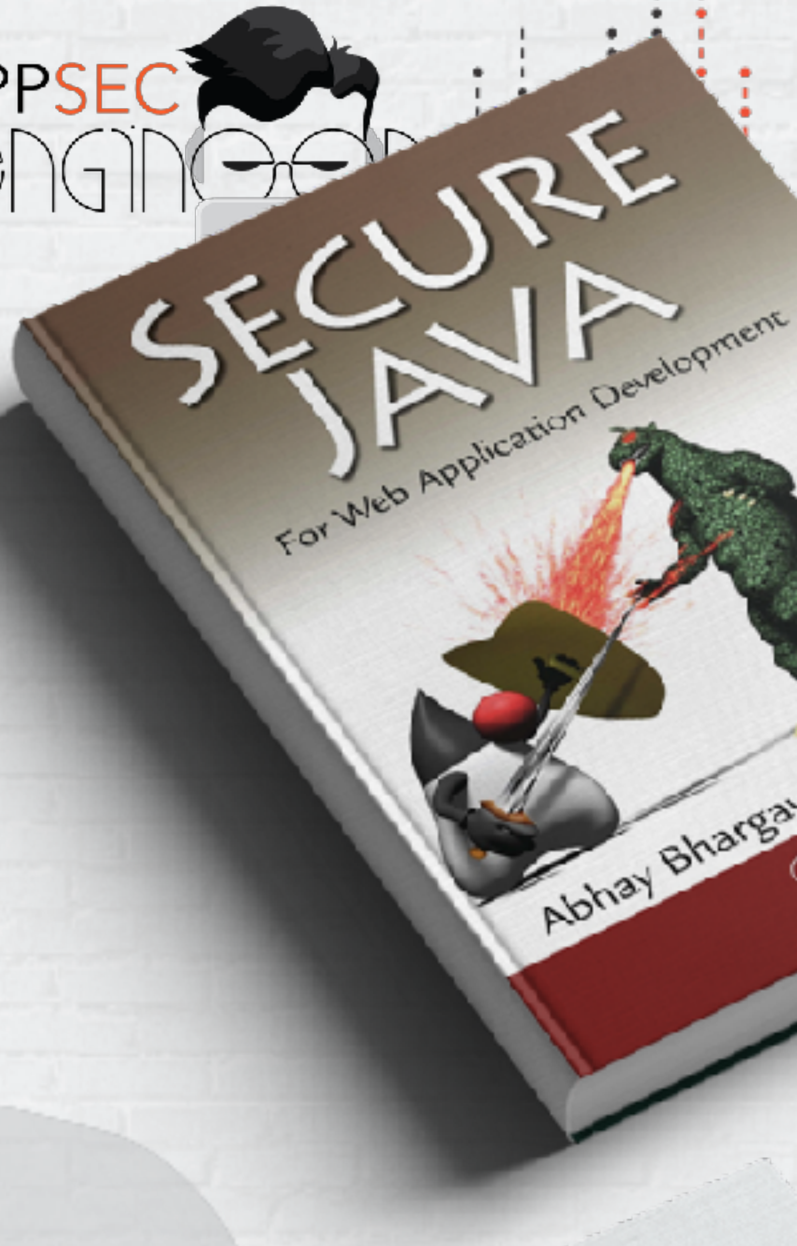
we45

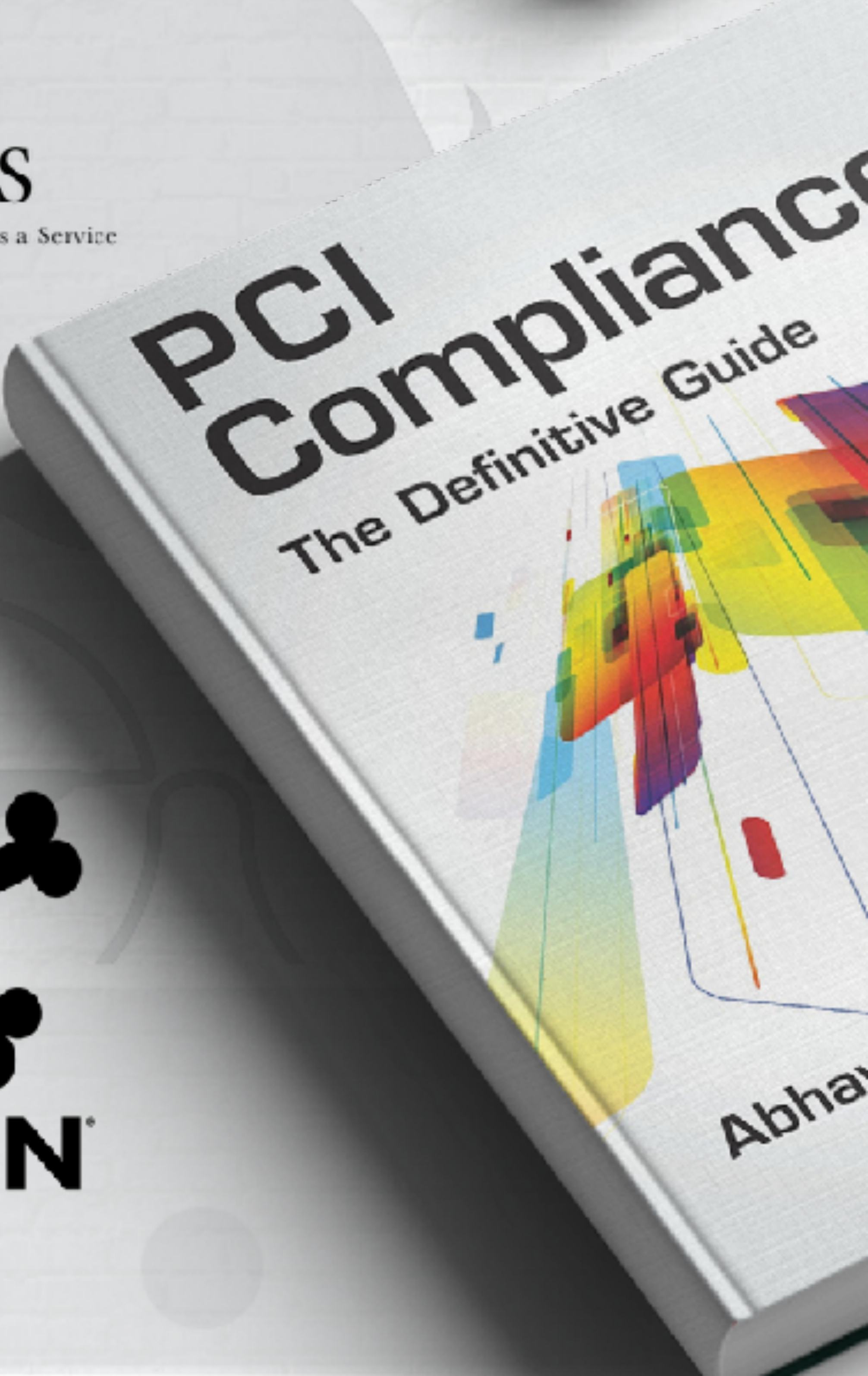
APPSEC engineer

Fantastic Vulnerabilities and Where to Find Them

Yours Truly

- Founder @ we45
- Founder @ AppSecEngineer
- AppSec Automation Junkie
- Trainer/Speaker at DEF CON, BlackHat, OWASP Events, etc world-wide
- Co-author of Secure Java For Web Application Development
- Author of PCI Compliance: A Definitive Guide



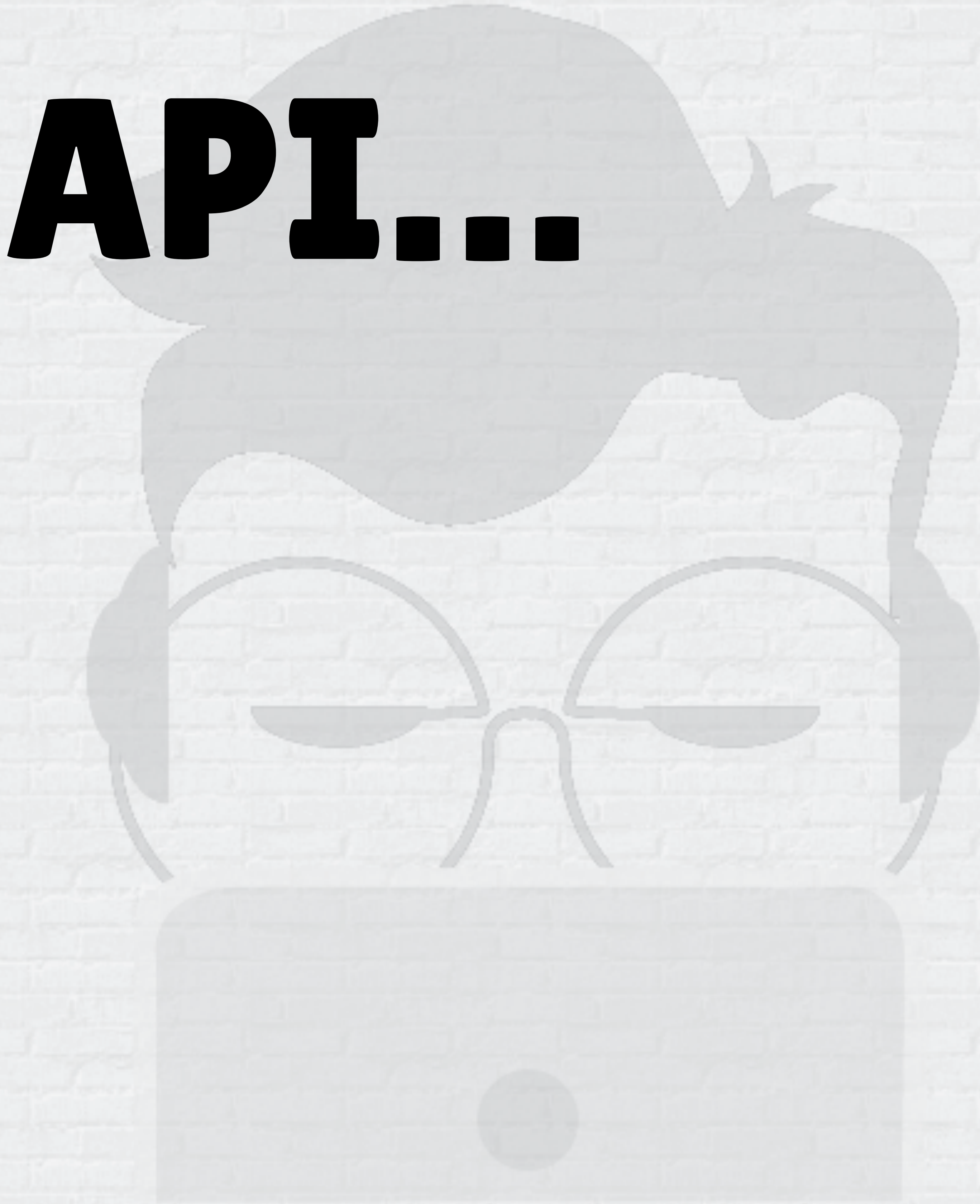


abhaybhargav

My talk...

