CONFLUENT

How safe is your domain?

Michael Kehoe
Sr Staff Security Engineer

Agenda

01 $ whoami

02 Introduction

03 DNS & Domain threat models

04 Top 1000 domain statistics

05 Registrar protection

06 Nameserver safety

07 DNS records for mail

08 Other best practices

09 Demo: Domain-Labs.com

10 Q & A

$ whoami

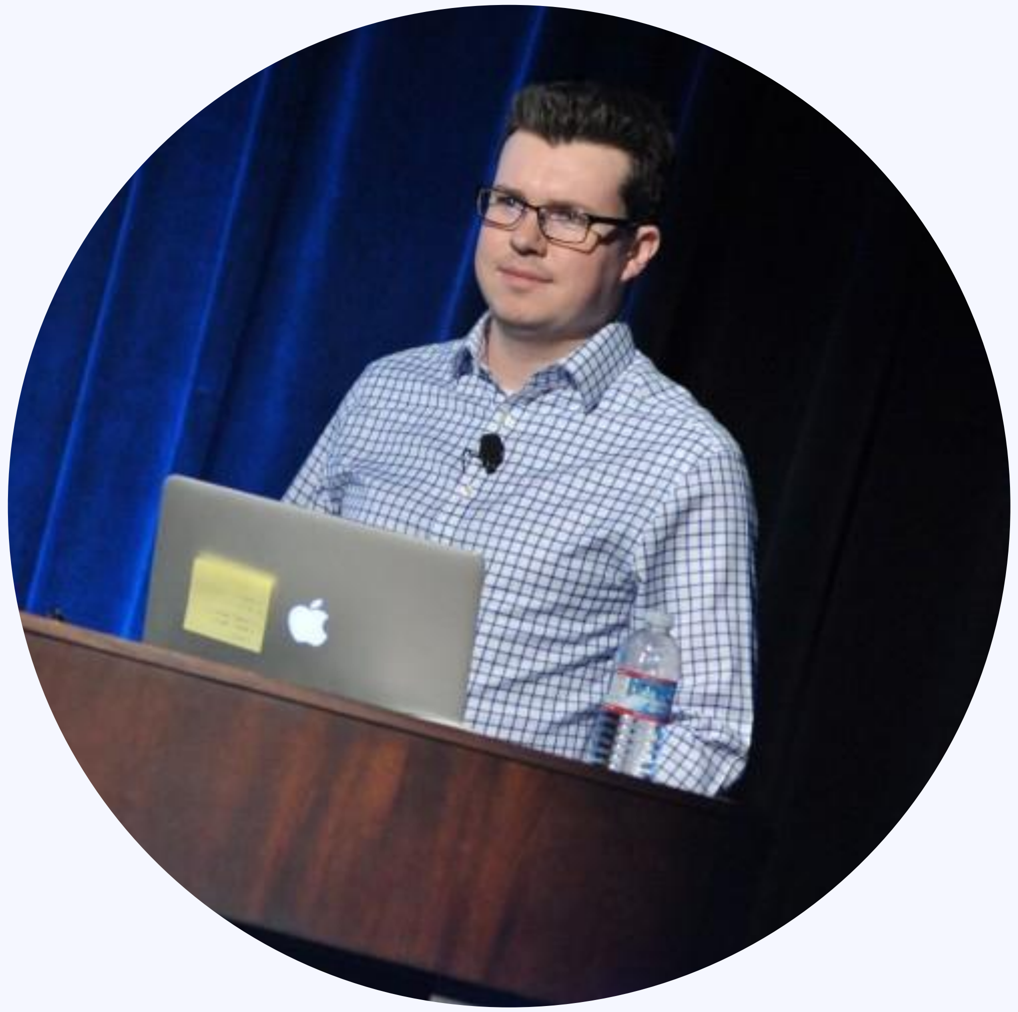
$ whoami

