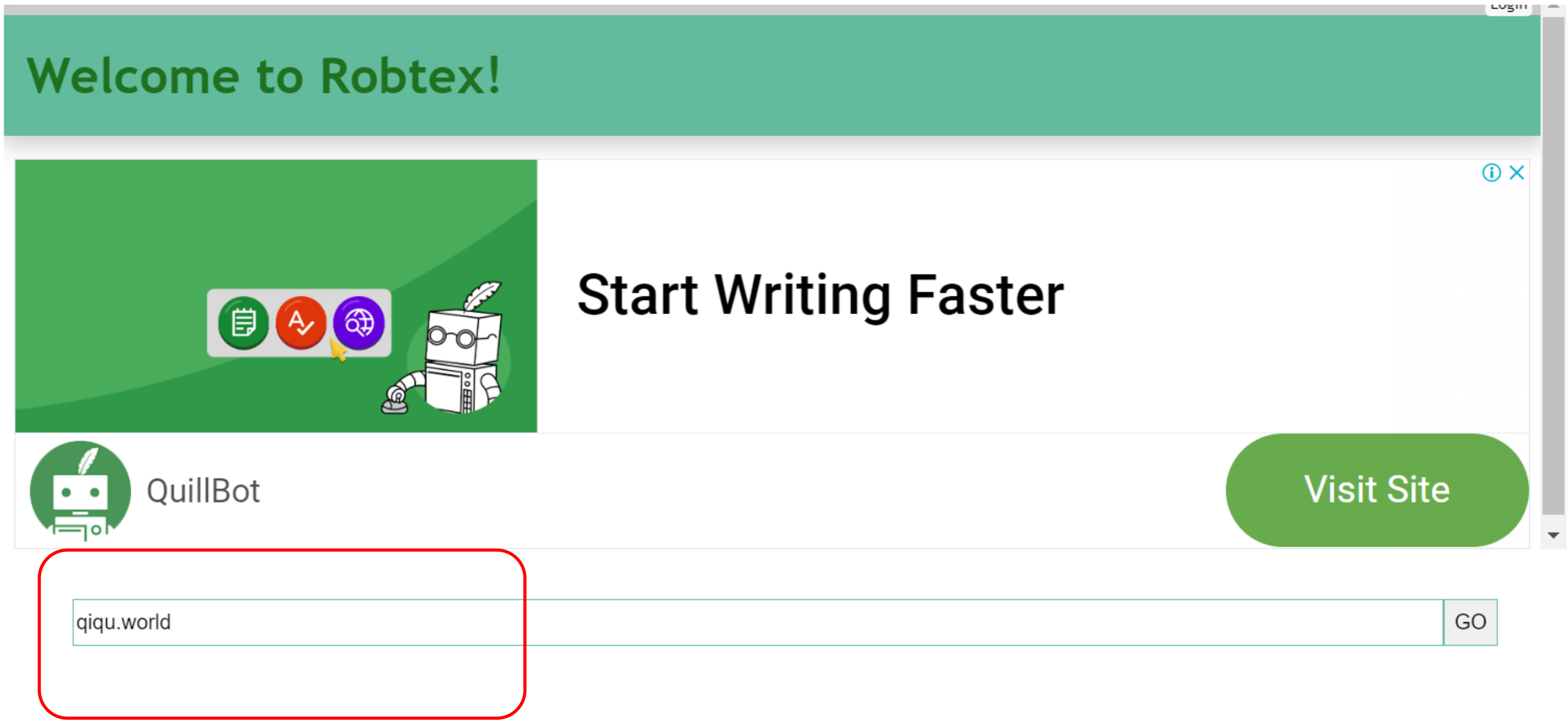
AS Numbers

Robtex. Per definition, an Autonomous System (AS) is a ...

Robtex API

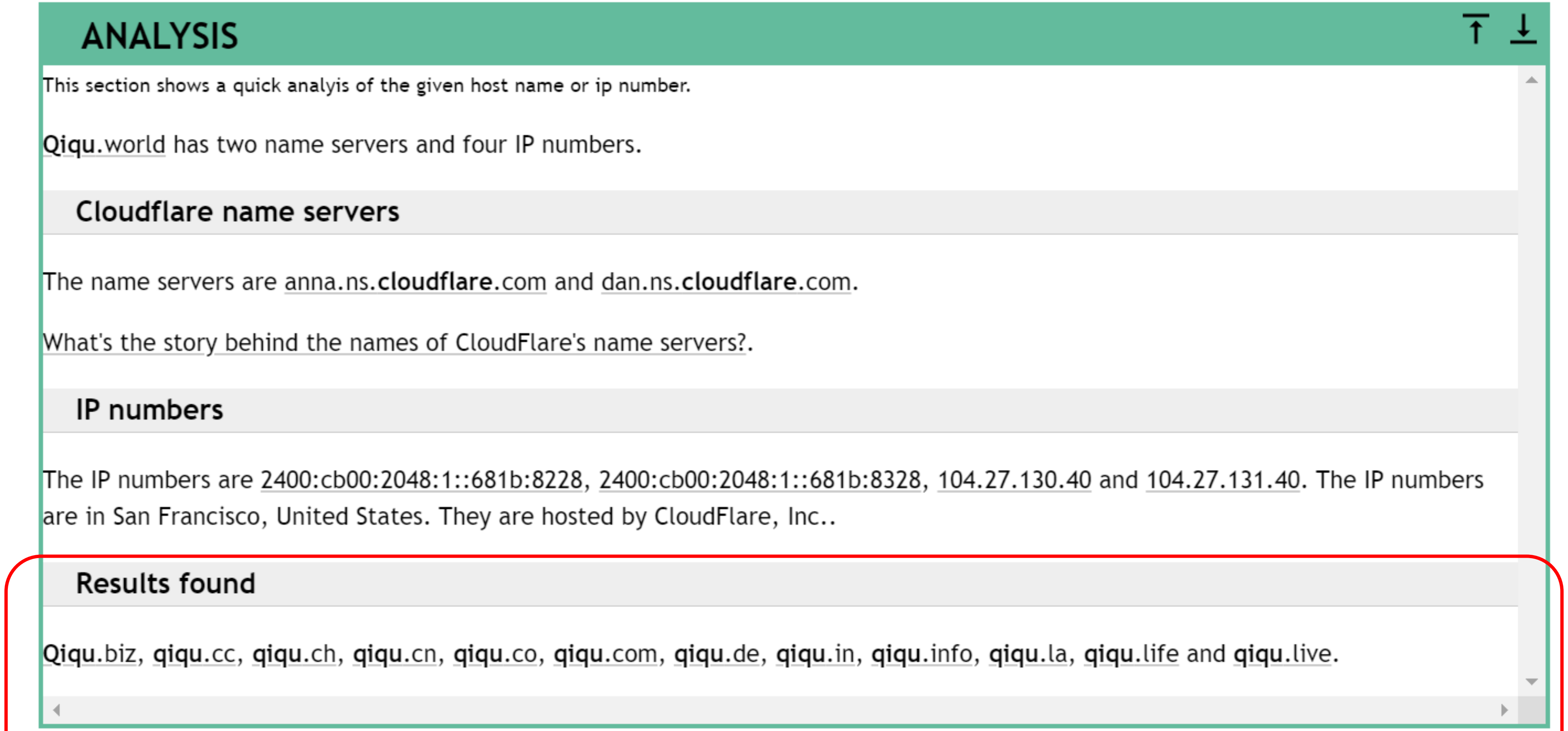
Robtex Free API. This API is free to use, however it is limited in rate ...

輸入目標網站domain



qiqu.world

可發現到相關來源



ANALYSIS

This section shows a quick analyis of the given host name or ip number.

Qiqu.world has two name servers and four IP numbers.

Cloudflare name servers

The name servers are anna.ns.cloudflare.com and dan.ns.cloudflare.com.

What's the story behind the names of CloudFlare's name servers?.

