Threat Hunting

HW03 - Use Pentest tools to hunting threat

Name: 劉定睿 ID: M11409313

Date: 2025-10-02

目錄

- 目錄
  - whois
  - DNS
  - Certificate Transparency
  - VirusTotal
  - Google dorks
  - BuiltWith / Wappalyzer
  - Photon
  - Dirhunt / wfuzz / wfuzz-like tools
  - CMSMap / WPScan
  - curl

> Claim: All of the action are conduct in my personal domain. The leak informations are Purposely.

whois

First of all, I use `whois` to check the information of this domain name. The information shows that this domain is host in cloudflare server. So I can't obtain the correct information of the personal and server.

```
└─$ whois jonakf555.org
Domain Name: jonakf555.org
Registry Domain ID: REDACTED
Registrar WHOIS Server: http://whois.cloudflare.com
Registrar URL: http://www.cloudflare.com
Updated Date: 2025-09-14T12:14:21Z
Creation Date: 2025-09-09T12:13:28Z
Registry Expiry Date: 2026-09-09T12:13:28Z
Registrar: Cloudflare, Inc.
Registrar IANA ID: 1910
Registrar Abuse Contact Email: registrar-abuse@cloudflare.com
Registrar Abuse Contact Phone: +1.6503198930
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: clark.ns.cloudflare.com
Name Server: paris.ns.cloudflare.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://icann.org/wicf/
>>> Last update of WHOIS database: 2025-09-26T06:40:44Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

DNS

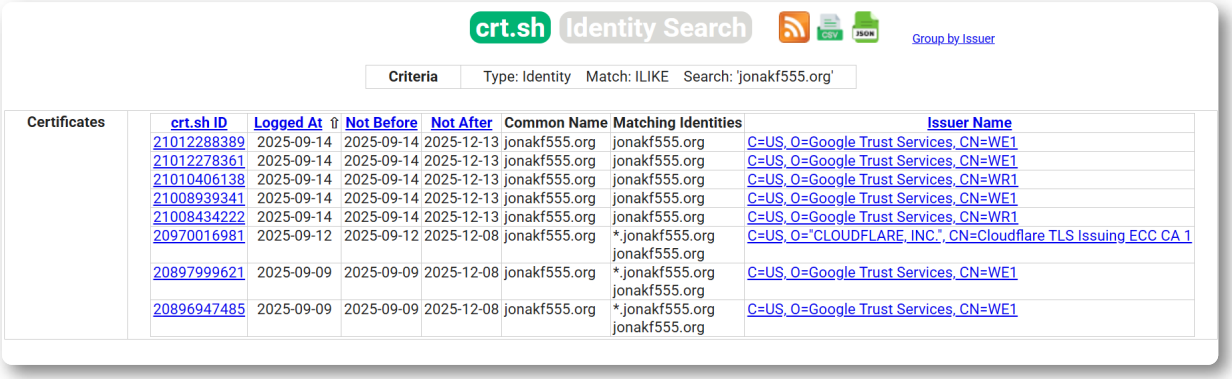
Then I check the DNS record via `dnsdumpster`.

