automated mail server testing

“LIKE SSLLABS, BUT FOR EMAIL”

Martin Boßlet

What is the first thing
you do when you put
a web server online?

ANSWER:

https://www.ssllabs.com/ssltest/

SSLLabs has made
the internet

a safer place

for web sites with https

What is the first thing you do when you put an email server online?

ANSWER:

https://??????

Wouldn't that be great?

a tool to check

SMTP
IMAP
POP3
HTTPS

...

Wouldn't that be great?

ANSWER:

YES

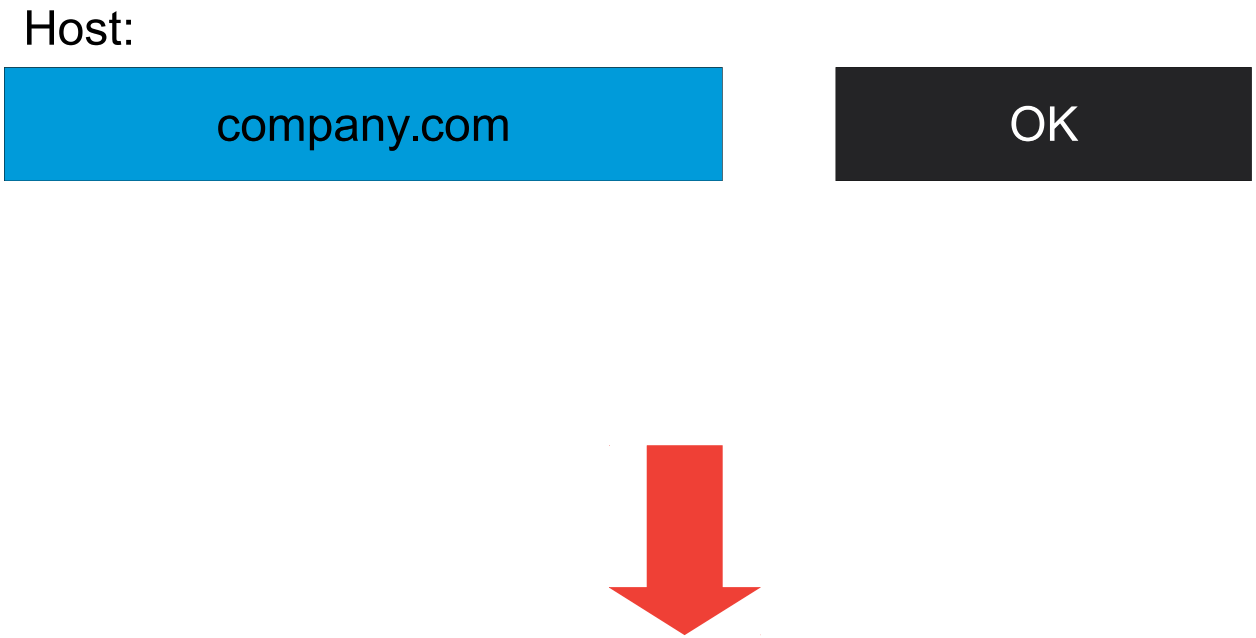
and guess what, we have something for you \o/

The magnificent

Automated
Email Server Tester

Name TBD

What does it do?



Host: company.com

TLS & DNS analysis report

How can you use it?

As a private person

See if your email provider
does things the right way

As a company

See if your email servers
do things the right way

Email security is vital

It's one of the places
likely to be attacked

Note:

Our focus is email server infrastructure

Brief History of the Project

Like any good project, we too started with a

Proof of Concept™

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

Thanks to our sponsors!

SECURITY
MADEIN.LU

aware.lu circl.lu cases.lu

Goal:

Get something running.
Asap.

Features of the PoC:

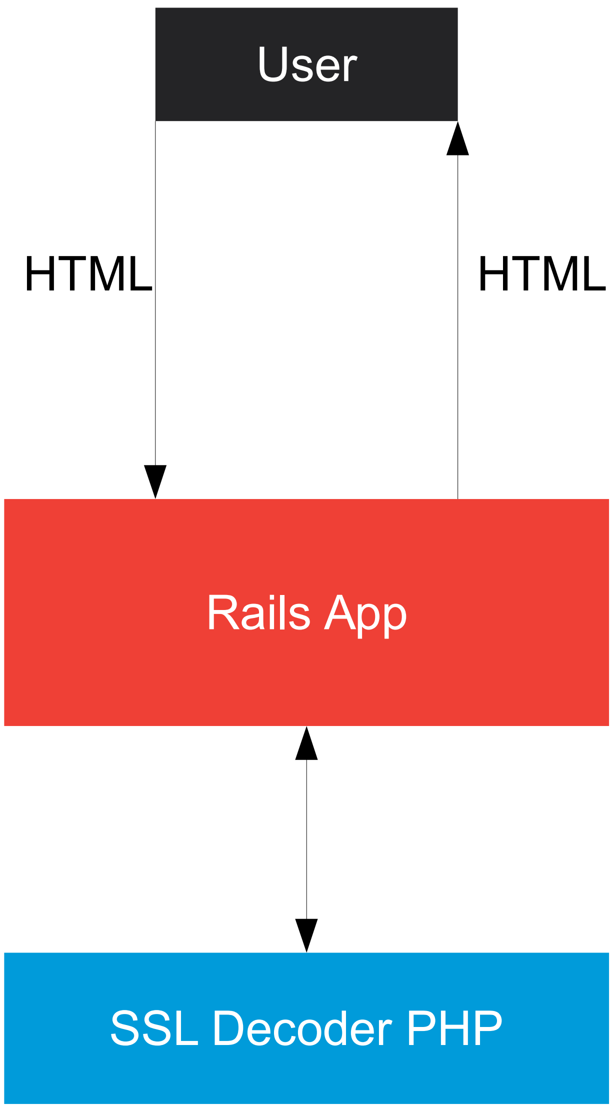
DNS record analysis

TLSA
CAA
DMARC
SPF

Basic TLS analysis

using an
open source PHP tool

https://github.com/RaymiiOrg/ssl-decoder



ARCHITECTURE | PoC

alt2.aspmx.l.google.com

Email Server (SMTP)

IP:74.125.200.26 ipv4 **Port:**25

Start:	18:12:26
End:	18:13:06

DNS RESULTS

DANE/TLSA

-	no records found

DMARC

Entries	v=DMARC1
	p=reject
	rua=mailto:mailauth-reports@google.com

SENDER POLICY FRAMEWORK (SPF)

Value	v=spf1 include:_spf.google.com ~all

CERTIFICATE AUTHORITY AUTHORIZATION

issue	symantec.com non-critical

DNS RESULTS

DANE/TLSA

Host	mx01.posteo.de
Certificate Usage	3
Selector	1
Matching Type	1
Certificate Association Data	YHg6lF6c81F7j83apmWtrzgANaHRN1gjRXGqMNGm5C0=
Host	mx01.posteo.de
Certificate Usage	3
Selector	1
Matching Type	1
Certificate Association Data	fN88JfnaJETU3r1IBBELkRBvZI27UHb5fjqFdqntyGo=
Host	mx01.posteo.de
Certificate Usage	3
Selector	1
Matching Type	1
Certificate Association Data	HuTEMYwfqNdawN9WdVswoviNt7+sEposUPMWoMOx5kA=

TLS RESULTS

CONNECTION DETAILS

Protocol Versions	TLS 1.0 TLS 1.1 TLS 1.2
Cipher Suites	ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA AES256-GCM-SHA384 AES256-SHA256 AES256-SHA ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA AES128-GCM-SHA256 AES128-SHA256 AES128-SHA DES-CBC3-SHA

SUPPORTED FEATURES

TLS Compression	no
TLS Fallback SCSV	yes
Heartbeat	no

VULNERABILITY CHECKS

Heartbleed	not vulnerable

CERTIFICATES

SERVER CERTIFICATE

Subject	/C=US/ST=California/L=Mountain View/O=Google Inc/CN=mx.google.com
Issuer	/C=US/O=Google Inc/CN=Google Internet Authority G2
Algorithm	RSA
Key Length	2048
Valid from	2016-10-06 12:28:00 UTC
Valid until	2016-12-29 12:28:00 UTC
Signature Algorithm	sha256WithRSAEncryption
Alternative Names	mx.google.com alt1.aspmx.l.google.com alt1.gmail-smtp-in.l.google.com alt1.gmr-smtp-in.l.google.com alt2.aspmx.l.google.com alt2.gmail-smtp-in.l.google.com alt2.gmr-smtp-in.l.google.com alt3.aspmx.l.google.com alt3.gmail-smtp-in.l.google.com alt3.gmr-smtp-in.l.google.com alt4.aspmx.l.google.com alt4.gmail-smtp-in.l.google.com alt4.gmr-smtp-in.l.google.com aspmx.l.google.com aspmx2.googlemail.com aspmx3.googlemail.com aspmx4.googlemail.com aspmx5.googlemail.com gmail-smtp-in.l.google.com gmr-mx.google.com gmr-smtp-in.l.google.com
Certificate Practice Statement	not available
Certificate Policies	1.3.6.1.4.1.11129.2.5.1 2.23.140.1.2.2

Problems

SSL Decoder is good for bootstrapping

But we need more control eventually

We can't check DKIM

without an actual email

DKIM DNS record lookup:

<selector>._domainkey.<domain>

e.g.

guessme._domainkey.example.org

The selector may change
and is not guessable a priori

We need an email
from that domain
to learn the selector!