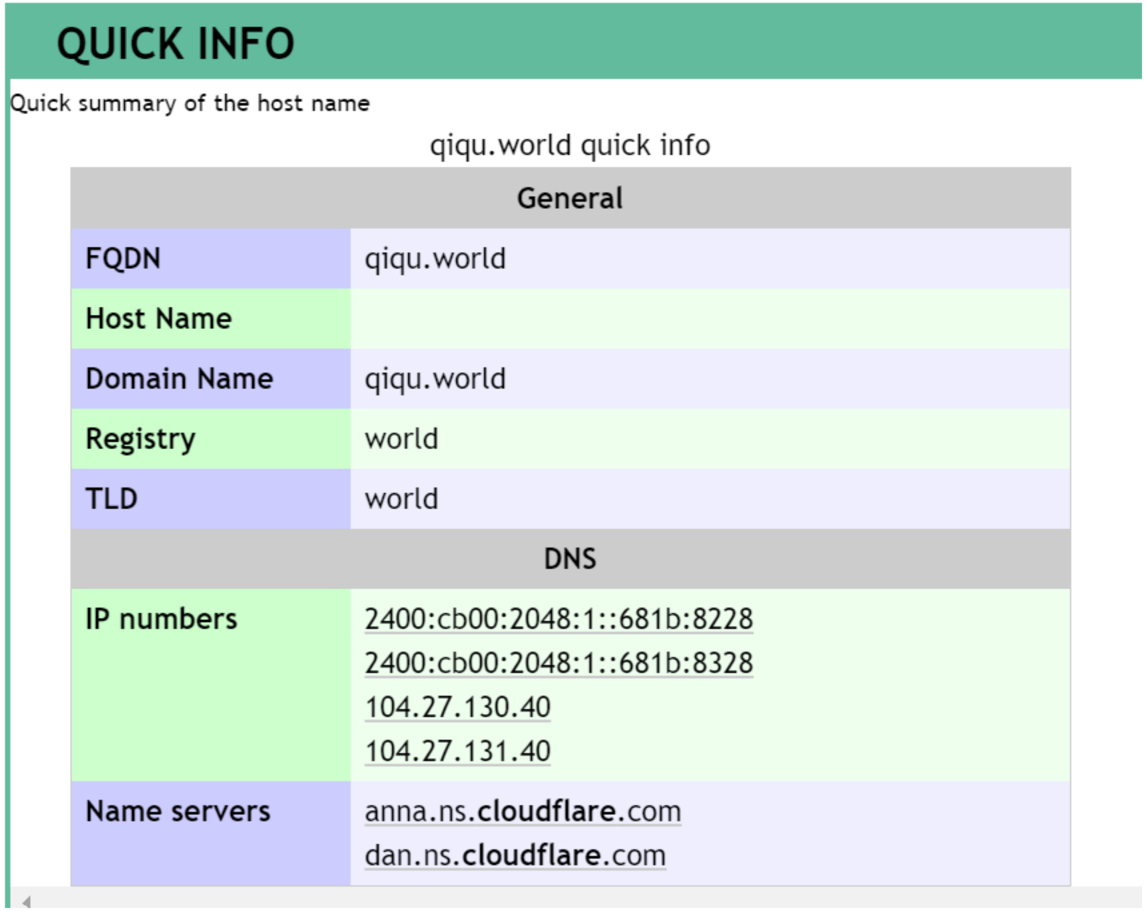
IP numbers

The IP numbers are 2400:cb00:2048:1::681b:8228, 2400:cb00:2048:1::681b:8328, 104.27.130.40 and 104.27.131.40. The IP numbers are in San Francisco, United States. They are hosted by CloudFlare, Inc..

Results found

Qiqu.biz, qiqu.cc, qiqu.ch, qiqu.cn, qiqu.co, qiqu.com, qiqu.de, qiqu.in, qiqu.info, qiqu.la, qiqu.life and qiqu.live.

域名、伺服器

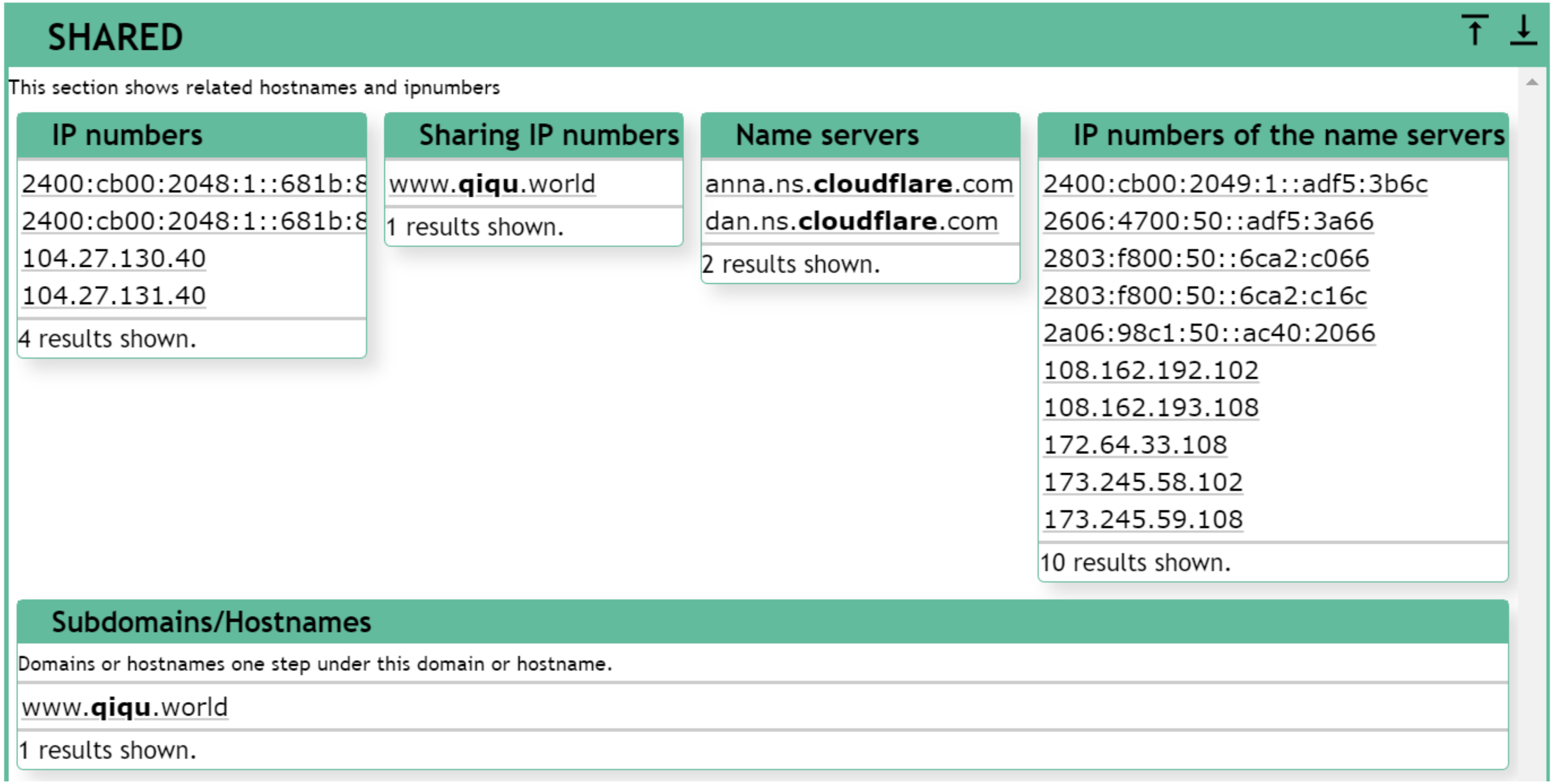


QUICK INFO

Quick summary of the host name

qiqu.world quick info

General	
FQDN	qiqu.world
Host Name	
Domain Name	qiqu.world
Registry	world
TLD	world
DNS	
IP numbers	2400:cb00:2048:1::681b:8228 2400:cb00:2048:1::681b:8328 104.27.130.40 104.27.131.40
Name servers	anna.ns.**cloudflare**.com dan.ns.**cloudflare**.com



SHARED

This section shows related hostnames and ipnumbers

IP numbers
2400:cb00:2048:1::681b:8
2400:cb00:2048:1::681b:8
104.27.130.40
104.27.131.40

4 results shown.