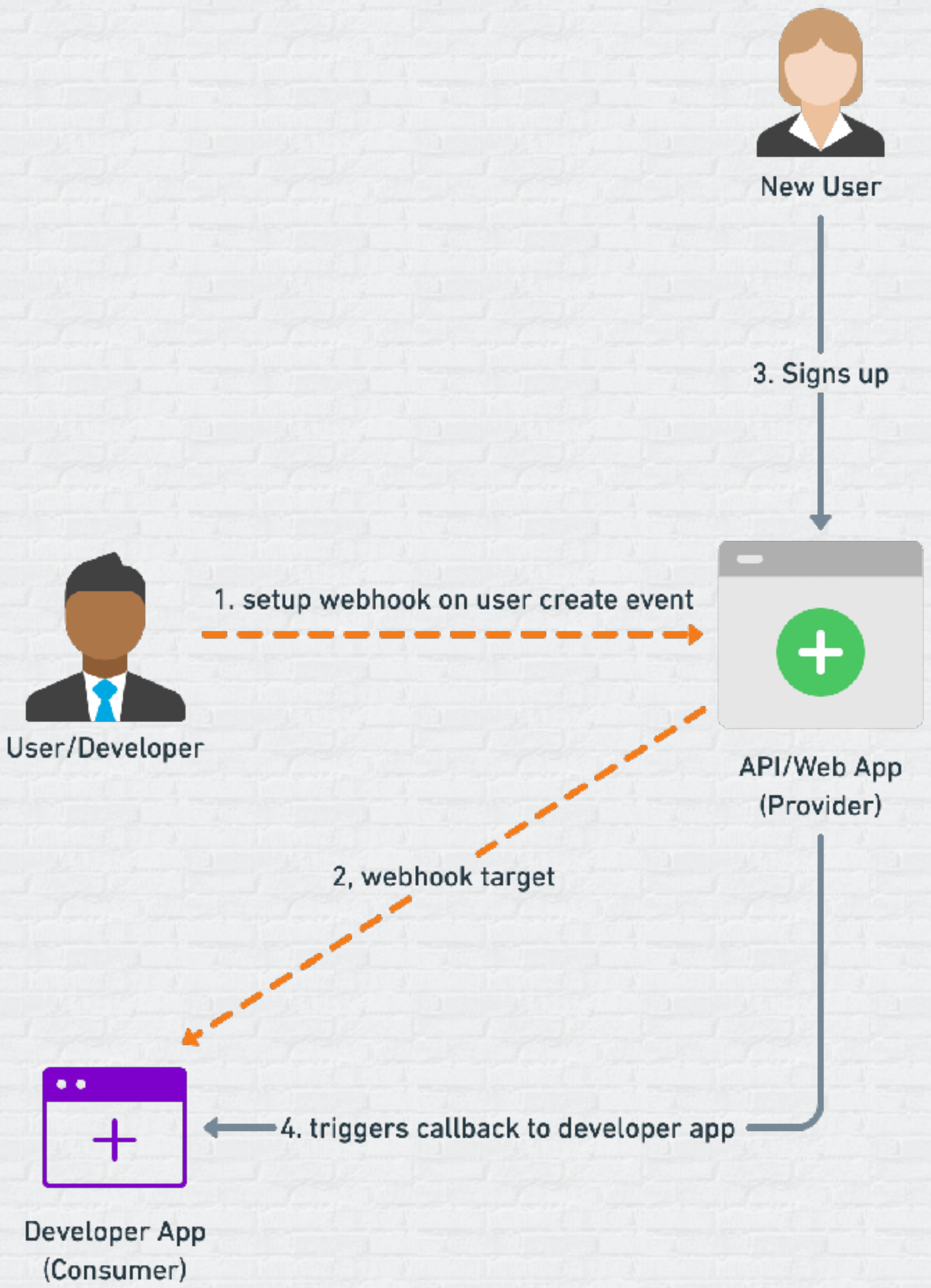
Story 1
Beware of the Boomerang

So you're building an API...



You probably need webhooks…

What are they?



Webhooks a.k.a "User Generated Callbacks"

abhaybhargav

Webhooks are everywhere!