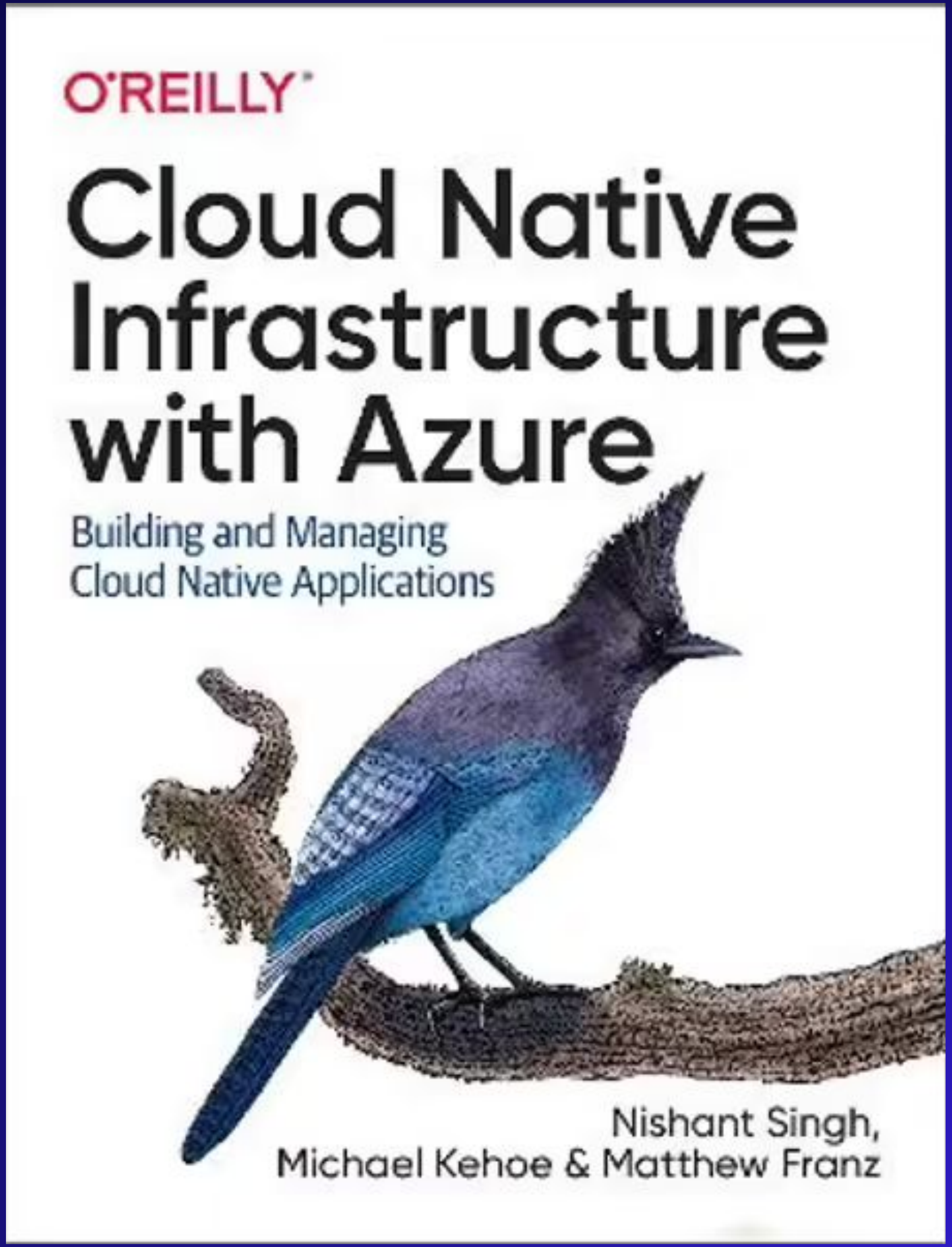
- Sr Staff Security Engineer - Confluent
  - Cloud Architecture & Reliability

- Previously:
  - Sr Staff SRE @ LinkedIn
  - PhoneSat intern @ NASA

- Background in:
  - Networks
  - Microservices
  - Traffic Engineering
  - KV Databases
  - Incident Management

- Twitter: @michaelkkehoe
- LinkedIn: linkedin.com/in/michaelkkkehoe
- Website: michael-kehoe.io