Sharing IP numbers
www.**qiqu**.world

1 results shown.

Name servers
anna.ns.**cloudflare**.com
dan.ns.**cloudflare**.com

2 results shown.

IP numbers of the name servers
2400:cb00:2049:1::adf5:3b6c
2606:4700:50::adf5:3a66
2803:f800:50::6ca2:c066
2803:f800:50::6ca2:c16c
2a06:98c1:50::ac40:2066
108.162.192.102
108.162.193.108
172.64.33.108
173.245.58.102
173.245.59.108

10 results shown.

Subdomains/Hostnames

Domains or hostnames one step under this domain or hostname.

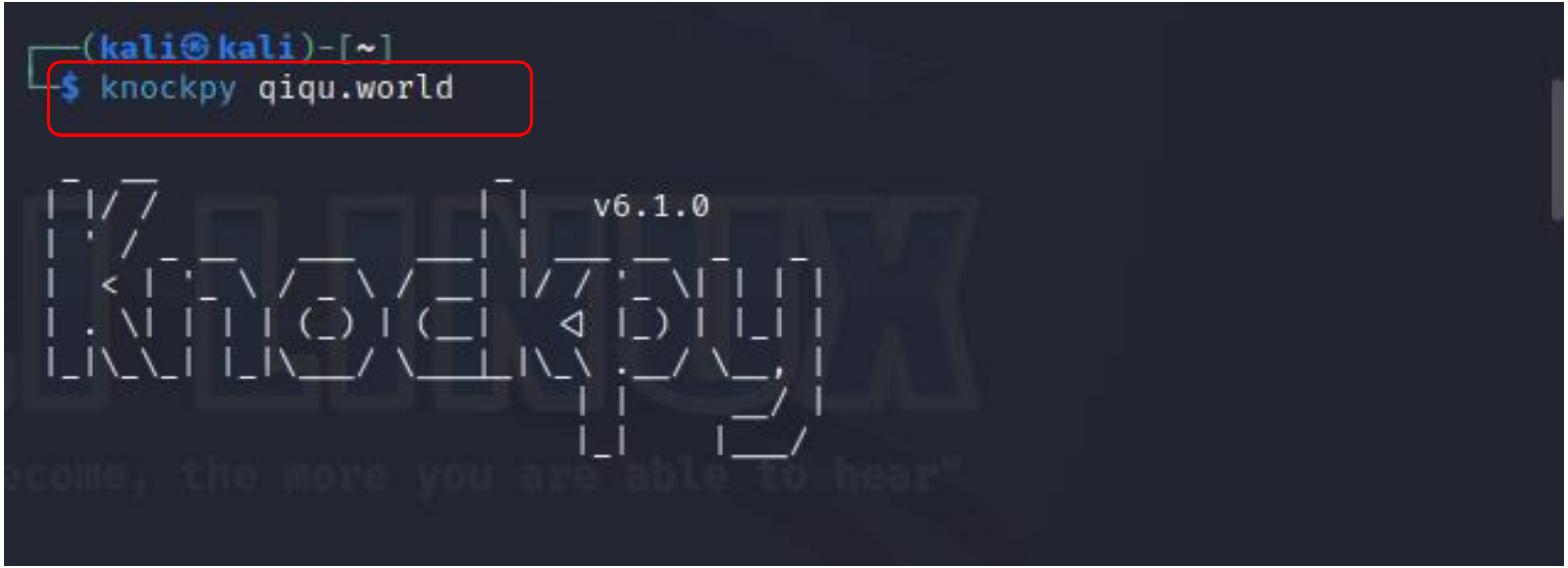
www.**qiqu**.world

1 results shown.

4. Knock

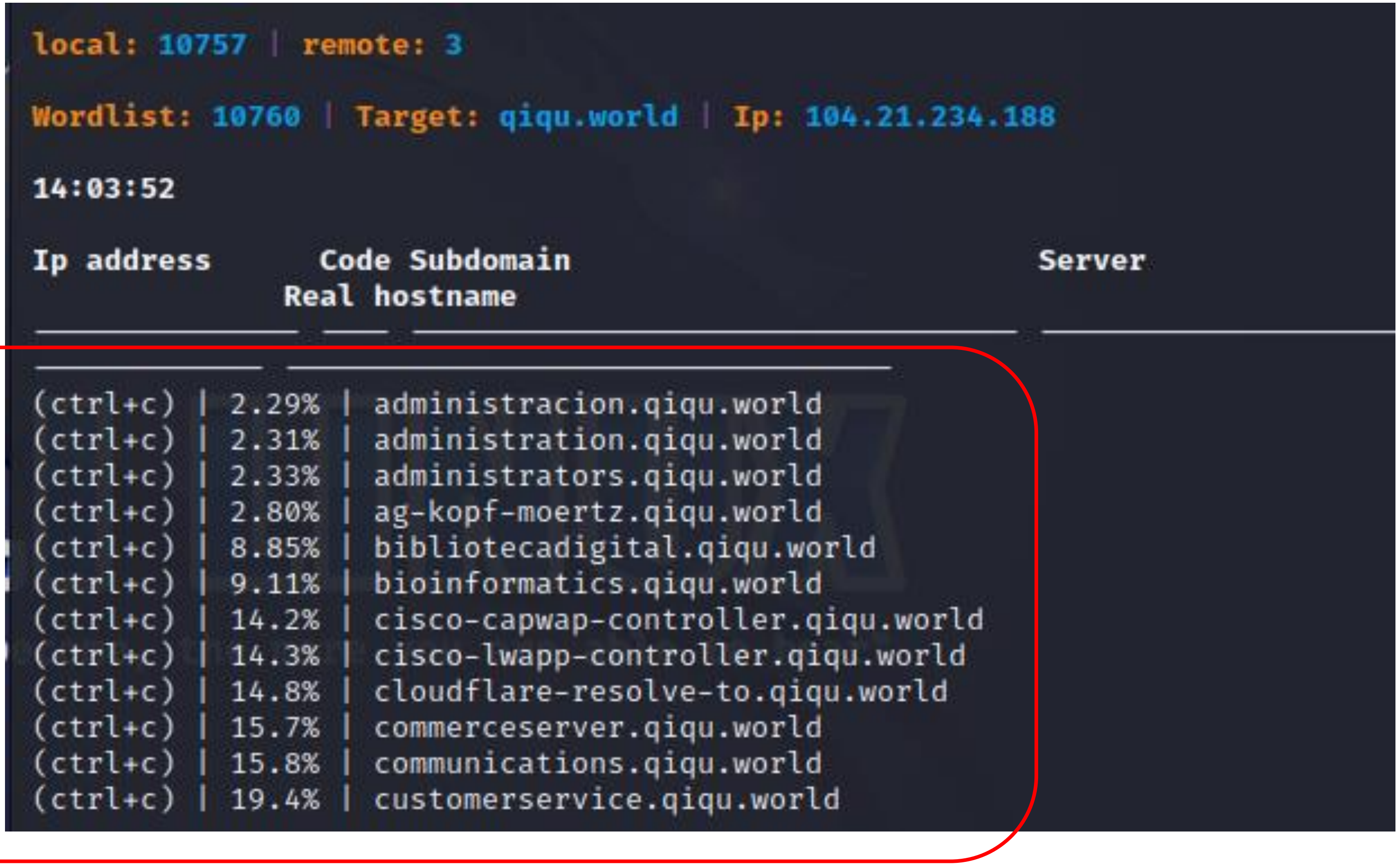
開啟kali linux command line

Command:
knockpy [目標網站domain]