zapier

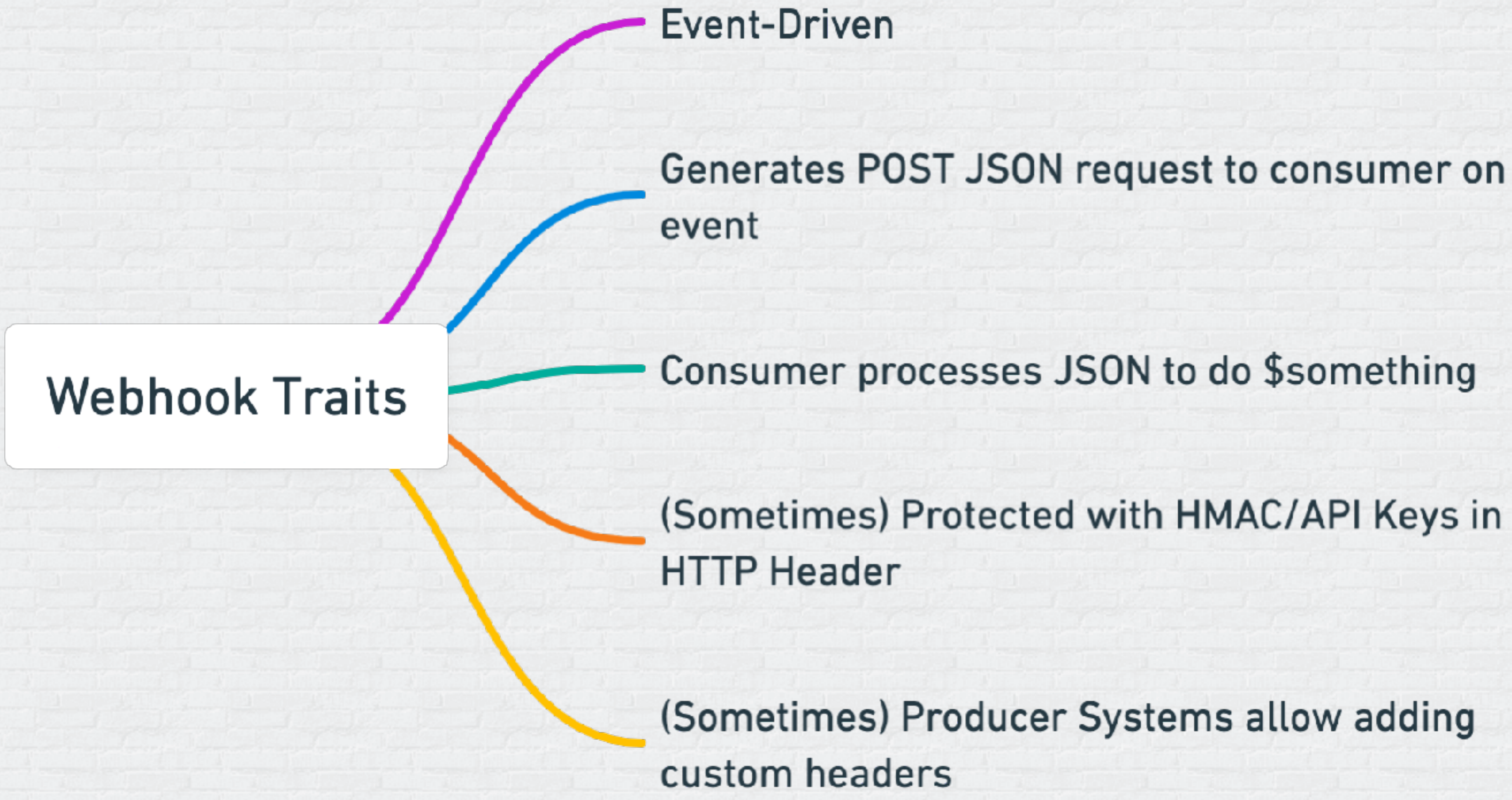
Jenkins

kubernetes

stripe

mailchimp

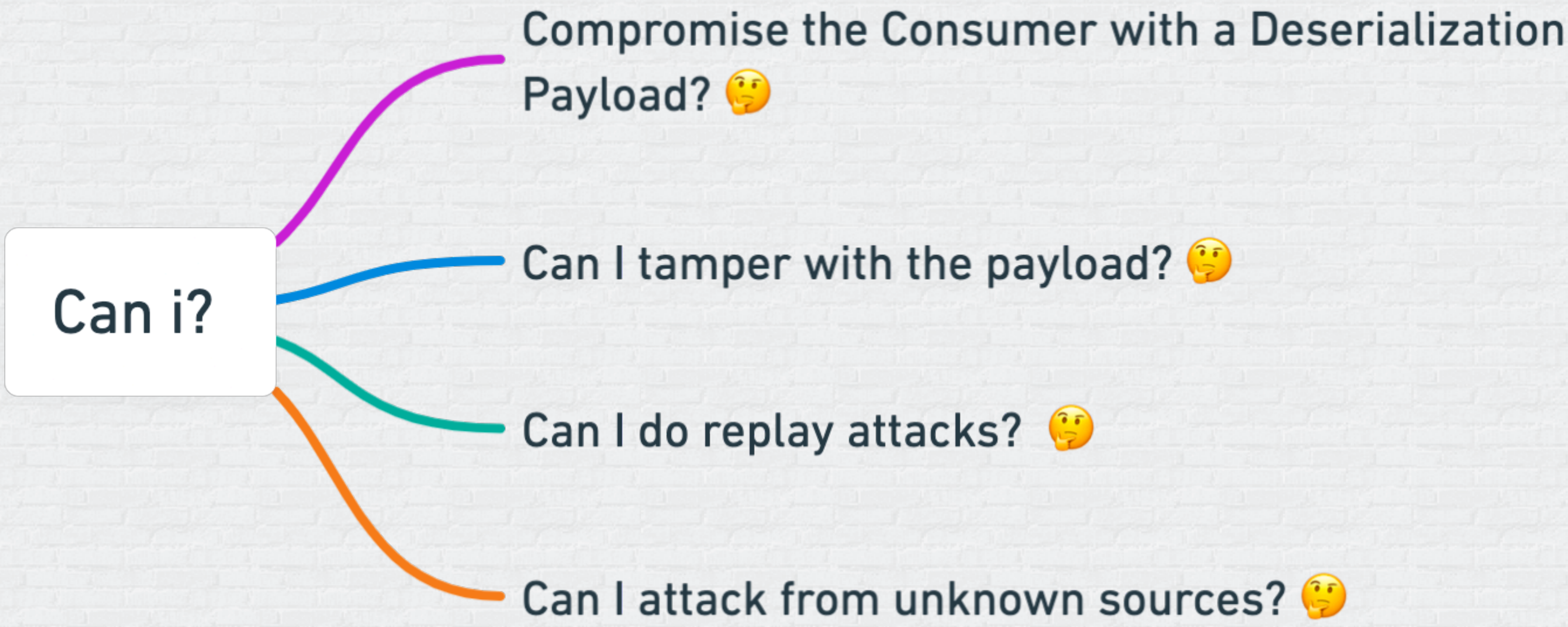
Common Webhook Traits



Webhook Traits

- Event-Driven
- Generates POST JSON request to consumer on event
- Consumer processes JSON to do $something
- (Sometimes) Protected with HMAC/API Keys in HTTP Header
- (Sometimes) Producer Systems allow adding custom headers

Natural Attack Focus/Assumptions



Can i?

Compromise the Consumer with a Deserialization Payload? 🤔

Can I tamper with the payload? 🤔

Can I do replay attacks? 🤔

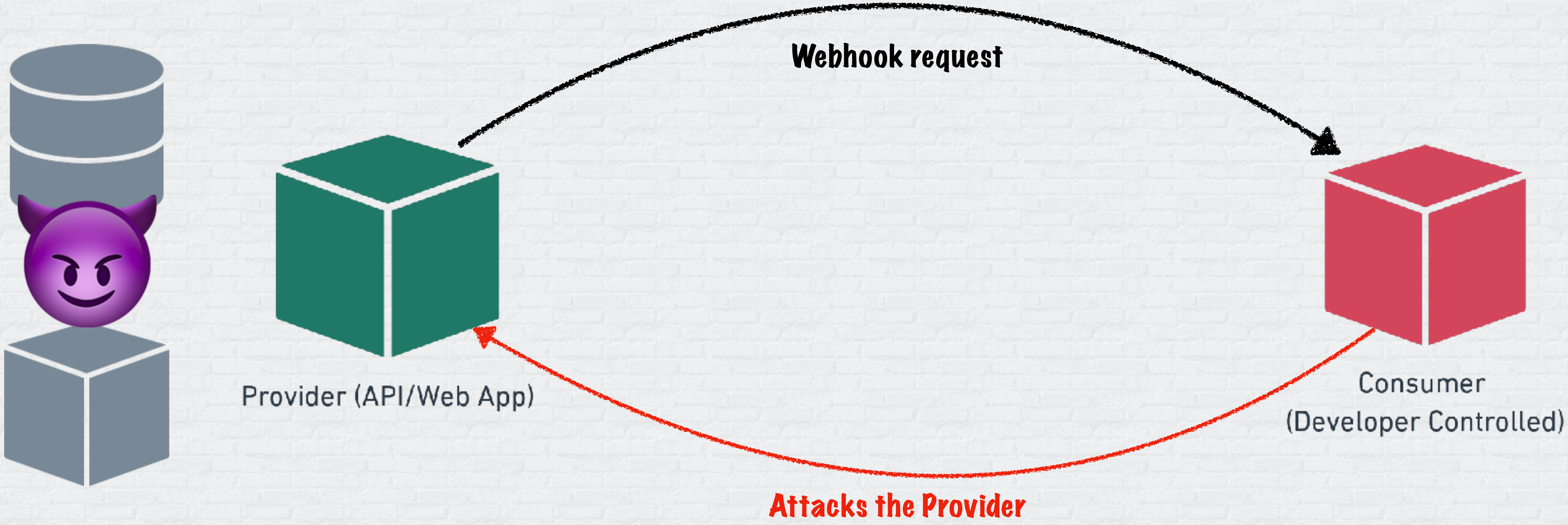
Can I attack from unknown sources? 🤔

abhaybhargav

Our Focus…

Can I compromise the Provider? 🤔

Can I...?



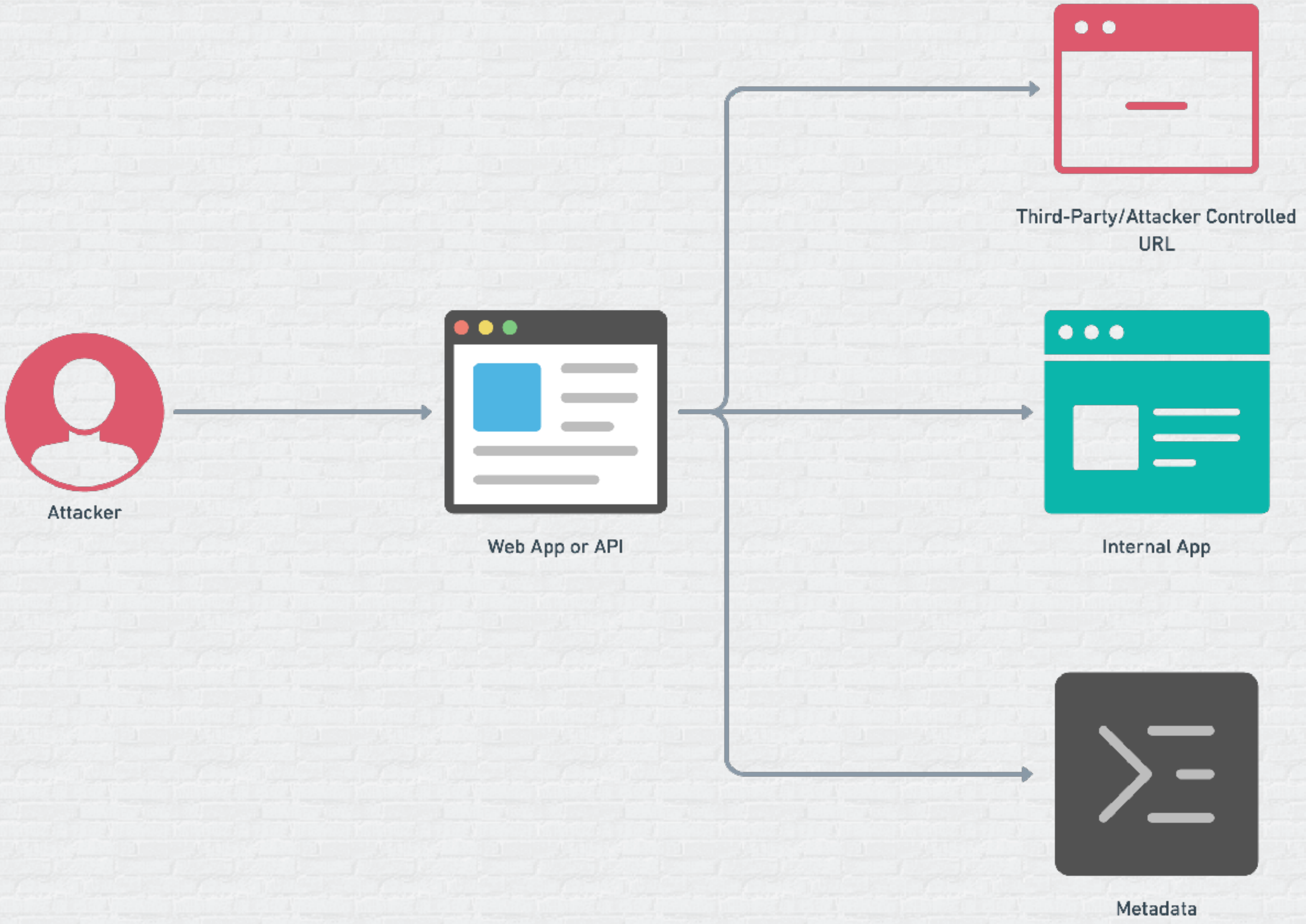
abhaybhargav

This can only mean....