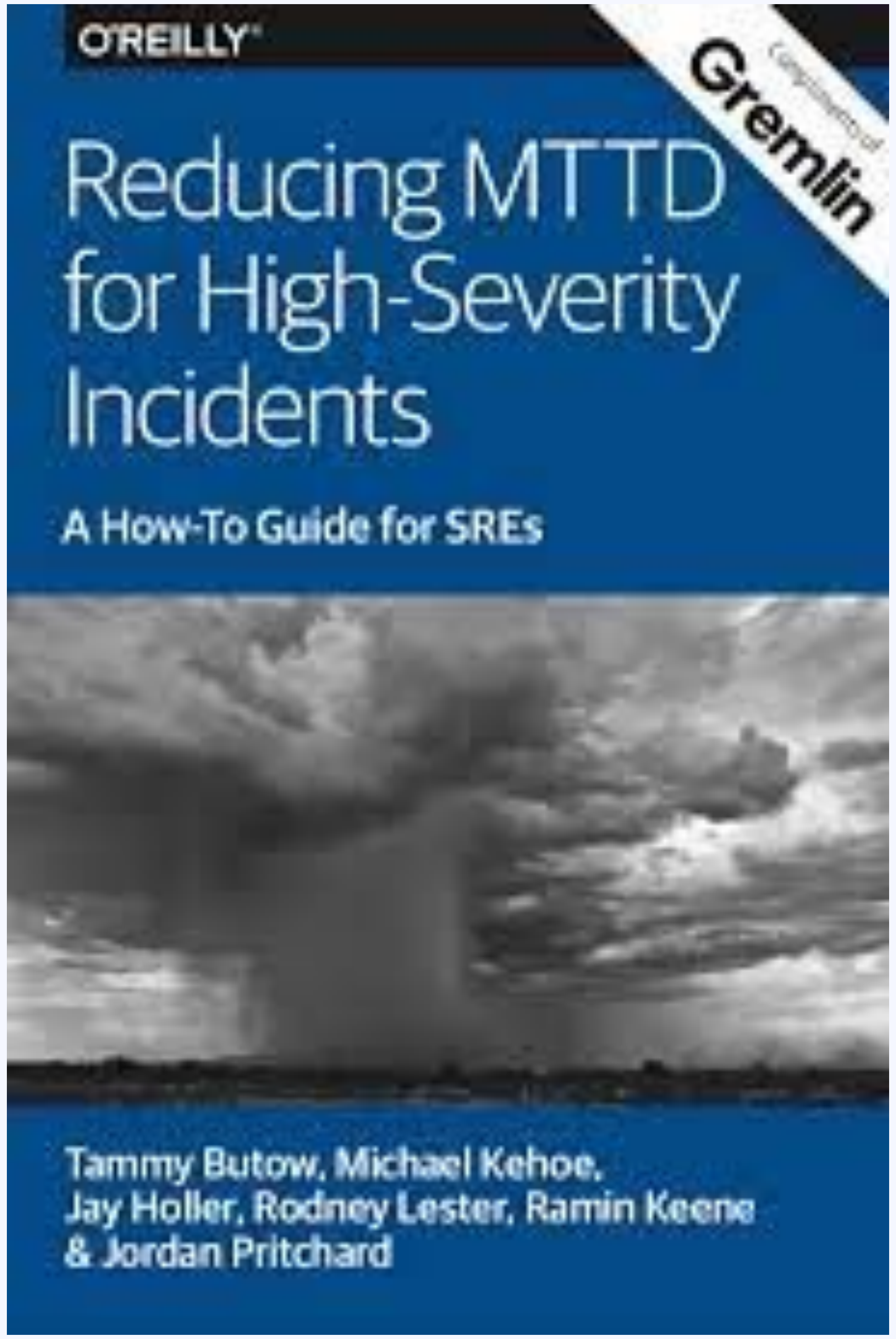


O'REILLY

Cloud Native Infrastructure with Azure

Building and Managing Cloud Native Applications

Nishant Singh, Michael Kehoe & Matthew Franz



O'REILLY

Compliments of Gremlin

Reducing MTTD for High-Severity Incidents

A How-To Guide for SREs

Tammy Butow, Michael Kehoe, Jay Holler, Rodney Lester, Ramin Keene & Jordan Pritchard

Introduction

Threat-models for DNS & Domains

Basic DNS Threat model

01	Denial of Service/ Availability	• DNS records are resolvable during outage/ DDoS
02	Spoofing/ Authentication	• Pretending to be someone else (i.e mail spoofing) • Typosquatting/ Bitflipping/ Homoglyph on domains
03	Tampering/ Integrity	• Modifying DNS responses in-transit
04	Repudiation/ non-repudiation	• Verified mail senders
05	Information disclosure/ Confidentiality	• Intercepting DNS traffic • Intercepting mail or other layer-7 services

Top 1000* domain statistics

* Cloudflare Radar Top 1000 domains (only 929 domains provided full results)

How many domains are following all best-practices?