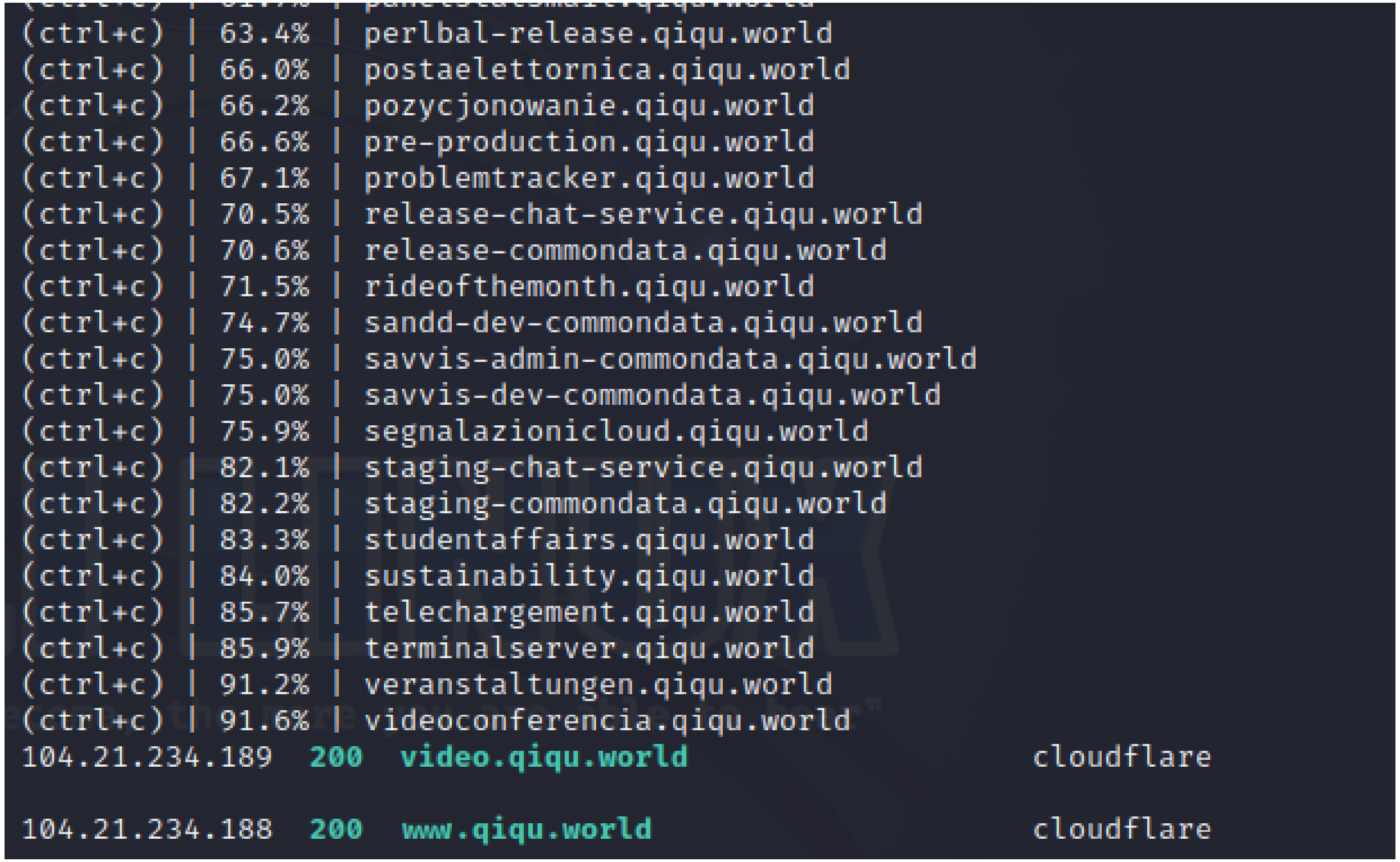
```
┌──(kali㉿kali)-[~]
└─$ knockpy qiqu.world

  _  __                 _
 | |/ /                | |   v6.1.0
 | ' / _ __   ___   ___| | ___ __  _   _
 |  < | '_ \ / _ \ / __| |/ / '_ \| | | |
 | . \| | | | (_) | (__|   ◁| |_) | |_| |
 |_|\_\_| |_|\___/ \___|_|\_\ .__/ \__, |
                            | |     __/ |
                            |_|    |___/
```

即可獲得相關的 Subdomain(1/3)



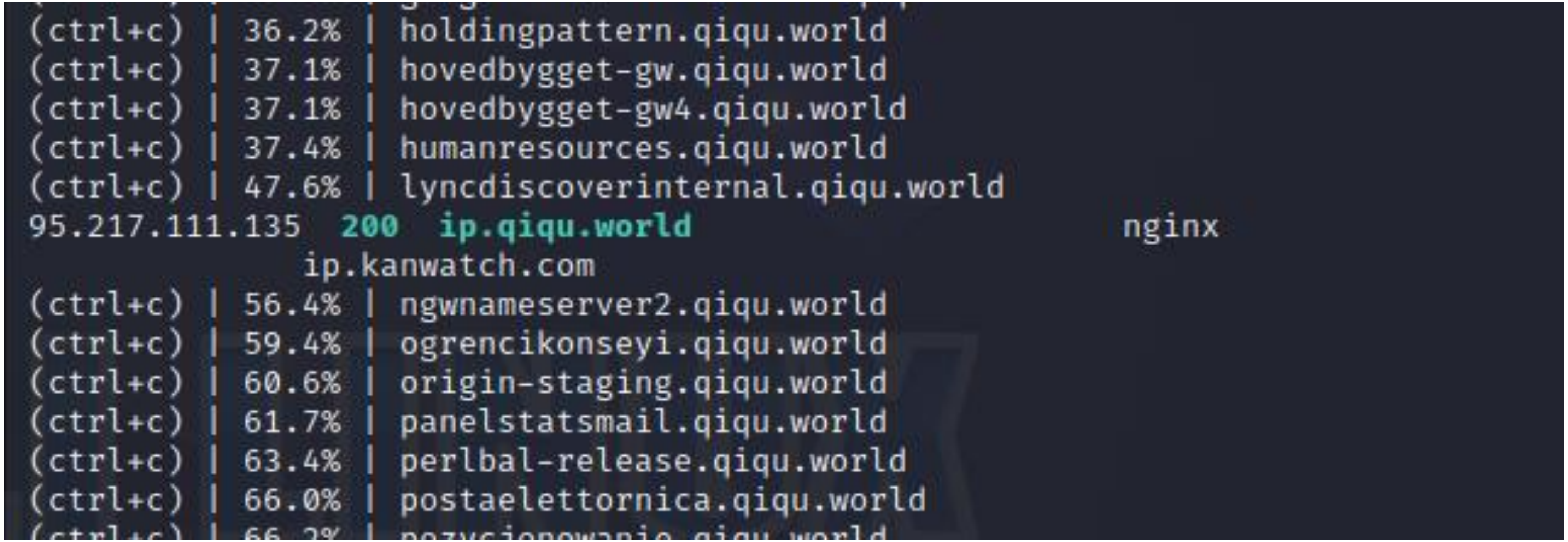
```
local: 10757 | remote: 3

Wordlist: 10760 | Target: qiqu.world | Ip: 104.21.234.188

14:03:52

Ip address          Code Subdomain                              Server
                  Real hostname

(ctrl+c) | 2.29% | administracion.qiqu.world
(ctrl+c) | 2.31% | administration.qiqu.world
(ctrl+c) | 2.33% | administrators.qiqu.world
(ctrl+c) | 2.80% | ag-kopf-moertz.qiqu.world
(ctrl+c) | 8.85% | bibliotecadigital.qiqu.world
(ctrl+c) | 9.11% | bioinformatics.qiqu.world
(ctrl+c) | 14.2% | cisco-capwap-controller.qiqu.world
(ctrl+c) | 14.3% | cisco-lwapp-controller.qiqu.world
(ctrl+c) | 14.8% | cloudflare-resolve-to.qiqu.world
(ctrl+c) | 15.7% | commerceserver.qiqu.world
(ctrl+c) | 15.8% | communications.qiqu.world
(ctrl+c) | 19.4% | customerservice.qiqu.world
```