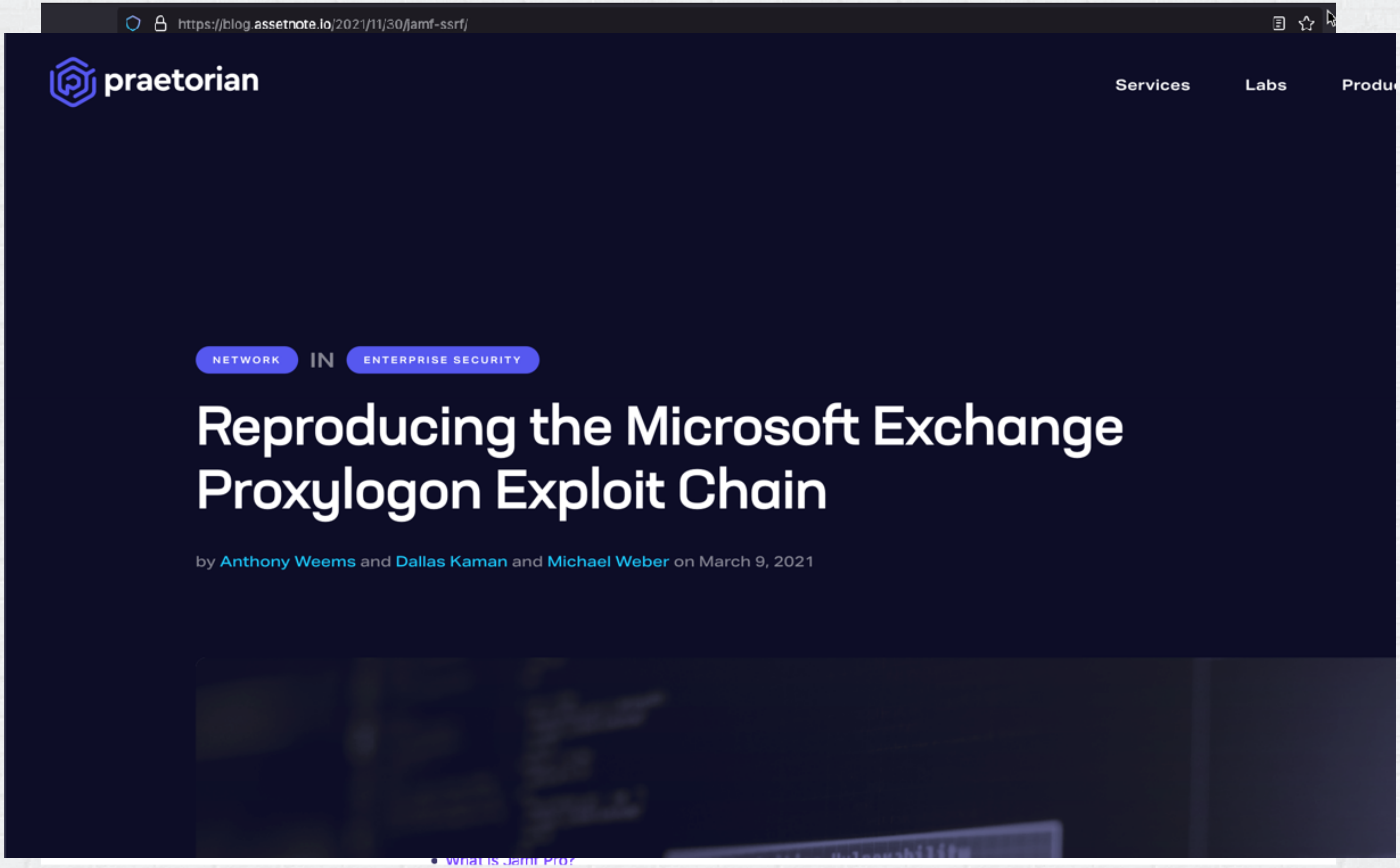
SSRF!

abhaybhargav

What is SSRF?


Attacker
Web App or API
Third-Party/Attacker Controlled URL
Internal App
Metadata

SSRF – Real-world Examples



https://blog.assetnote.io/2021/11/30/jamf-ssrf/

praetorian

NETWORK IN ENTERPRISE SECURITY

Reproducing the Microsoft Exchange Proxylogon Exploit Chain

by Anthony Weems and Dallas Kaman and Michael Weber on March 9, 2021

- What is Jamf Pro?

Effects and Impact of SSRF

APPSEC engineer we45

Steal Metadata for Cloud Compromise

Remote File Read

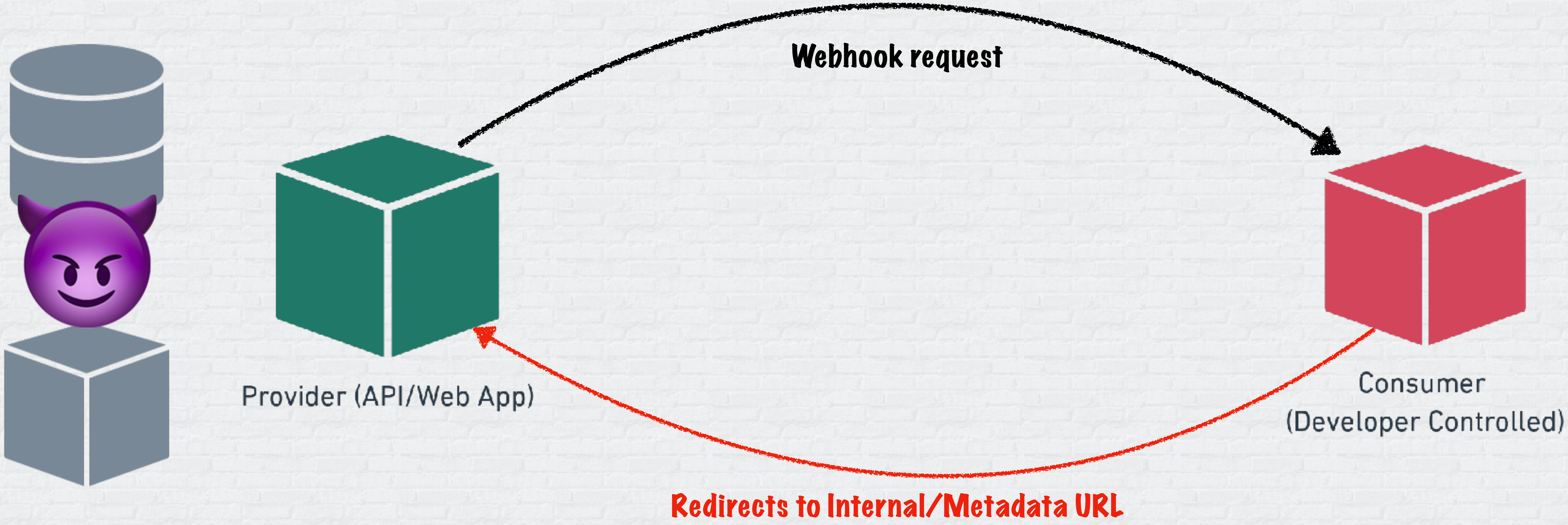
Remote Code Execution

Information Disclosure Internal Hosts

Denial of Service

abhaybhargav

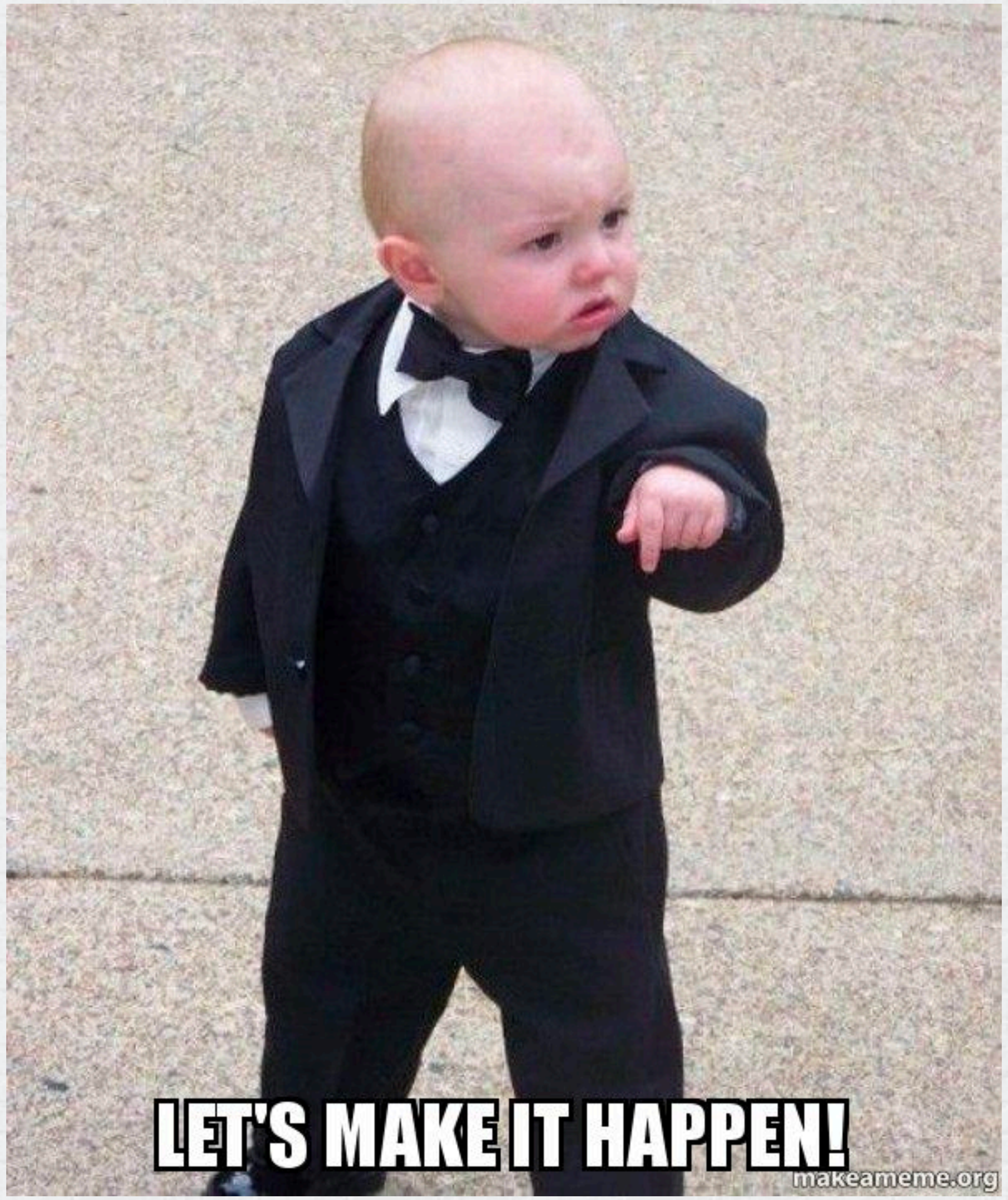
What we want….