Domain Locks

17%

Implement all controls

All 6 Server Lock & Client Locks are implemented

38%

Implement half of controls

All 3 Client Locks are implemented

36%

Implement one control

1 Client lock is implemented

9%

No controls implemented

No server lock or client lock is implemented

Nameserver Safety

25%

Utilize diverse nameservers

Utilize more than 1 DNS provider

75%

Do not have diverse nameservers

Only use 1 provider

5%

Implement DNSSec

Protects the integrity of DNS responses

95%

Do not implement DNSSec

Responses could be tampered with

Mail Server Safety

68%

Have a SPF record

Specify which IPs can send mail for your domain

58%

Have a DMARC record

Policy for unauthenticated messages

0.2%

Implement TLSA

Authenticates public key of certificate with the TLS connection

1.5%

Implement MTA-STS

Policy for determining if inbound mail must be encrypted

Misc Controls

8%

Implement security.txt

Lets the public know how to report security issues

25%

Implement CAA

Lists which Certificate Authorities can issue a certificate against your domain

What are the best practices?

Registrar Protection

Registrar Protection

Enable all locks

Ensure that your domain can only be modified through established procedures with the registrar

Enable 2FA

Utilize (non-SMS) 2FA to provide extra security for account credentials.

Implement IP controls

Only allow your IP space to access your domain registrar

Integrate SSO

If possible, authenticate with your domain registrar through your existing SSO solution.

Registrars that support server-locks

Known supporting registrars

- MarkMonitor, Inc.
- NOM-IQ Ltd dba Com Laude
- CSC CORPORATE DOMAINS, INC.
- RegistrarSafe, LLC
- Cloudflare, Inc.
- Nameshield SAS
- RegistrarSEC, LLC
- (Shanghai) Co., Ltd.
- Lexsynergy Limited
- Safenames Ltd

Nameserver Safety

Name Server Safety

Implement DNSSec

Ensure that DNS results for your domain are not modified by MITM attackers

Use multiple DNS providers

Remove a single point of failure and reduce the risk of DDOS/ failure taking down your domains DNS resolution

DNS Records for Mail

DNS Records for Mail

1. **SPF**

   Specify what IP addresses can send email addresses for your domain

2. **DMARC/ DKIM**

   DMARC: Policy for authenticating email and reporting
   DKIM: Provides authentication for email senders using public-keys

3. **TLSA**

   DNS record that is a SHA256 hash of the certificate public-key

4. **MTA-STS**

   Policy stating your domain requires authentication and encryption for SMTP connections.

5. **SMTP-TLS**

   Enables standard reporting on senders ability for secure email delivery to your domain.

6. **BIMI/ VMC**

   An open standard that allows email senders to use their brand logo in emails.

https://email-security-scans.org/
https://support.google.com/mail/answer/13130196
https://www.mailhardener.com/

Records for domains that do not send mail

SPF	TXT	Host: yourdomain.com Value: v=spfv1 -all
DMARC	TXT	Host: _dmarc.yourdomain.com Value: v=DMARC1;p=reject;sp=reject;adkim=s;aspf=s;fo=1;rua=mailto:dmarc@anotherdomain.com
DKIM	TXT	Host: *._domainkey.yourdomain.com Value: v=DKIM1; p=
MX	MX	Host: yourdomain.com Priority: 0 Value .