A Records (subdomains from dataset)

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
jonakf555.org	172.67.194.32	ASN: 13335 172.67.192.0/20	CLOUDFLARENET	http: cloudflare title: Direct IP access not allowed tech: Cloudflare http8080: cloudflare title: Direct IP access not allowed tech: Cloudflare	558
jonakf555.org	104.21.20.200	ASN: 13335 104.21.16.0/20	CLOUDFLARENET	http: cloudflare title: Just a moment... tech: Cloudflare http8080: cloudflare title: Direct IP access not allowed tech: Cloudflare	534

Certificate Transparency

After that. I search the certificate transparency record data via `crt.sh`.



crt.sh Identity Search — Group by Issuer

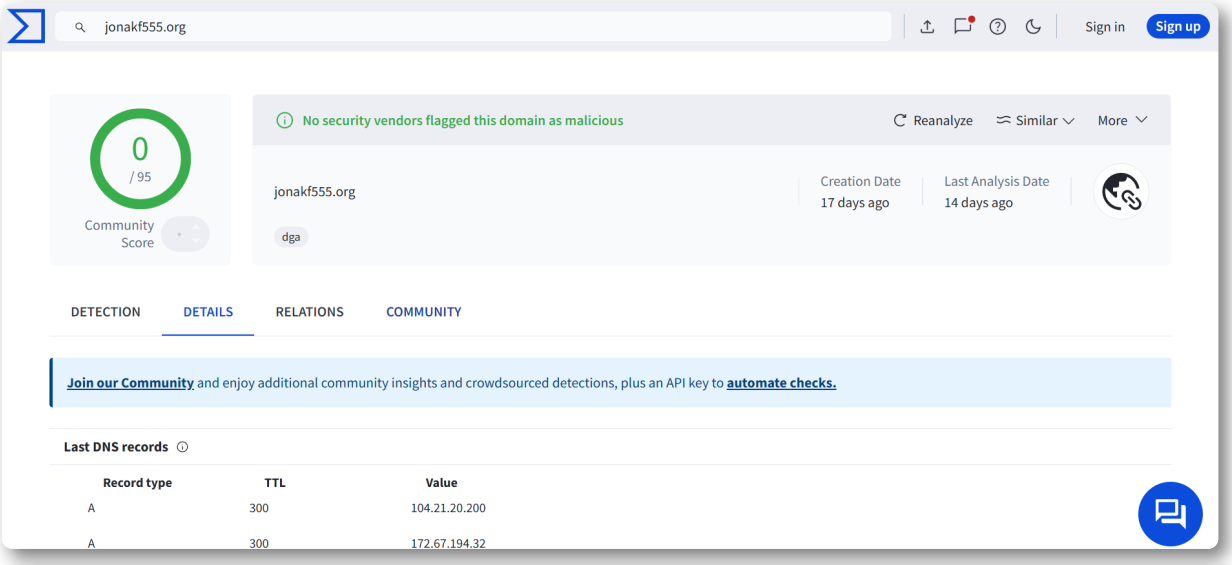
Criteria: Type: Identity Match: ILIKE Search: 'jonakf555.org'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
21012288389	2025-09-14	2025-09-14	2025-12-13	jonakf555.org	jonakf555.org	C=US, O=Google Trust Services, CN=WE1
21012278361	2025-09-14	2025-09-14	2025-12-13	jonakf555.org	jonakf555.org	C=US, O=Google Trust Services, CN=WE1
21010406138	2025-09-14	2025-09-14	2025-12-13	jonakf555.org	jonakf555.org	C=US, O=Google Trust Services, CN=WR1
21008939341	2025-09-14	2025-09-14	2025-12-13	jonakf555.org	jonakf555.org	C=US, O=Google Trust Services, CN=WE1
21008434222	2025-09-14	2025-09-14	2025-12-13	jonakf555.org	jonakf555.org	C=US, O=Google Trust Services, CN=WR1