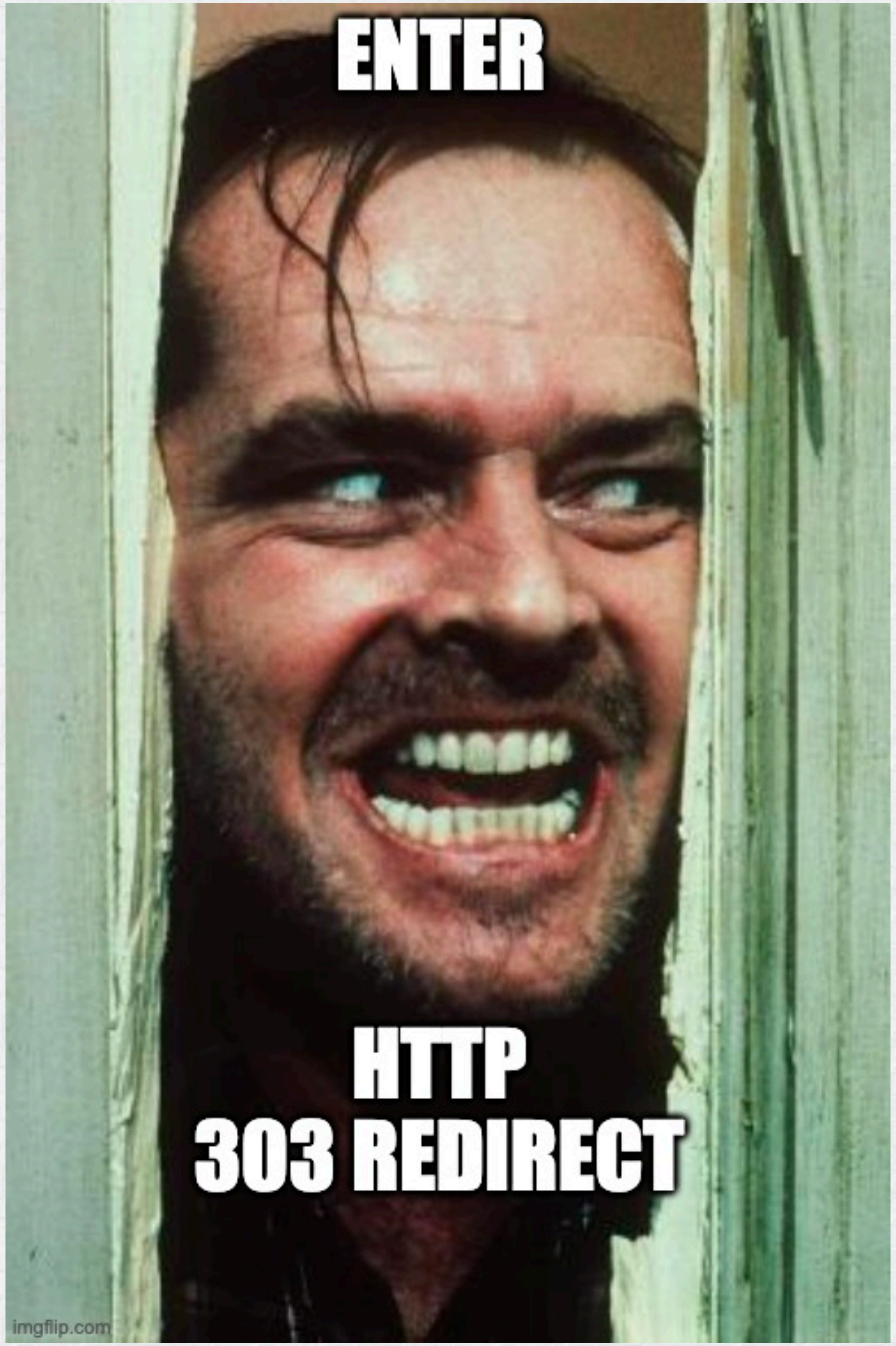

Webhook request
Provider (API/Web App)
Consumer
(Developer Controlled)
Redirects to Internal/Metadata URL

But there's a problem....

SSRF works…

- When there's a GET request involved
- Most Webhooks make POST requests (some PUT cases as well)
- That are difficult to weaponize as an SSRF
- Most 3XX Redirects require clients NOT to follow redirects

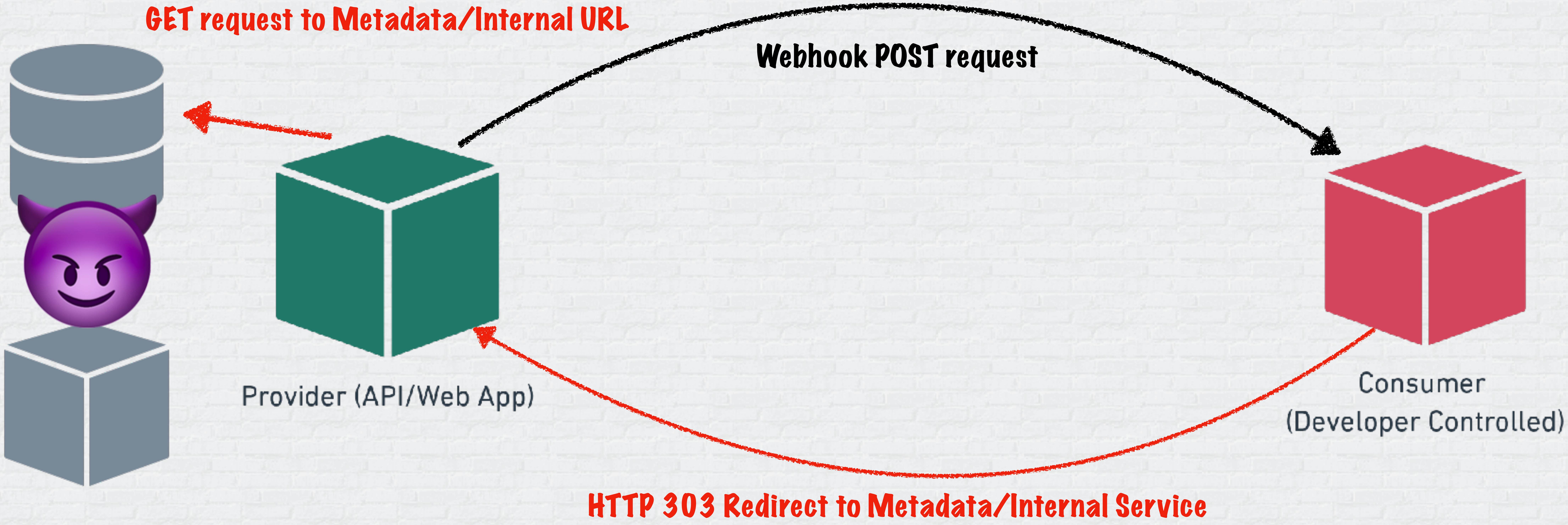



ENTER
HTTP
303 REDIRECT
imgflip.com

HTTP 303 See other

- Is a response that can be triggered for an originated POST/PUT request
- Usually used when a resource has been replaced
- Redirect response is a GET (which works for us)
- Prompts clients to follow with a GET request to the specified location

What we want....



GET request to Metadata/Internal URL

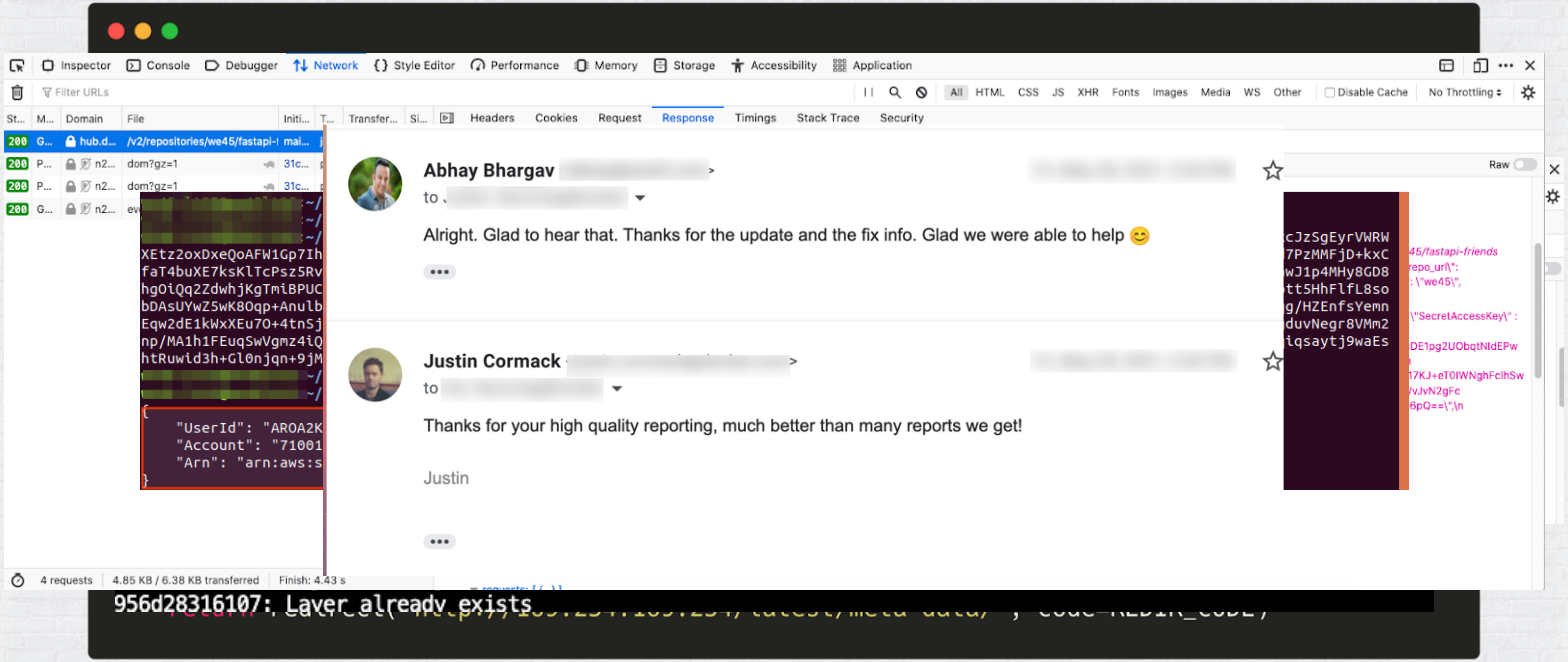
Webhook POST request

Provider (API/Web App)

Consumer (Developer Controlled)

HTTP 303 Redirect to Metadata/Internal Service

How we used this on Docker…



St...	M...	Domain	File	Initi...	T...
200	G...	hub.d...	/v2/repositories/we45/fastapi-1	mai...	j
200	P...	n2...	dom?gz=1	31c...	p
200	P...	n2...	dom?gz=1	31c...	p
200	G...	n2...	ev		

4 requests | 4.85 KB / 6.38 KB transferred | Finish: 4.43 s

```
[redacted]~/
XEtz2oxDxeQoAFW1Gp7Ih
faT4buXE7ksKlTcPsz5Rv
hgOiQq2ZdwhjKgTmiBPUC
bDAsUYwZ5wK8Oqp+Anulb
Eqw2dE1kWxXEu7O+4tnSj
np/MA1h1FEuqSwVgmz4iQ
htRuwid3h+Gl0njqn+9jM
[redacted]~/
{
    "UserId": "AROA2K
    "Account": "71001
    "Arn": "arn:aws:s
}
```

Abhay Bhargav [redacted]>
to [redacted]

Alright. Glad to hear that. Thanks for the update and the fix info. Glad we were able to help 😊

•••

Justin Cormack [redacted]>
to [redacted]

Thanks for your high quality reporting, much better than many reports we get!