https://www.gov.uk/guidance/protect-domains-that-dont-send-email

Other best security practices

Content with icons

Implement security.txt

Let people know where/ how to report security issues

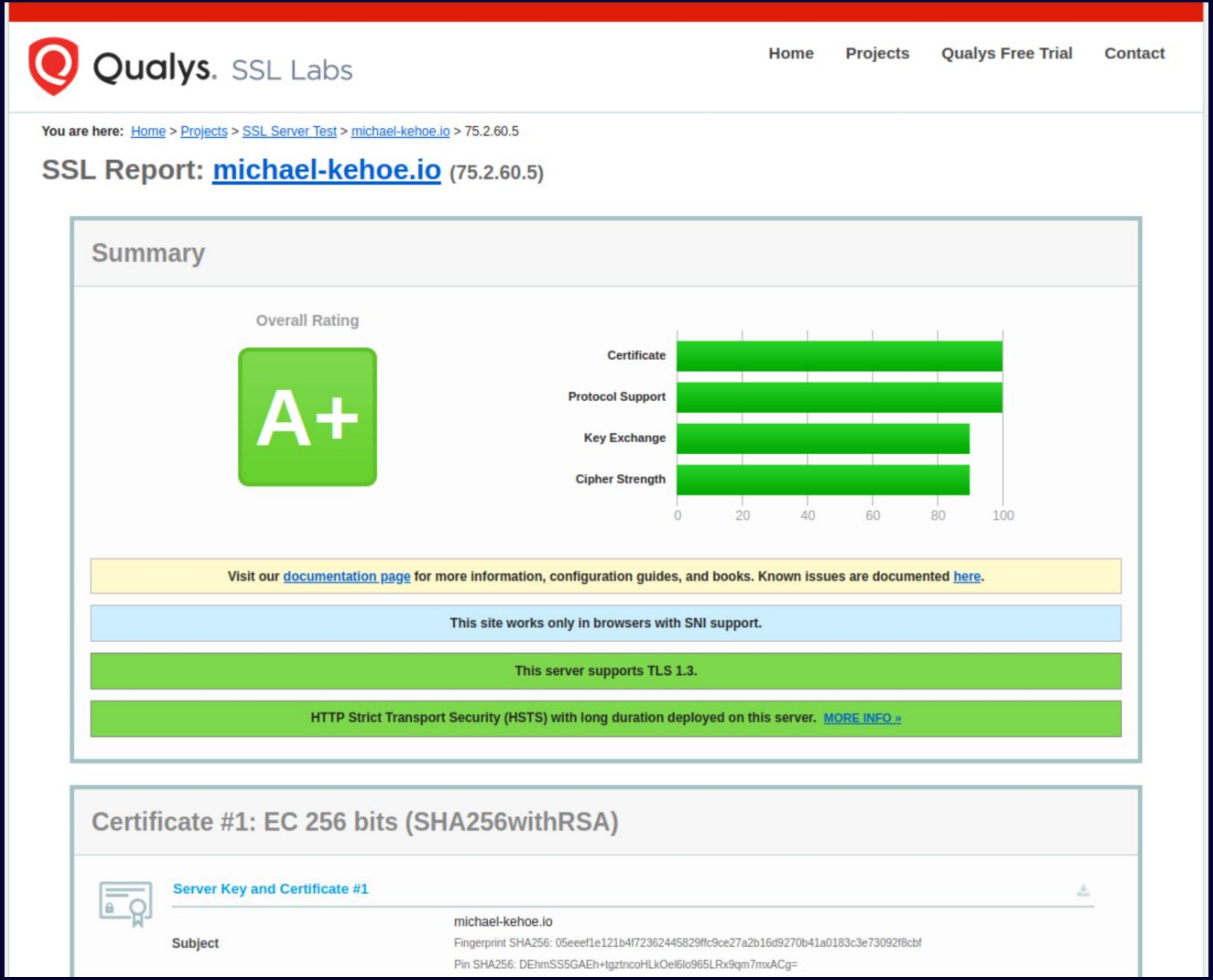
Implement CAA records

Restrict what CA’s can issue certificates for your domain

https://securitytxt.org/
https://docs.digitalocean.com/products/networking/dns/how-to/create-caa-records/

Demo:
domain-labs.com

ssllabs.com



You are here: Home > Projects > SSL Server Test > michael-kehoe.io > 75.2.60.5

SSL Report: michael-kehoe.io (75.2.60.5)

Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This site works only in browsers with SNI support.