20970016981	2025-09-12	2025-09-12	2025-12-08	jonakf555.org	*.jonakf555.org jonakf555.org	C=US, O="CLOUDFLARE, INC.", CN=Cloudflare TLS Issuing ECC CA 1
20897999621	2025-09-09	2025-09-09	2025-12-08	jonakf555.org	*.jonakf555.org jonakf555.org	C=US, O=Google Trust Services, CN=WE1
20896947485	2025-09-09	2025-09-09	2025-12-08	jonakf555.org	*.jonakf555.org jonakf555.org	C=US, O=Google Trust Services, CN=WE1

VirusTotal

Virustotal help me to check lot of infos. ex: malicious or not? and relation data ... .



jonakf555.org — Sign in — Sign up

0 / 95 Community Score

No security vendors flagged this domain as malicious — Reanalyze — Similar — More

jonakf555.org

dga

Creation Date: 17 days ago

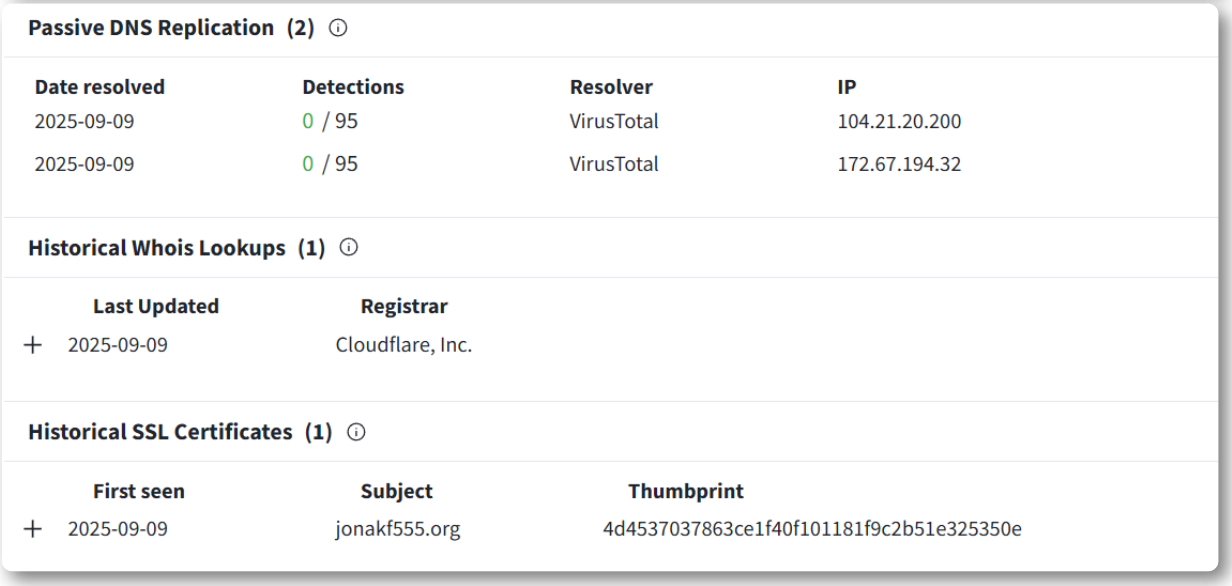
Last Analysis Date: 14 days ago

DETECTION DETAILS RELATIONS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Last DNS records

Record type	TTL	Value
A	300	104.21.20.200
A	300	172.67.194.32



Passive DNS Replication (2)

Date resolved	Detections	Resolver	IP
2025-09-09	0 / 95	VirusTotal	104.21.20.200
2025-09-09	0 / 95	VirusTotal	172.67.194.32

Historical Whois Lookups (1)

	Last Updated	Registrar
+	2025-09-09	Cloudflare, Inc.

Historical SSL Certificates (1)

	First seen	Subject	Thumbprint
+	2025-09-09	jonakf555.org	4d4537037863ce1f40f101181f9c2b51e325350e

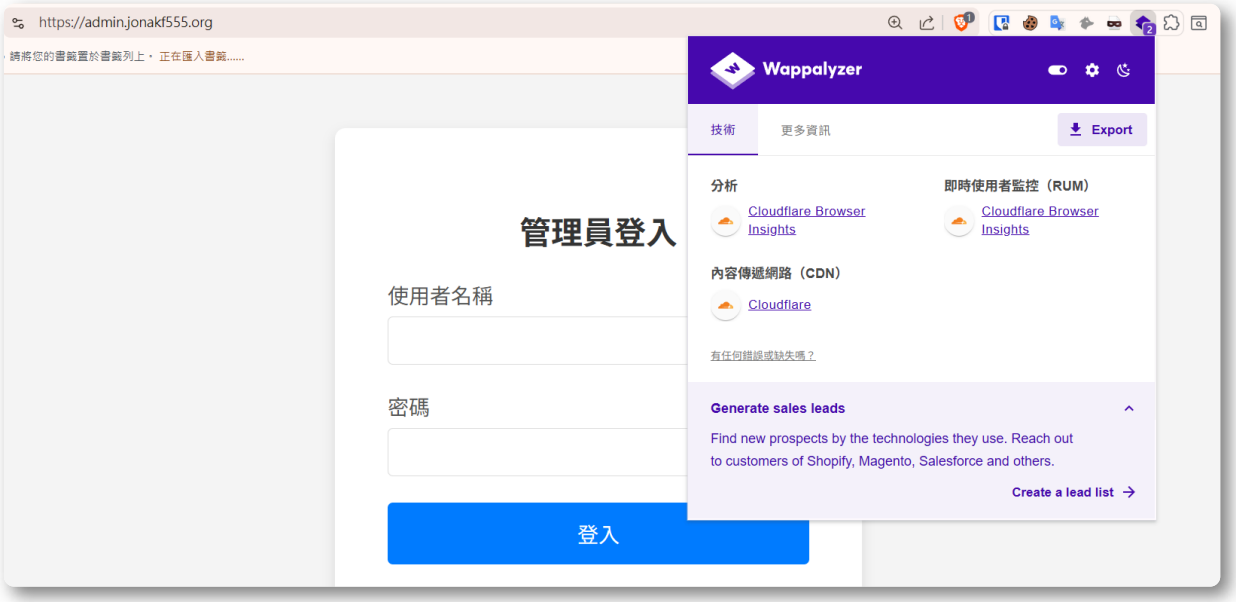
Google dorks

Google Dorking a.k.a. Google Hacking can find lot of infomation. In this case, there's not too much things I can collect.