Phase II

How could we solve the DKIM issue?

ANSWER:

Use the grandfather of REST APIs
The venerable

“send an email, get an email back”

web service

Turning fallbacks into features^{TM}

Actually, sending an email
does feel natural in this context!

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

Again thanks to our sponsors!

SECURITY
MADEIN.LU

aware.lu circl.lu cases.lu

New problem:

How do we make a nice email report?

By not doing it!

We send a simple response including a link to the HTML report

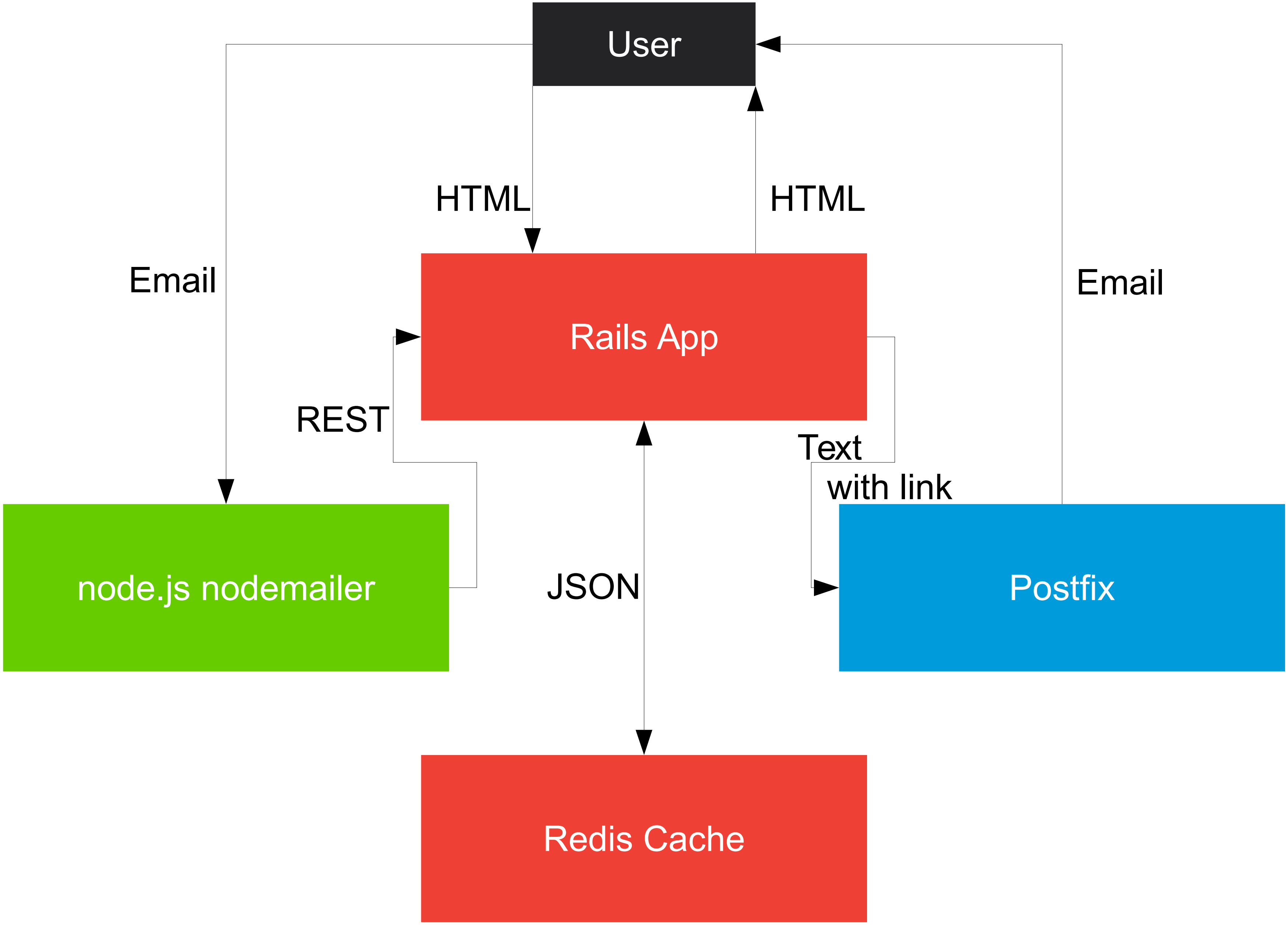
Next problem:

We don't store the results

(and we never will, privacy and all...)