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

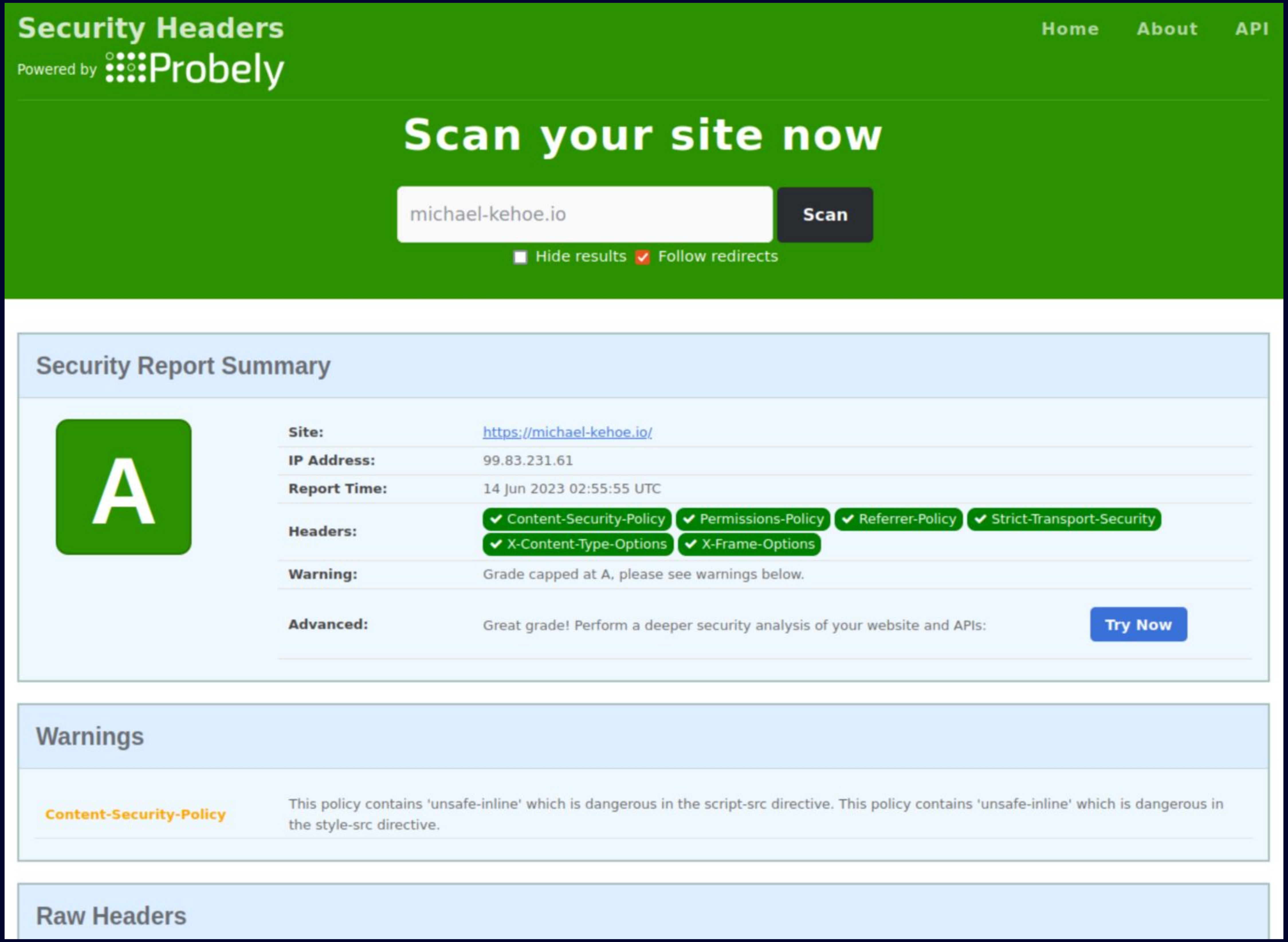
Certificate #1: EC 256 bits (SHA256withRSA)

Server Key and Certificate #1

Subject

michael-kehoe.io
Fingerprint SHA256: 05eeef1e121b4f72362445829ffc9ce27a2b16d9270b41a0183c3e73092f8cbf
Pin SHA256: DEhmSS5GAEh+tgztncoHLkOel6lo965LRx9qm7mxACg=