```
- site:"jonakf555.org"
```

BuiltWith / Wappalyzer

After Check the informations by passive recon. I connect to the URL and do active recon. I check the website information by Wappalyzer.



Photon

Scanner tool photon help me to collect different data. These datas come from website's javascript.

```
└─$ photon --keys -u https://jonakf555.org
        ____  __          __
       / __ \/ /_  ____  / /_____  ____
      / /_/ / __ \/ __ \/ __/ __ \/ __ \
     / ____/ / / / /_/ / /_/ /_/ / / / /
    /_/   /_/ /_/\____/\__/\____/_/ /_/ v1.2.2

[+] URLs retrieved from robots.txt: 1
[~] Level 1: 2 URLs
[!] Progress: 2/2
[~] Level 2: 2 URLs
[!] Progress: 2/2
[~] Crawling 2 JavaScript files
[!] Progress: 2/2
-------------------------------------------------
[+] Robots: 1
[+] Internal: 4
[+] Scripts: 2
[+] External: 2
-------------------------------------------------
[!] Total requests made: 7
[!] Total time taken: 0 minutes 2 seconds
[!] Requests per second: 2
[+] Results saved in jonakf555.org directory
```

```
└─$ cat external.txt
https://github.com/jonafk555
https://www.linkedin.com/in/jonathan-liu-localhost/
```

```
└─$ cat internal.txt
https://jonakf555.org/cdn-cgi/l/email-protection
https://jonakf555.org//cdn-cgi/l/email-protection
https://jonakf555.org
https://jonakf555.org/
```

```
└─$ cat robots.txt
https://jonakf555.org/
```

```
└─$ cat scripts.txt
https://jonakf555.org/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js
https://jonakf555.org/cdn-cgi/challenge-platform/scripts/jsd/main.js;document.getElementsByTagName(head)[0].ap
pendChild(a);;b.getElementsByTagName(head)[0].appendChild(d)}}if(document.body){var
```

Dirhunt / wfuzz / wfuzz-like tools

Later, I use `dirb` to fuzzing the website. Then I find a `secrets.txt`. The file leak sensitive information.

```
└─$ dirb https://jonakf555.org -X .txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Sep 26 15:40:12 2025
URL_BASE: https://jonakf555.org/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.txt) | (.txt) [NUM = 1]

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://jonakf555.org/ ----
+ https://jonakf555.org/secrets.txt (CODE:200|SIZE:25)
```

CMSMap / WPScan

Because this website isn't use wordpress to creat. So wpscan hasn't provide useful information.

```
└─$ wpscan --url https://jonakf555.org
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

Scan Aborted: The remote website is up, but does not seem to be running WordPress.
```

Cmsmap's result are similar as wpscan.

```
└─$ cmsmap https://jonakf555.org
[-] Date & Time: 28/09/2025 21:44:26
[I] Threads: 5
[-] Target: https://jonakf555.org (172.67.194.32)
[I] Server: cloudflare
[L] X-Frame-Options: Not Enforced
[I] Strict-Transport-Security: Not Enforced
[I] X-Content-Security-Policy: Not Enforced
[L] Robots.txt Found: https://jonakf555.org/robots.txt
[I] CMS Detection: WordPress
[M] XML-RPC services are enabled
[I] Autocomplete Off Not Found: https://jonakf555.org/wp-login.php
[-] Default WordPress Files:
[-] Searching Wordpress Plugins ...
11%Exception in thread Thread-3:
```

curl

curl can shows the website front-end code. I found the username and password.

```
└─$ curl -L https://admin.jonakf555.org
<!DOCTYPE html>
<html lang="zh-TW">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>管理員登入</title>
    <link rel="stylesheet" href="style.css">
</head>
<body>
    <div class="login-container">
        <form id="login-form">
            <h2>管理員登入</h2>
            <div class="input-group">
                <label for="username">使用者名稱</label>
                <input type="text" id="username" name="username" required>
            </div>
            <div class="input-group">
                <label for="password">密碼</label>
                <input type="password" id="password" name="password" required>
            </div>
                <!-- username:admin, password:6yhb5tgv7ujkl -->
            <button type="submit" class="login-button">登入</button>
```