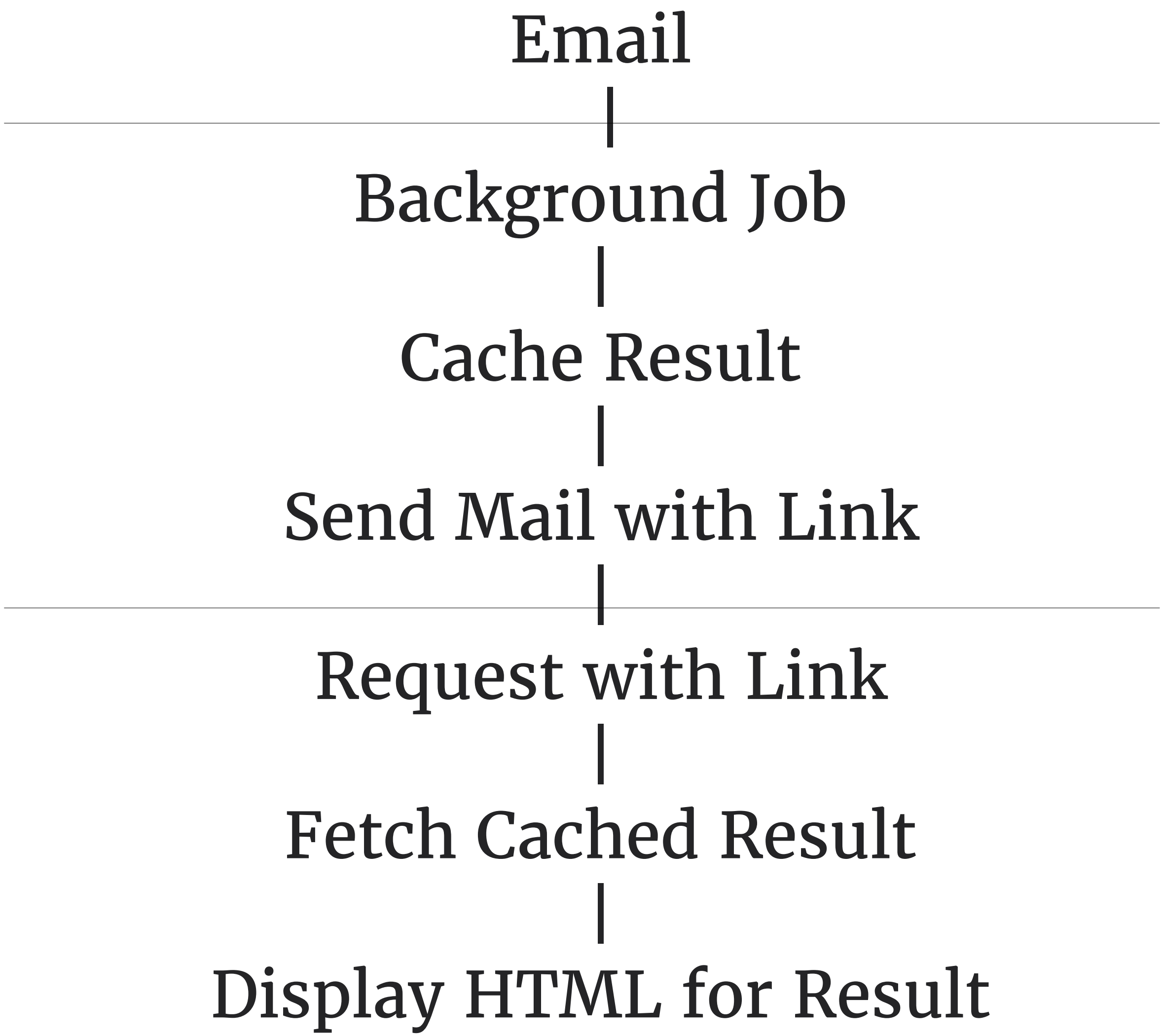
Solution:

Cache with Expiration



ARCHITECTURE | PHASE II

Async Processing of emails



Email

Background Job

Cache Result

Send Mail with Link

Request with Link

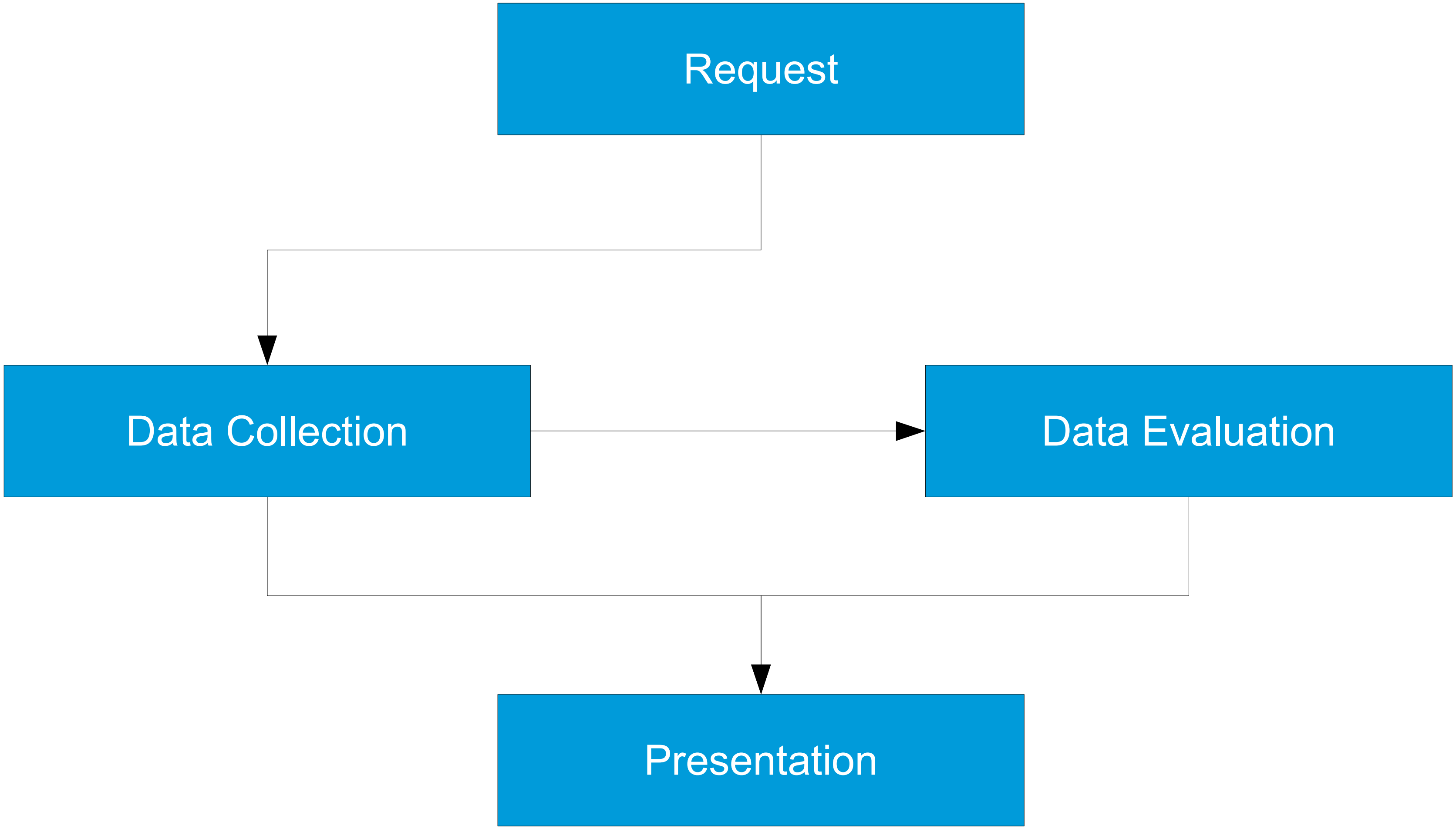
Fetch Cached Result

Display HTML for Result

Big New Feature #2

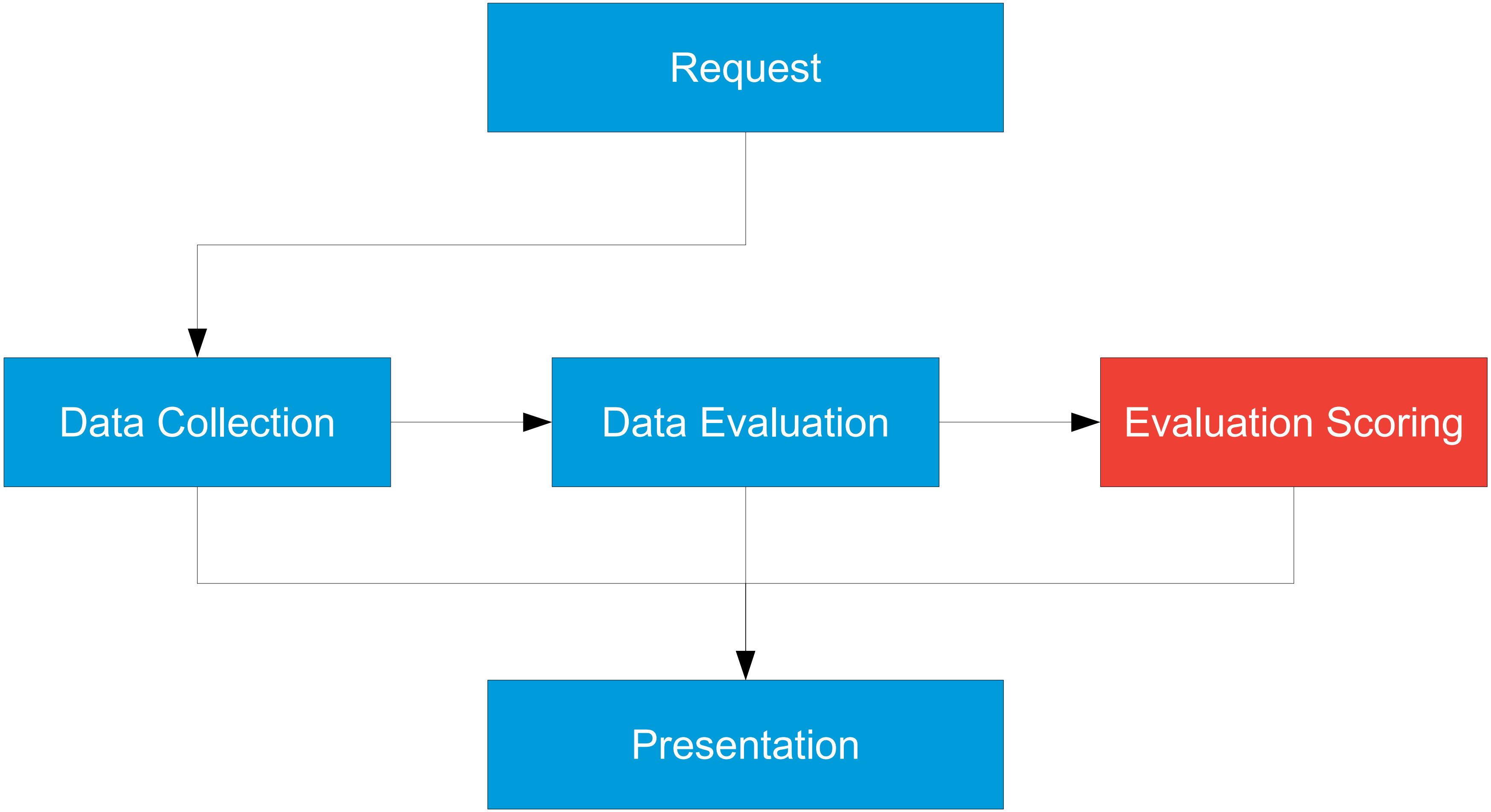
Evaluation

In the PoC, we collected data and displayed it without assessing it



REQUEST PROCESSING STAGES

Where to go from here?



FUTURE REQUEST PROCESSING STAGES

Evaluation and Scoring

implies

Need for Explanation

implies

Documentation & Education

API access for easy integration

Command Line Interface

(offline!!!)

Cover all TLS-based protocols

Feature Parity

with SSLLabs, MxToolbox etc.

Our tool is open source
and
we want to create a community

To build it, we need

Sponsors
Partnerships
Expert Knowledge

Domain Experts
for evaluation & scoring

Together, we can build
the ultimate

“SSLLabs for Email”

Even better, the ultimate

“SSLLabs for TLS”

STIDIA

THANK YOU

https://email.secureluxembourg.lu
(email/secure)

mailto:contact@emailmadein.lu