securityheaders.com



Scan your site now

michael-kehoe.io

□ Hide results ☑ Follow redirects

Security Report Summary

A

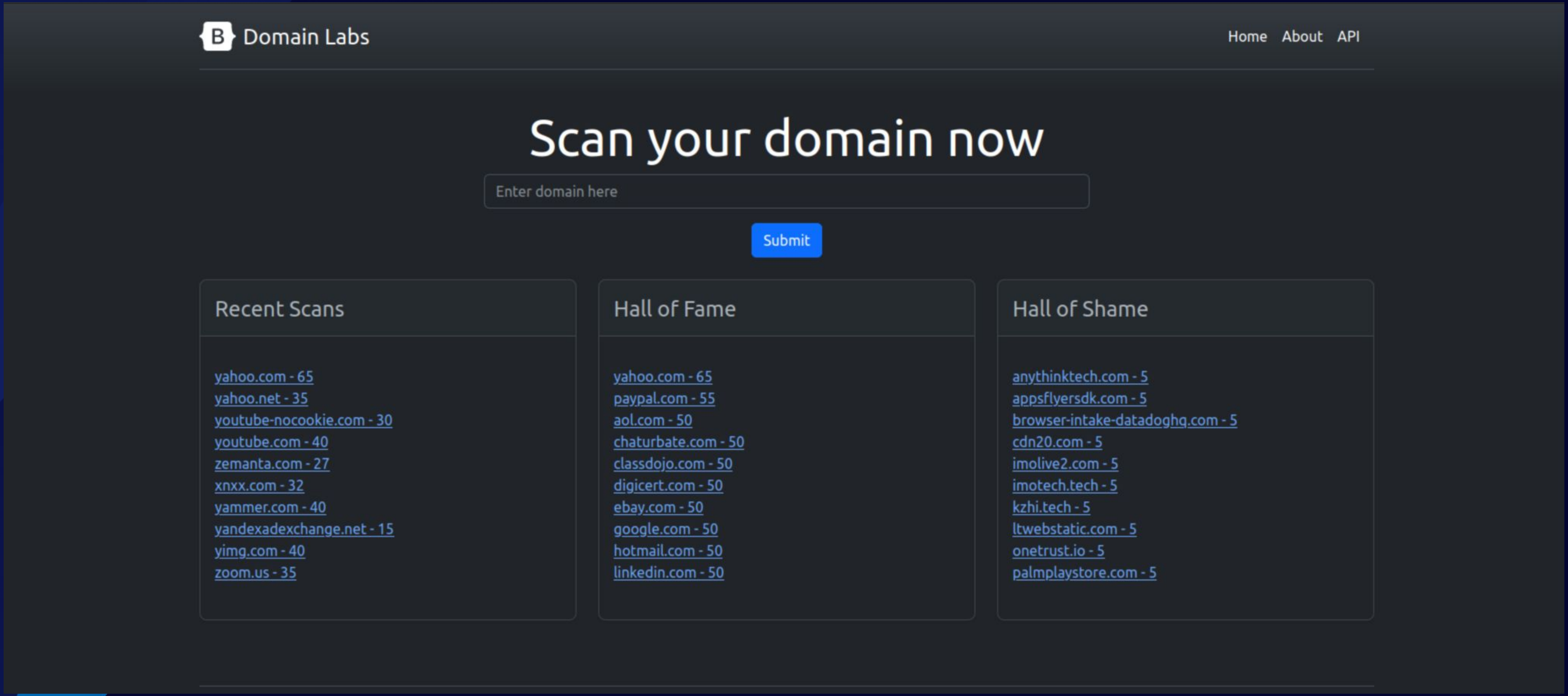
Site:	https://michael-kehoe.io/
IP Address:	99.83.231.61
Report Time:	14 Jun 2023 02:55:55 UTC
Headers:	✓ Content-Security-Policy ✓ Permissions-Policy ✓ Referrer-Policy ✓ Strict-Transport-Security ✓ X-Content-Type-Options ✓ X-Frame-Options
Warning:	Grade capped at A, please see warnings below.
Advanced:	Great grade! Perform a deeper security analysis of your website and APIs:

Warnings

Content-Security-Policy	This policy contains 'unsafe-inline' which is dangerous in the script-src directive. This policy contains 'unsafe-inline' which is dangerous in the style-src directive.