即可獲得相關的 Subdomain(2/3)



```
(ctrl+c) | 63.4% | perlbal-release.qiqu.world
(ctrl+c) | 66.0% | postaelettornica.qiqu.world
(ctrl+c) | 66.2% | pozycjonowanie.qiqu.world
(ctrl+c) | 66.6% | pre-production.qiqu.world
(ctrl+c) | 67.1% | problemtracker.qiqu.world
(ctrl+c) | 70.5% | release-chat-service.qiqu.world
(ctrl+c) | 70.6% | release-commondata.qiqu.world
(ctrl+c) | 71.5% | rideofthemonth.qiqu.world
(ctrl+c) | 74.7% | sandd-dev-commondata.qiqu.world
(ctrl+c) | 75.0% | savvis-admin-commondata.qiqu.world
(ctrl+c) | 75.0% | savvis-dev-commondata.qiqu.world
(ctrl+c) | 75.9% | segnalazionicloud.qiqu.world
(ctrl+c) | 82.1% | staging-chat-service.qiqu.world
(ctrl+c) | 82.2% | staging-commondata.qiqu.world
(ctrl+c) | 83.3% | studentaffairs.qiqu.world
(ctrl+c) | 84.0% | sustainability.qiqu.world
(ctrl+c) | 85.7% | telechargement.qiqu.world
(ctrl+c) | 85.9% | terminalserver.qiqu.world
(ctrl+c) | 91.2% | veranstaltungen.qiqu.world
(ctrl+c) | 91.6% | videoconferencia.qiqu.world
104.21.234.189  200  video.qiqu.world                     cloudflare

104.21.234.188  200  www.qiqu.world                       cloudflare
```

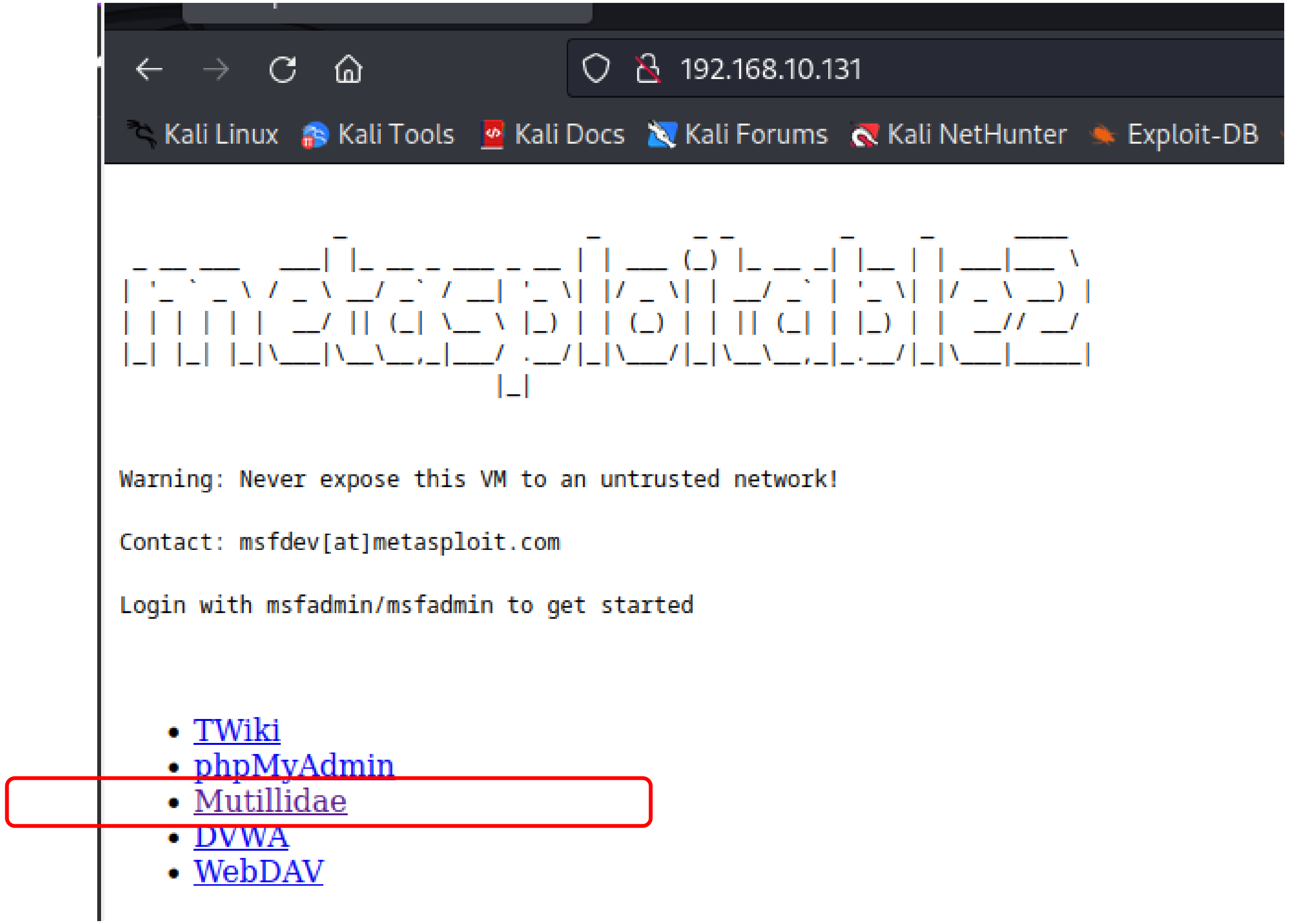
即可獲得相關的 Subdomain(3/3)



```
(ctrl+c) | 36.2% | holdingpattern.qiqu.world
(ctrl+c) | 37.1% | hovedbygget-gw.qiqu.world
(ctrl+c) | 37.1% | hovedbygget-gw4.qiqu.world
(ctrl+c) | 37.4% | humanresources.qiqu.world
(ctrl+c) | 47.6% | lyncdiscoverinternal.qiqu.world
95.217.111.135  200  ip.qiqu.world                      nginx
              ip.kanwatch.com
(ctrl+c) | 56.4% | ngwnameserver2.qiqu.world
(ctrl+c) | 59.4% | ogrencikonseyi.qiqu.world
(ctrl+c) | 60.6% | origin-staging.qiqu.world
(ctrl+c) | 61.7% | panelstatsmail.qiqu.world
(ctrl+c) | 63.4% | perlbal-release.qiqu.world
(ctrl+c) | 66.0% | postaelettornica.qiqu.world
(ctrl+c) | 66.2% | pozycjonowanie.qiqu.world
```