Justin

•••

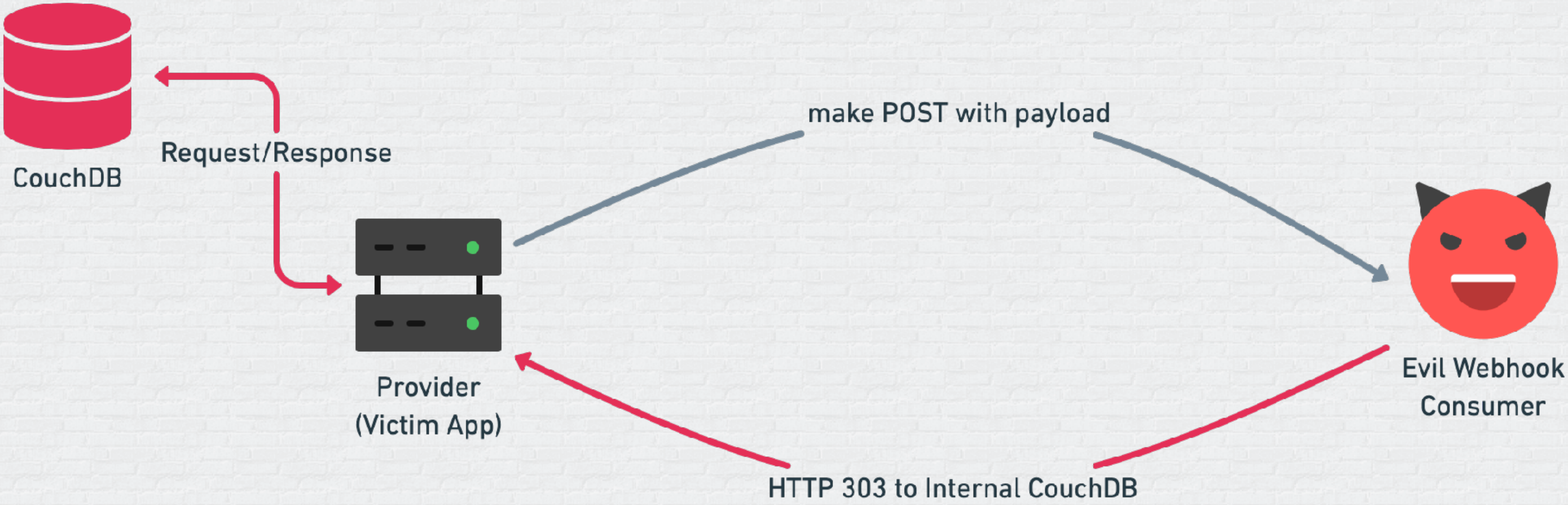
```
cJzSgEyrVWRW
7PzMMFjD+kxC
wJ1p4MHy8GD8
tt5HhFlfL8so
g/HZEnfsYemn
duvNegr8VMm2
iqsaytj9waEs
```

```
45/fastapi-friends
repo_url\":
: \"we45\",

\"SecretAccessKey\" :

DE1pg2UObqtNIdEPw
n
17KJ+eT0IWNghFclhSw
VvJvN2gFc
6pQ==\",\n
```

```
956d28316107: Laver alreadv exists
```

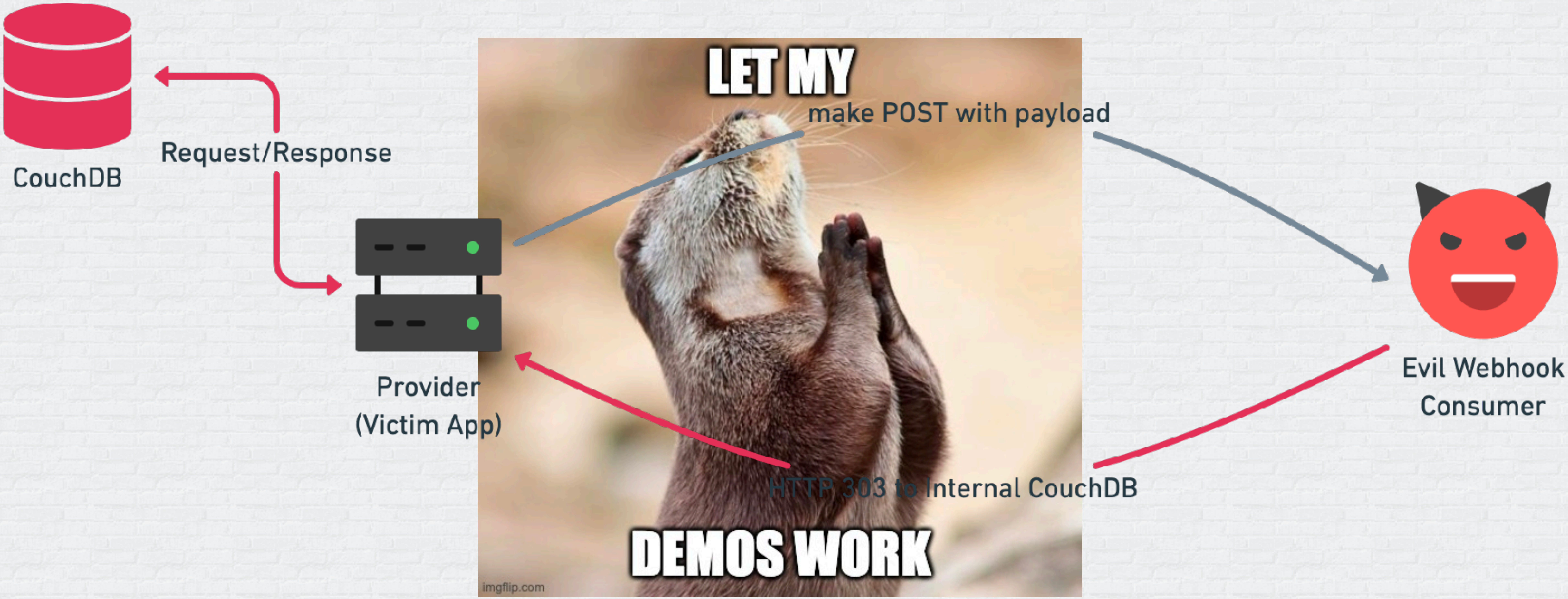
abhaybhargav

Demo time



abhaybhargav

Needless to say!



CouchDB

Request/Response

Provider
(Victim App)

make POST with payload

Evil Webhook
Consumer

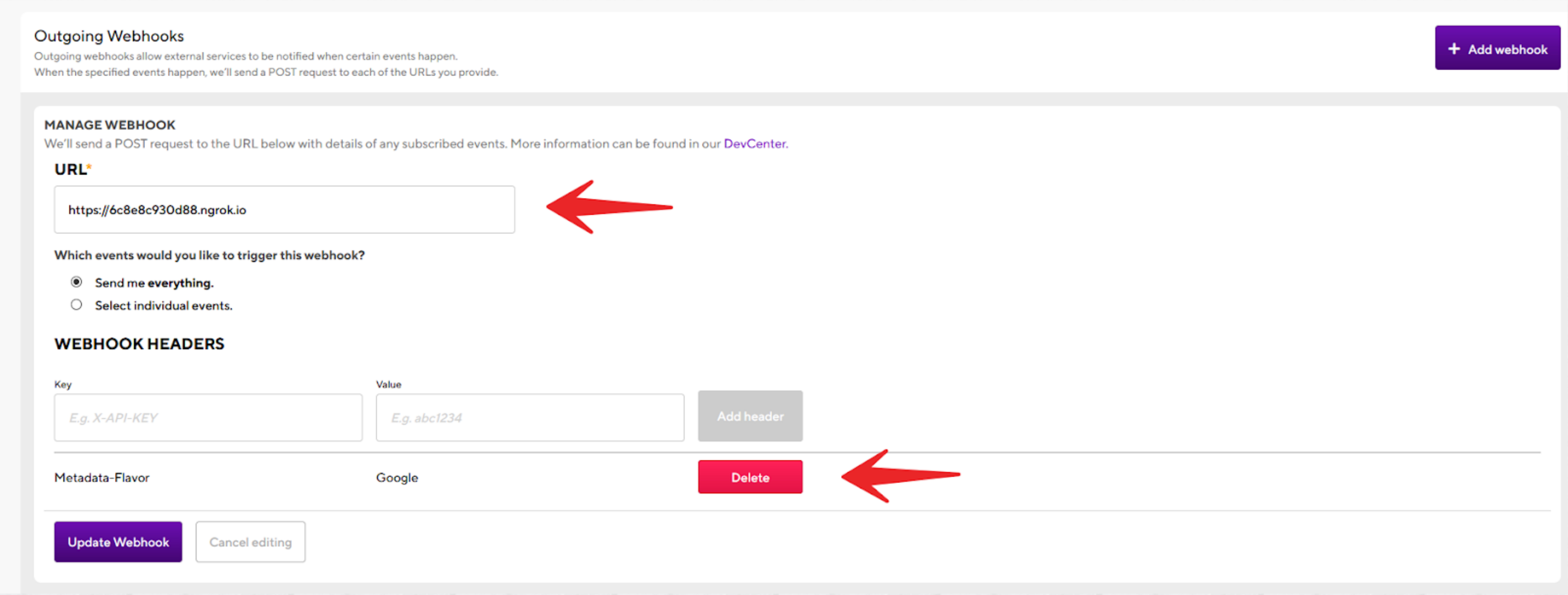
HTTP 303 to Internal CouchDB

Custom Headers FTW!