Raw Headers

domain-labs.com



Scan your domain now

Recent Scans

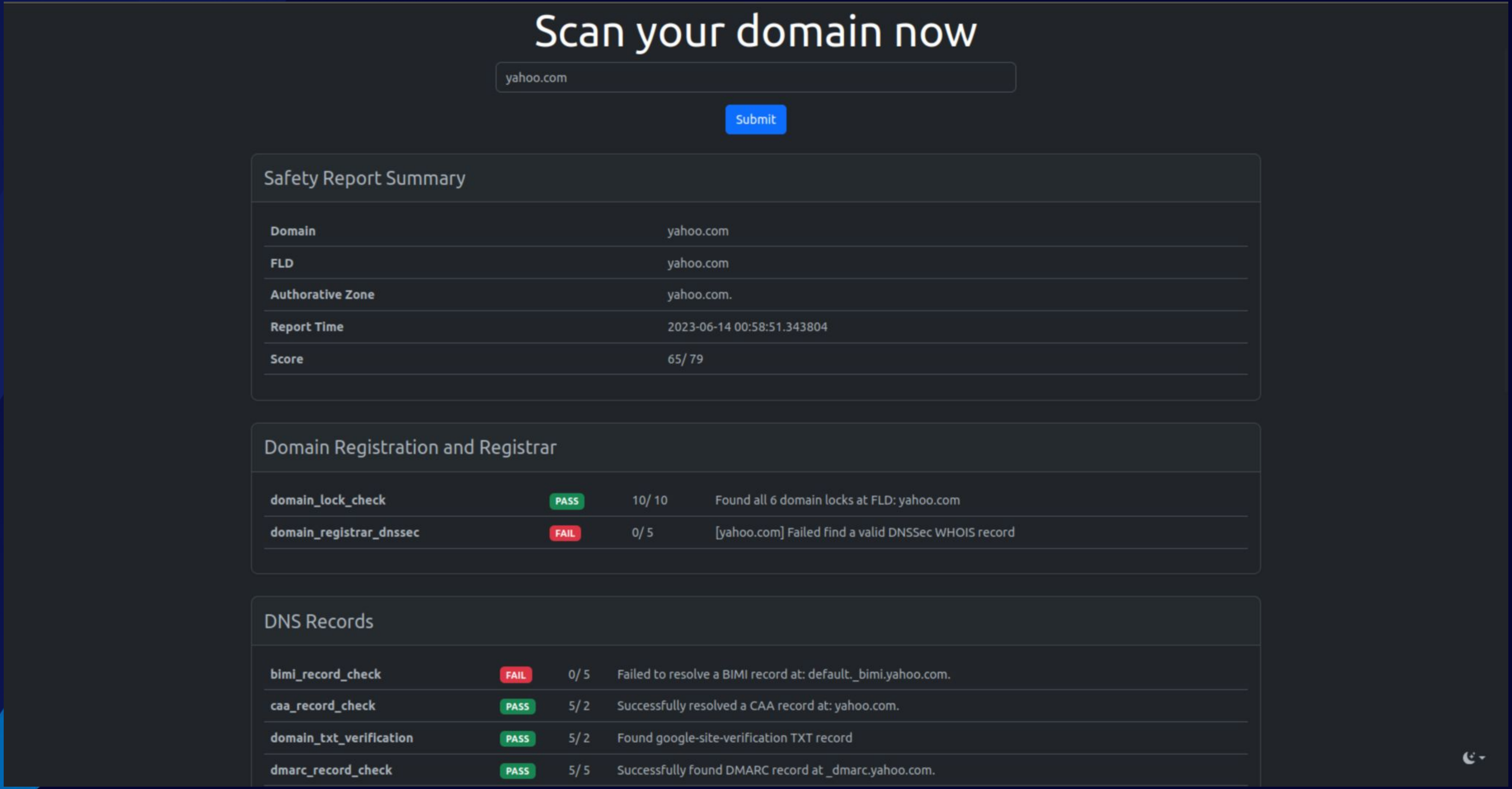
- yahoo.com - 65
- yahoo.net - 35
- youtube-nocookie.com - 30
- youtube.com - 40
- zemanta.com - 27
- xnxx.com - 32
- yammer.com - 40
- yandexadexchange.net - 15
- yimg.com - 40
- zoom.us - 35

Hall of Fame

- yahoo.com - 65
- paypal.com - 55
- aol.com - 50
- chaturbate.com - 50
- classdojo.com - 50
- digicert.com - 50
- ebay.com - 50
- google.com - 50
- hotmail.com - 50
- linkedin.com - 50

Hall of Shame

- anythinktech.com - 5
- appsflyersdk.com - 5
- browser-intake-datadoghq.com - 5
- cdn20.com - 5
- imolive2.com - 5
- imotech.tech - 5
- kzhi.tech - 5
- ltwebstatic.com - 5
- onetrust.io - 5
- palmplaystore.com - 5



Scan your domain now

yahoo.com

Safety Report Summary

Domain	yahoo.com
FLD	yahoo.com
Authorative Zone	yahoo.com.
Report Time	2023-06-14 00:58:51.343804
Score	65/ 79

Domain Registration and Registrar

domain_lock_check	PASS	10/ 10	Found all 6 domain locks at FLD: yahoo.com
domain_registrar_dnssec	FAIL	0/ 5	[yahoo.com] Failed find a valid DNSSec WHOIS record

DNS Records

bimi_record_check	FAIL	0/ 5	Failed to resolve a BIMI record at: default._bimi.yahoo.com.
caa_record_check	PASS	5/ 2	Successfully resolved a CAA record at: yahoo.com.
domain_txt_verification	PASS	5/ 2	Found google-site-verification TXT record
dmarc_record_check	PASS	5/ 5	Successfully found DMARC record at _dmarc.yahoo.com.

Q&A

CONFLUENT