5. Dirb

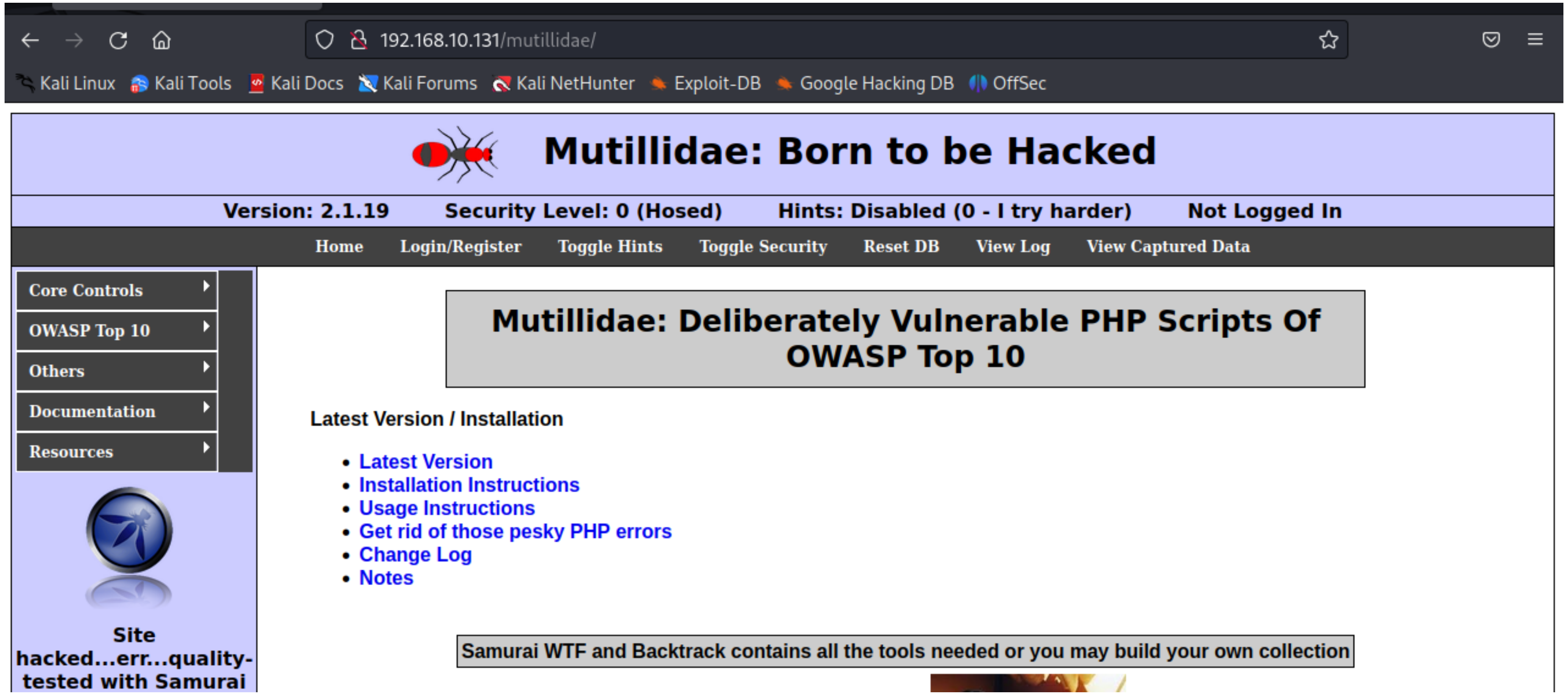
開啟 metasploitable2 中的 Mutillidae



```
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

網站頁面



Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

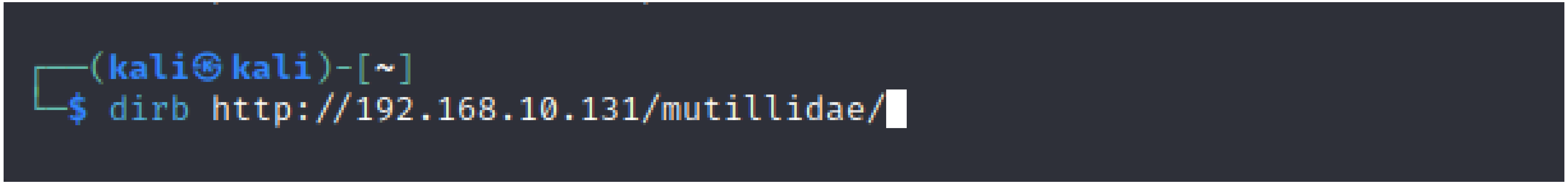
- Latest Version
- Installation Instructions
- Usage Instructions
- Get rid of those pesky PHP errors
- Change Log
- Notes

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

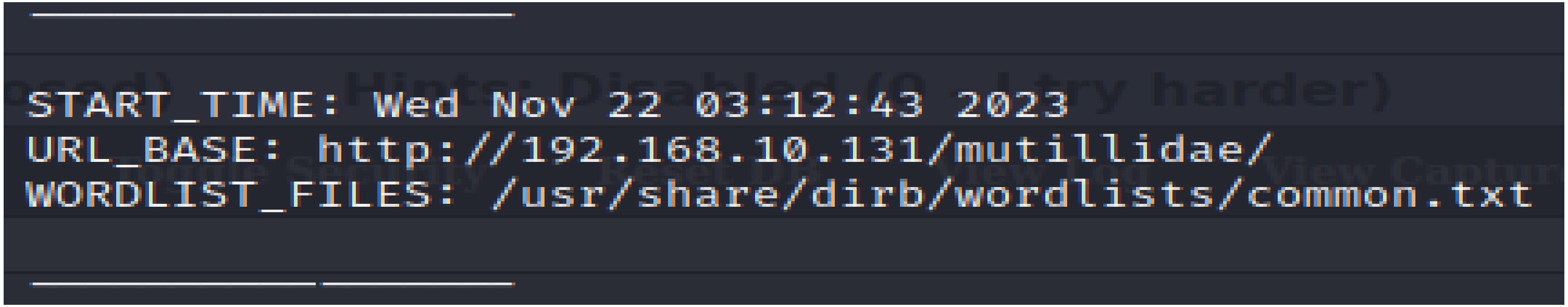
Site hacked...err...quality-tested with Samurai

使用 dirb 根據目標網路鏡進行目錄檢測

Command:
dirb [目標網站路徑]

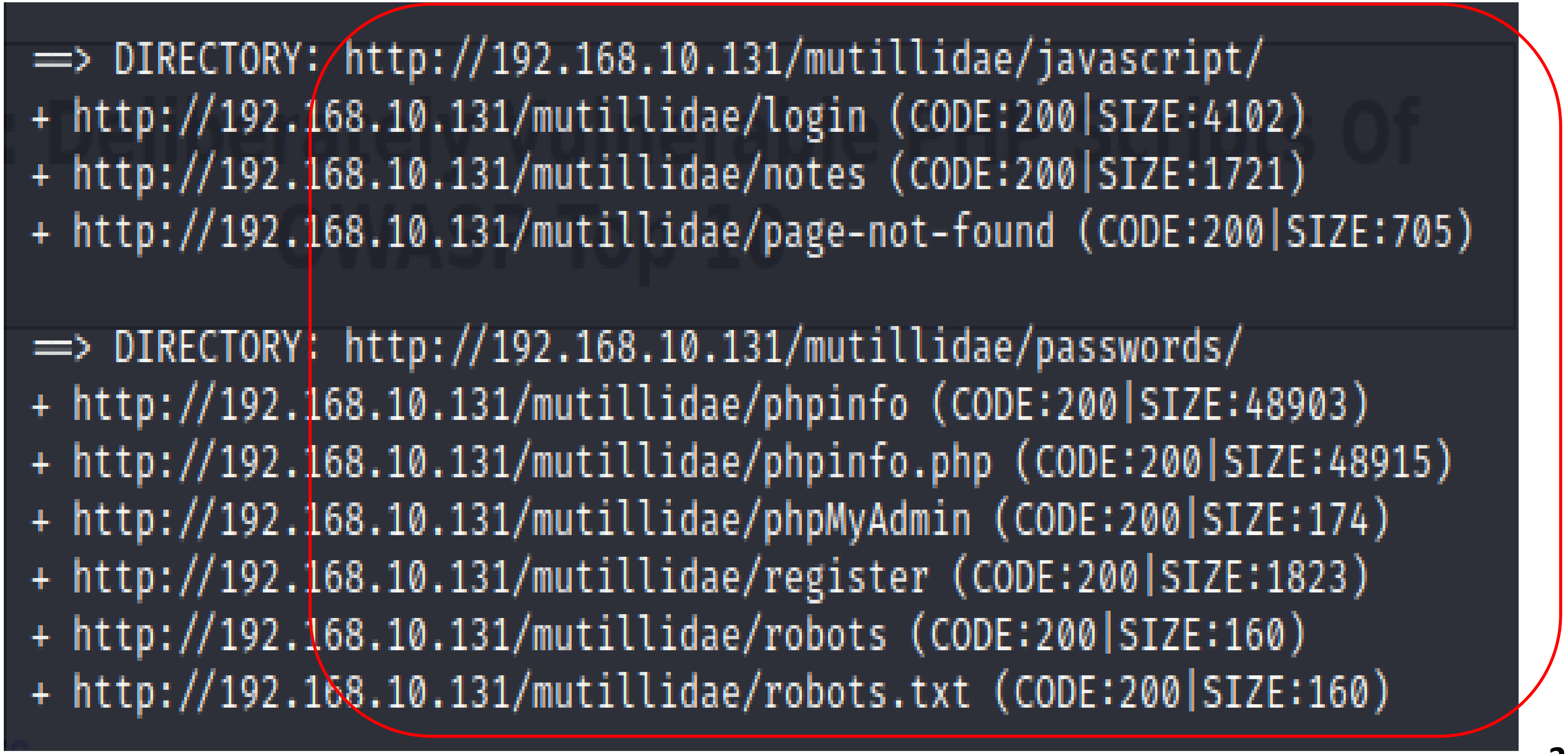