- Several apps (providers) allow you to configure custom headers for Webhooks

- So all you have to do now is use Cloud Metadata Headers in the Custom Headers and you're in!

Custom headers FTW!



Outgoing Webhooks

Outgoing webhooks allow external services to be notified when certain events happen.
When the specified events happen, we'll send a POST request to each of the URLs you provide.

MANAGE WEBHOOK

We'll send a POST request to the URL below with details of any subscribed events. More information can be found in our DevCenter.

URL*

https://6c8e8c930d88.ngrok.io

Which events would you like to trigger this webhook?

● Send me **everything.**

○ Select individual events.

WEBHOOK HEADERS

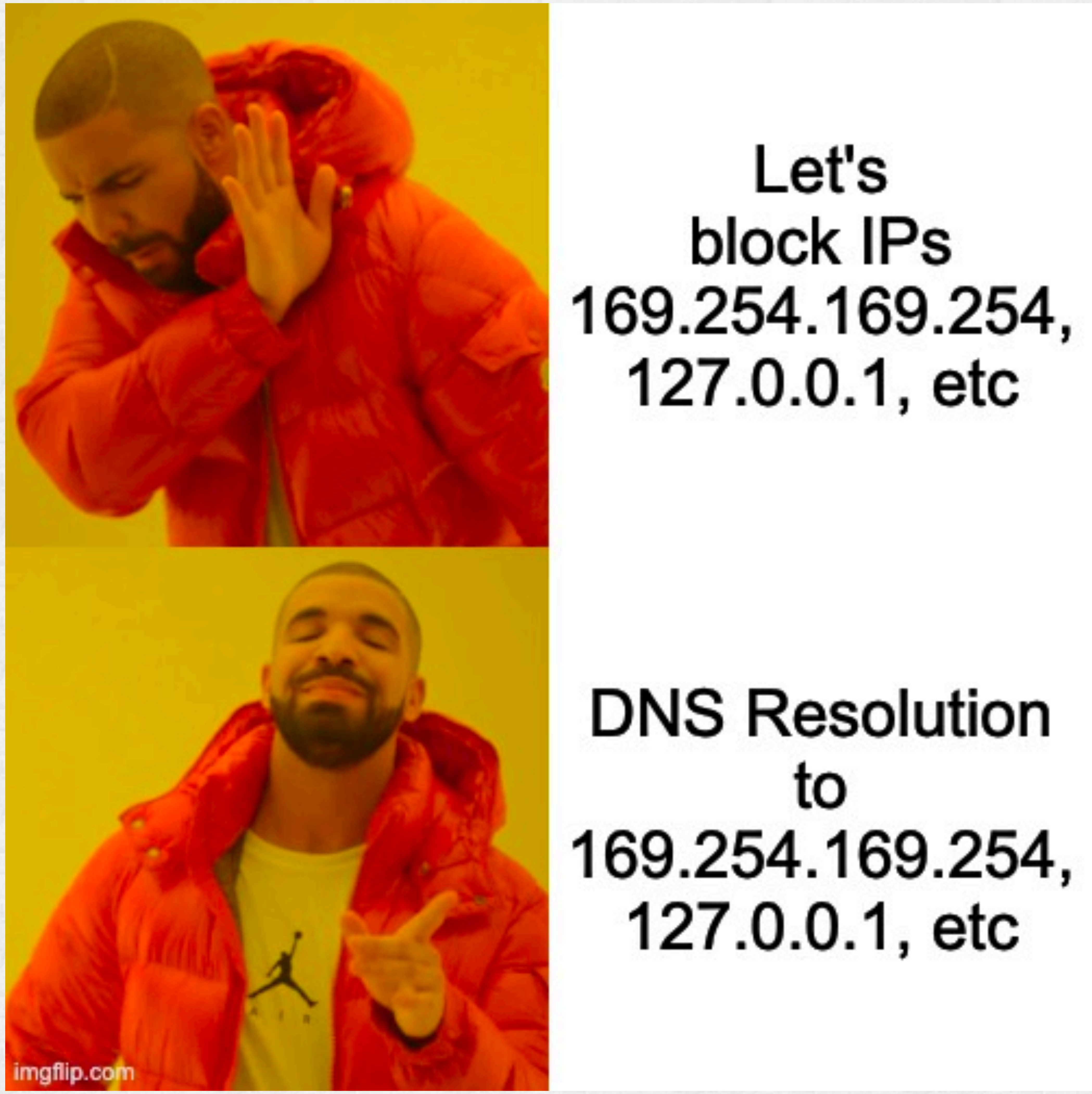
Key: E.g. X-API-KEY

Value: E.g. abc1234

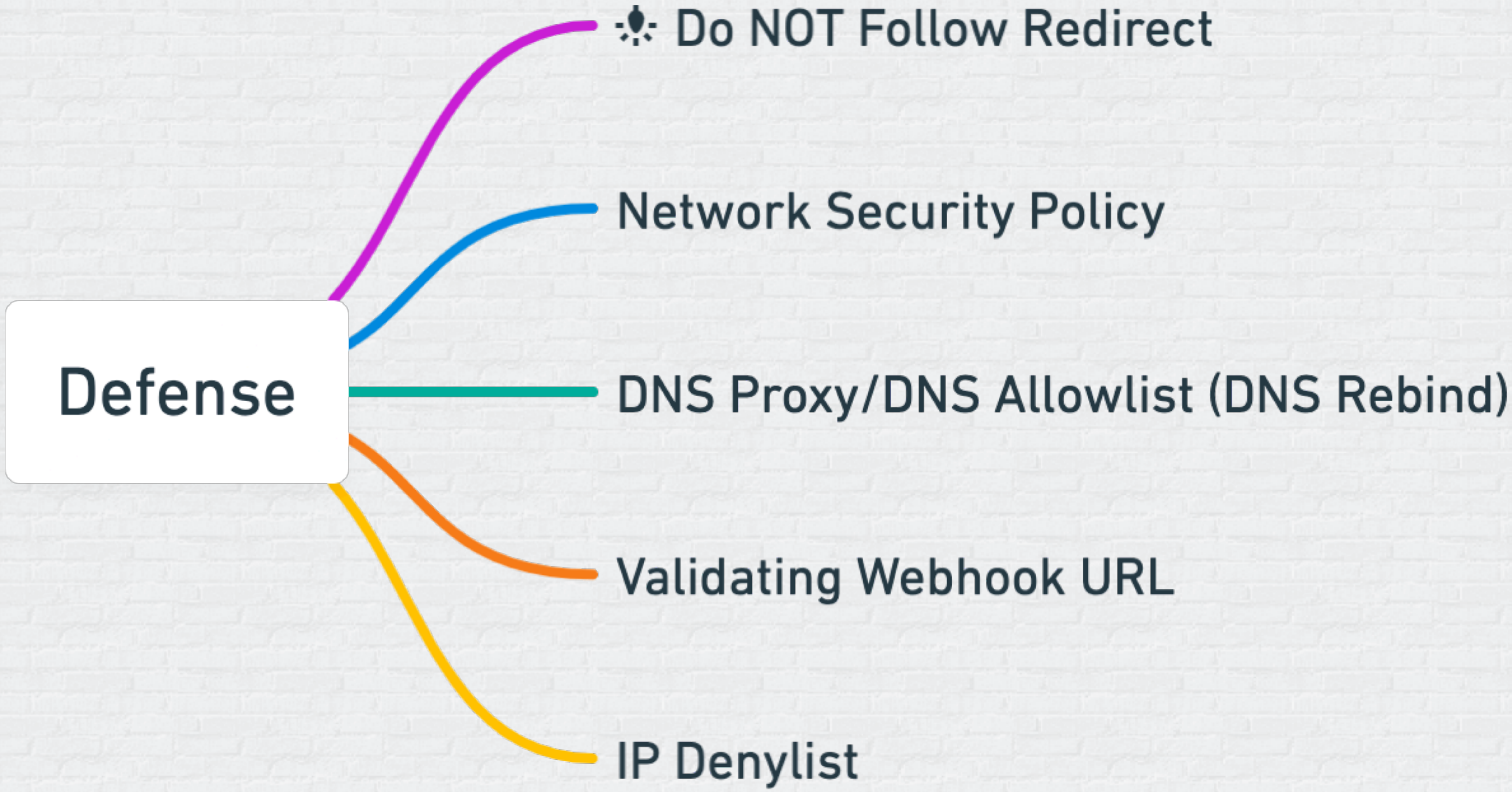
Metadata-Flavor Google

abhaybhargav

App Level IP Blocklisting?