```
┌──(kali㉿kali)-[~]
└─$ dirb http://192.168.10.131/mutillidae/
```



```
START_TIME: Wed Nov 22 03:12:43 2023
URL_BASE: http://192.168.10.131/mutillidae/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

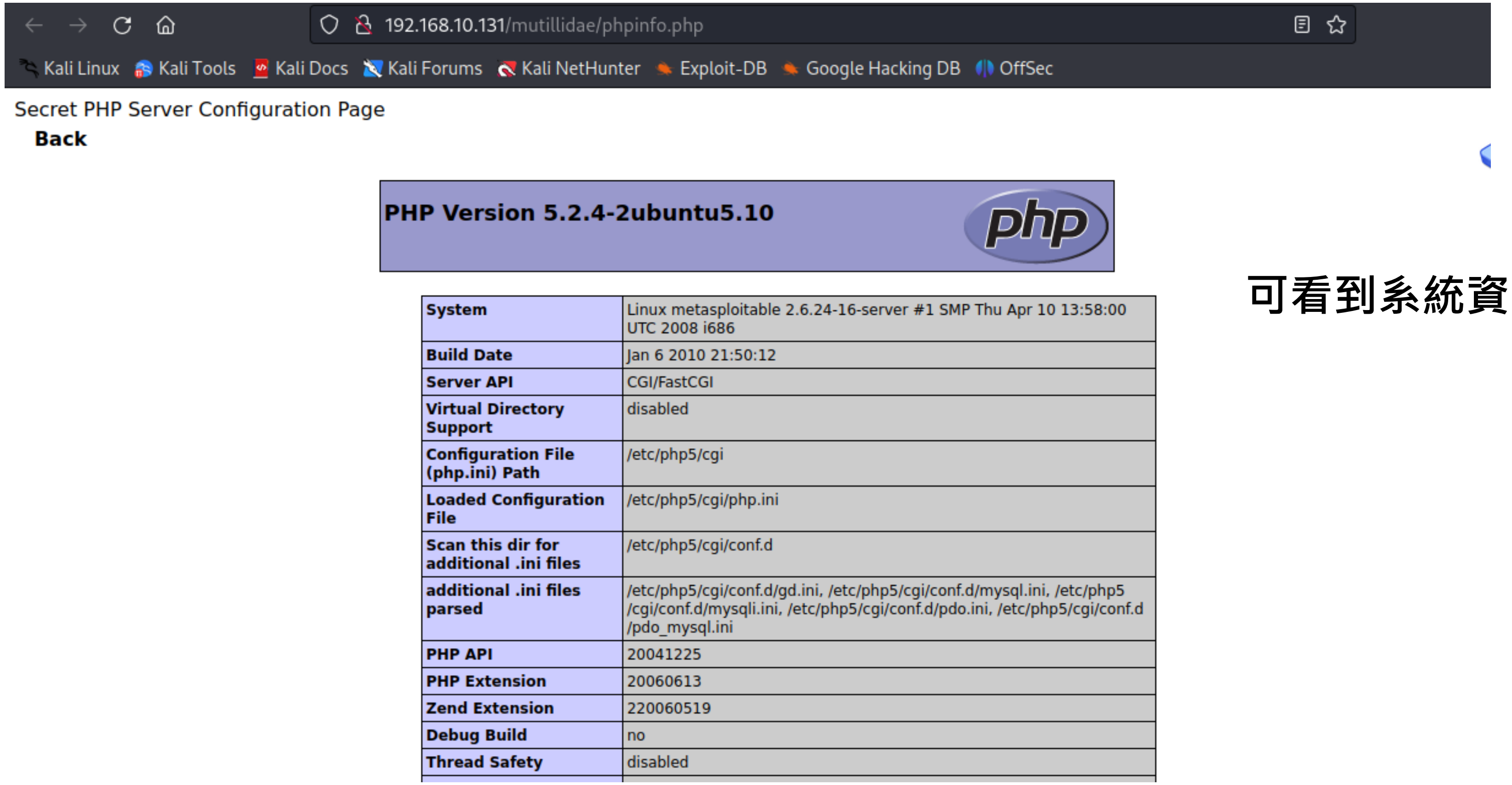
發現相關重要目錄



```
==> DIRECTORY: http://192.168.10.131/mutillidae/javascript/
+ http://192.168.10.131/mutillidae/login (CODE:200|SIZE:4102)
+ http://192.168.10.131/mutillidae/notes (CODE:200|SIZE:1721)
+ http://192.168.10.131/mutillidae/page-not-found (CODE:200|SIZE:705)

==> DIRECTORY: http://192.168.10.131/mutillidae/passwords/
+ http://192.168.10.131/mutillidae/phpinfo (CODE:200|SIZE:48903)
+ http://192.168.10.131/mutillidae/phpinfo.php (CODE:200|SIZE:48915)
+ http://192.168.10.131/mutillidae/phpMyAdmin (CODE:200|SIZE:174)
+ http://192.168.10.131/mutillidae/register (CODE:200|SIZE:1823)
+ http://192.168.10.131/mutillidae/robots (CODE:200|SIZE:160)
+ http://192.168.10.131/mutillidae/robots.txt (CODE:200|SIZE:160)
```

實際查看

192.168.10.131/mutillidae/phpinfo.php



Secret PHP Server Configuration Page

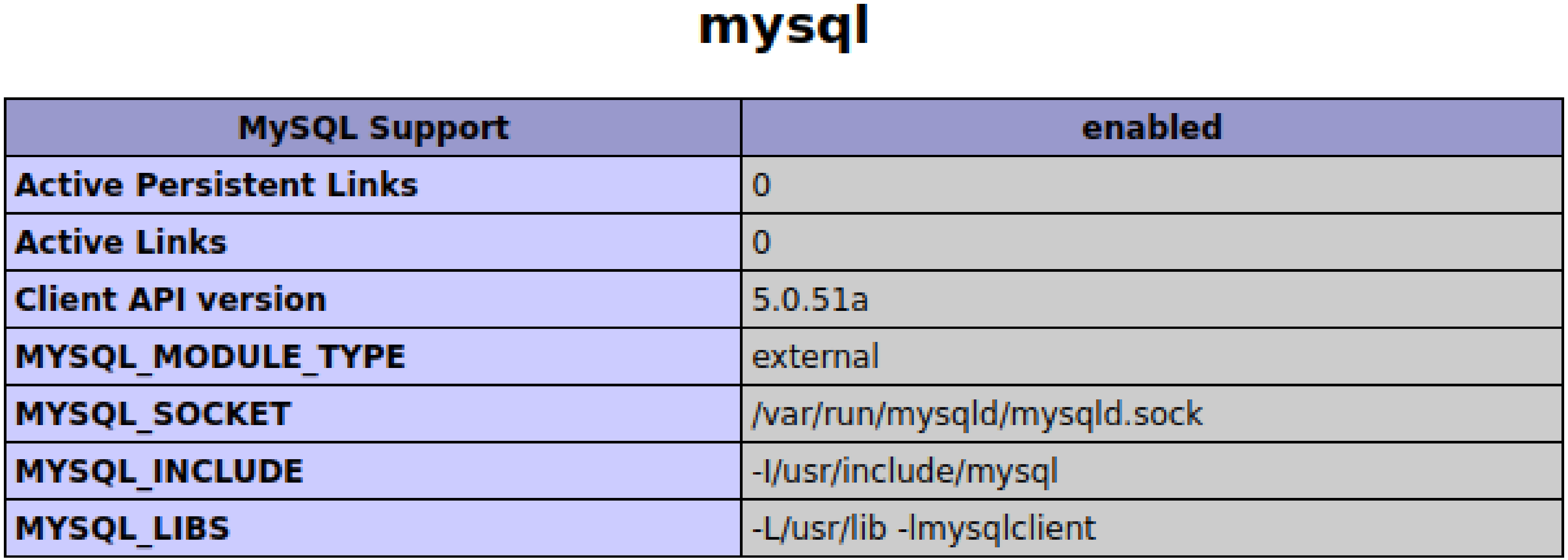
Back

PHP Version 5.2.4-2ubuntu5.10

System	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled

可看到系統資訊

使用的資料庫



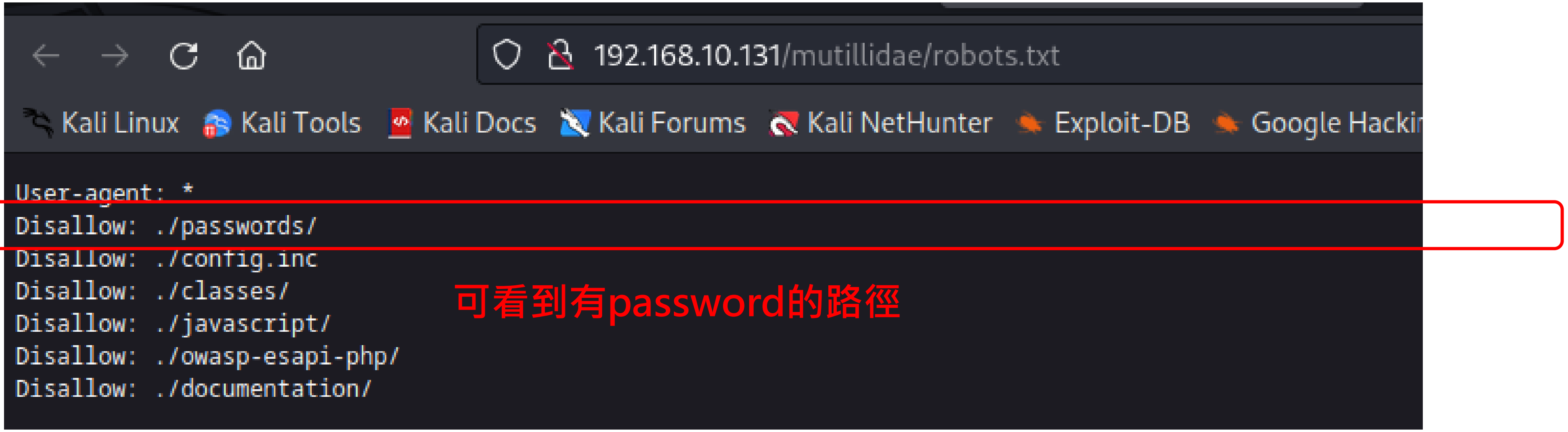
mysql

MySQL Support	enabled
Active Persistent Links	0
Active Links	0
Client API version	5.0.51a
MYSQL_MODULE_TYPE	external
MYSQL_SOCKET	/var/run/mysqld/mysqld.sock
MYSQL_INCLUDE	-I/usr/include/mysql
MYSQL_LIBS	-L/usr/lib -lmysqlclient

查看robot.txt

192.168.10.131/mutillidae/robot.txt

robot.txt 為不允許被蒐尋的路徑，代表都是存有重要資訊的路徑

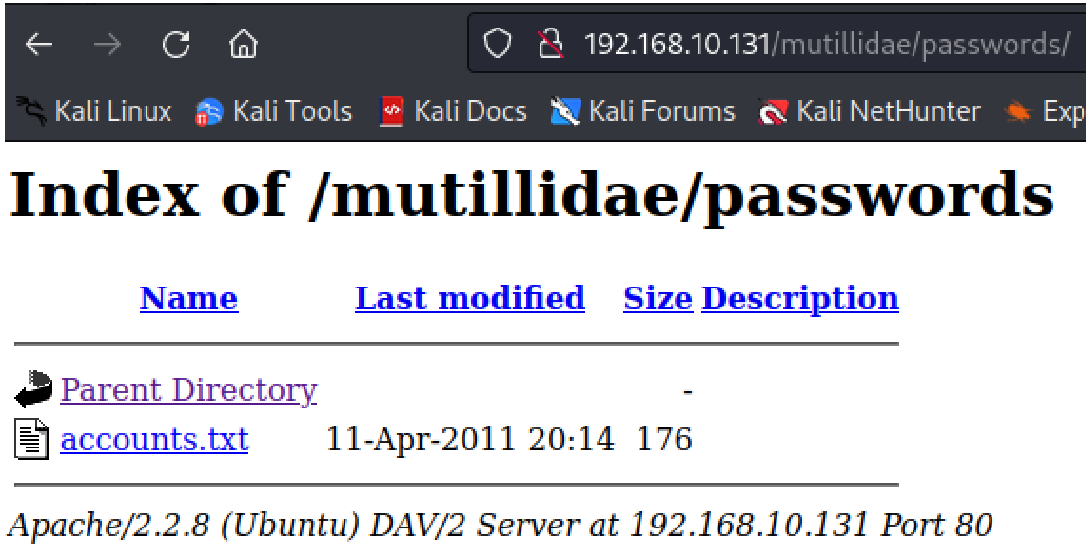


```
User-agent: *
Disallow: ./passwords/
Disallow: ./config.inc
Disallow: ./classes/
Disallow: ./javascript/
Disallow: ./owasp-esapi-php/
Disallow: ./documentation/
```

可看到有password的路徑

實際查看.password路徑

192.168.10.131/mutillidae/passwords



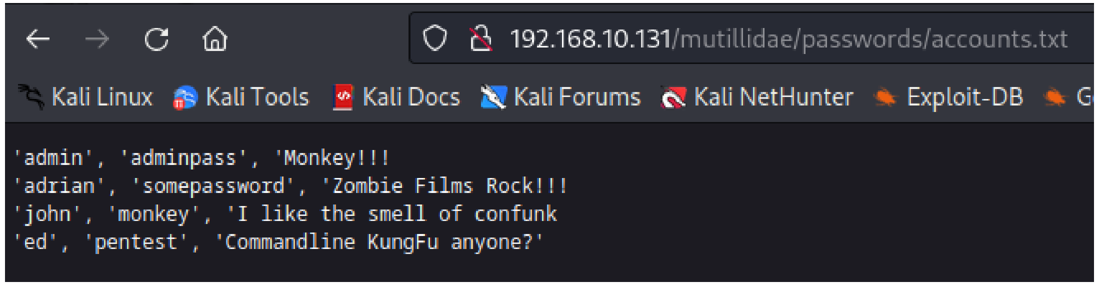
Index of /mutillidae/passwords

Name	Last modified	Size	Description
Parent Directory		-	
accounts.txt	11-Apr-2011 20:14	176	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.10.131 Port 80

點選 accounts.txt

可發現 帳號與密碼



```
'admin', 'adminpass', 'Monkey!!!
'adrian', 'somepassword', 'Zombie Films Rock!!!
'john', 'monkey', 'I like the smell of confunk
'ed', 'pentest', 'Commandline KungFu anyone?'
```

End