Defense



Defense

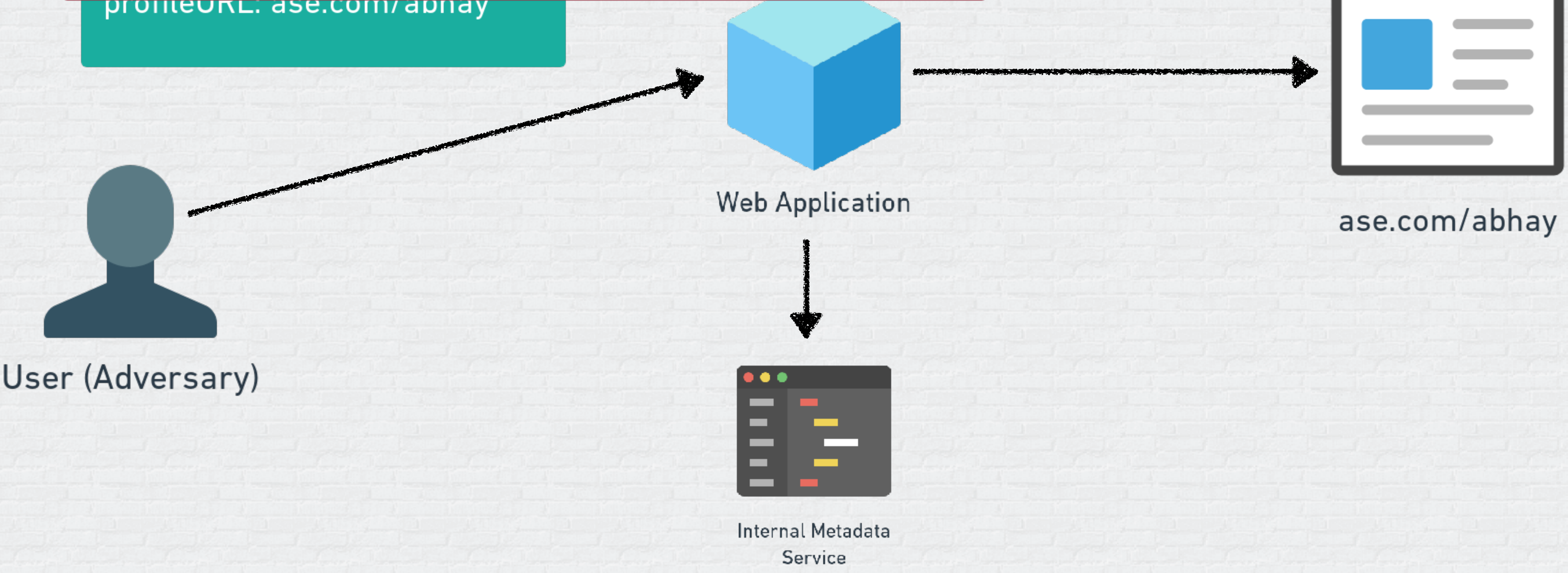
- Do NOT Follow Redirect
- Network Security Policy
- DNS Proxy/DNS Allowlist (DNS Rebind)
- Validating Webhook URL
- IP Denylist

Story 2: The Fully Loaded PDF Generator

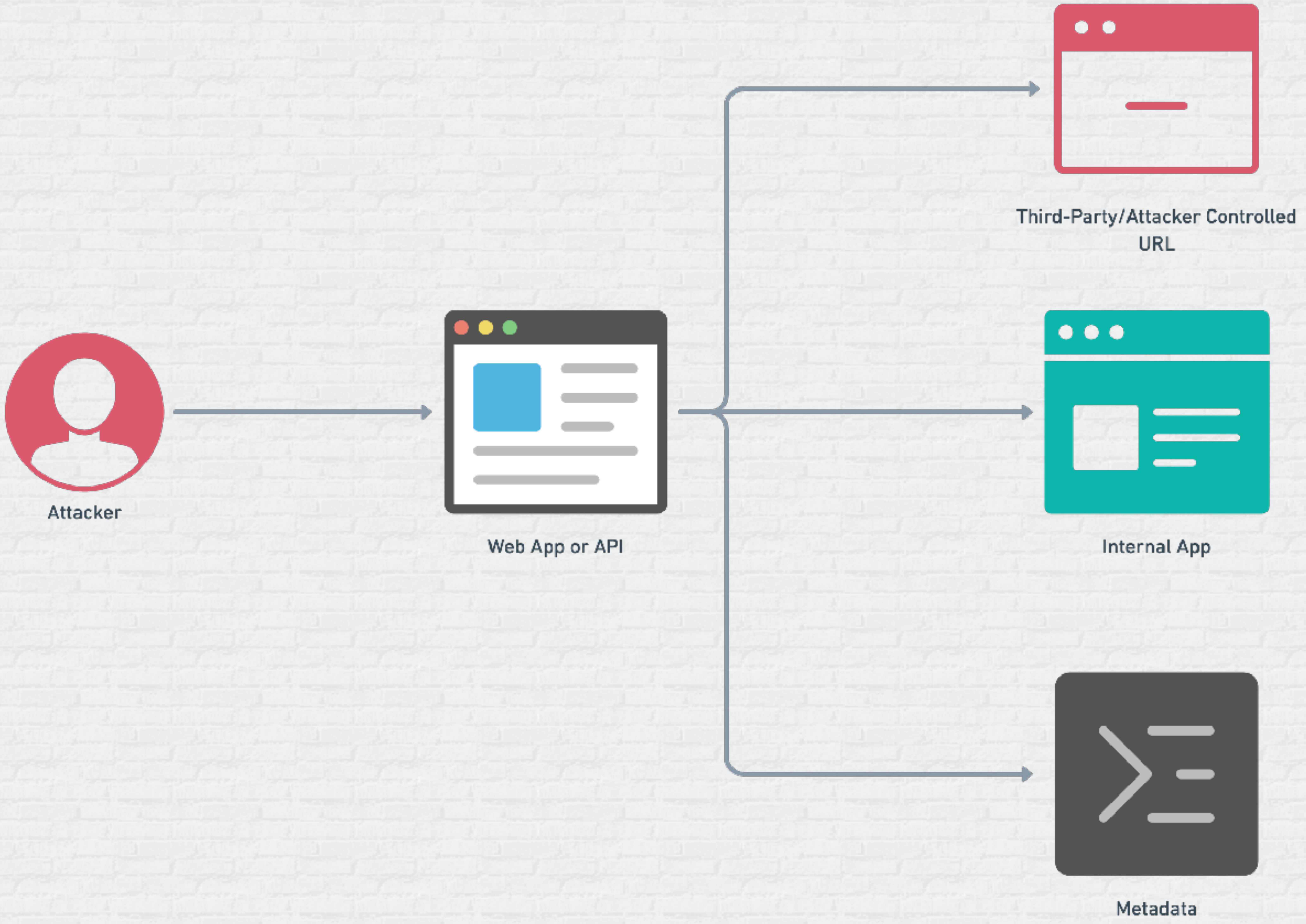
What is SSRF?

user: tom@ase.com
profileURL: 169.254.169.254/metadata/credentials/my-cred

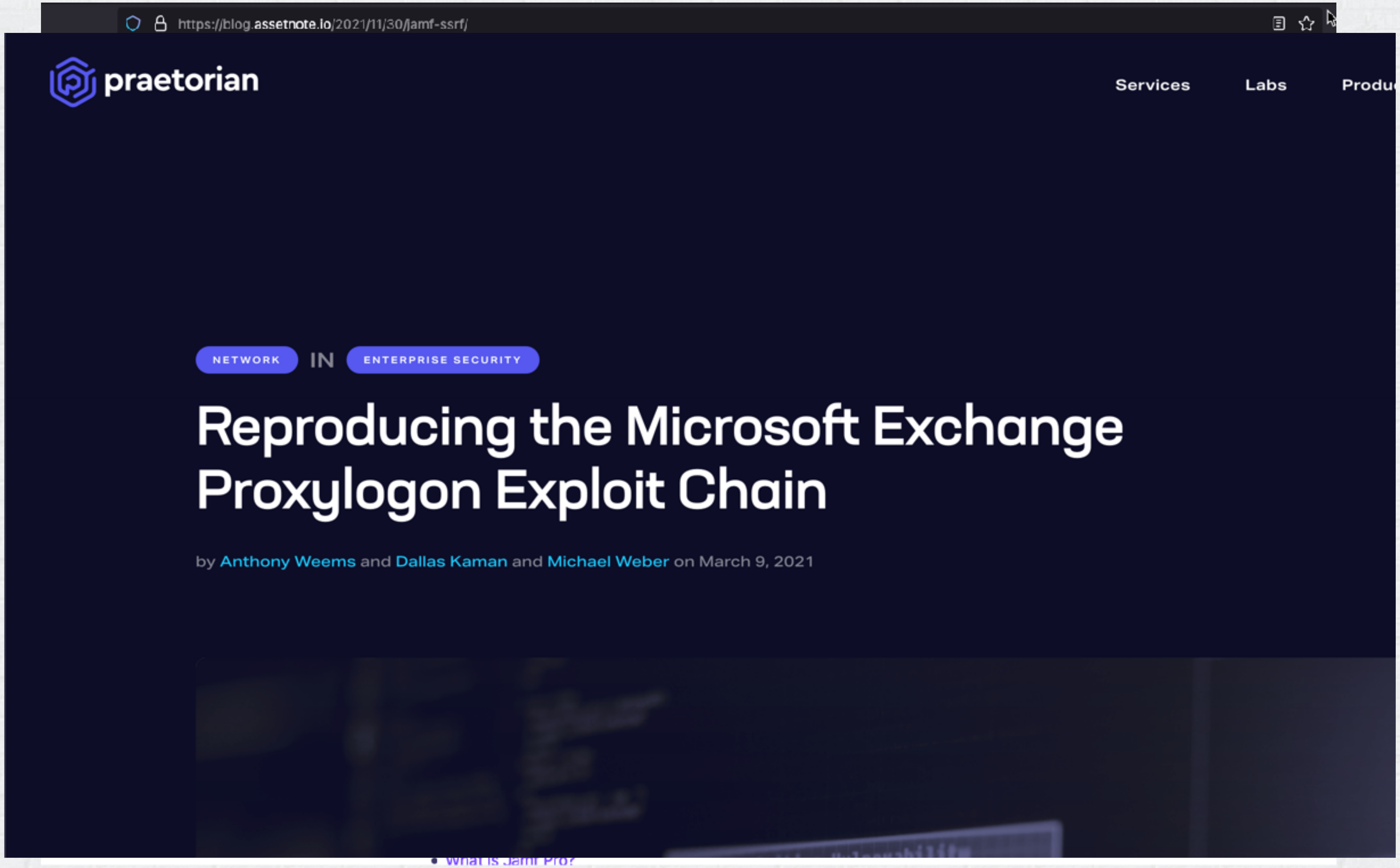
profileURL: ase.com/abhay



What is SSRF?


Third-Party/Attacker Controlled URL
Attacker
Web App or API
Internal App
Metadata

SSRF – Real-world Examples



https://blog.assetnote.io/2021/11/30/jamf-ssrf/

NETWORK IN ENTERPRISE SECURITY

Reproducing the Microsoft Exchange Proxylogon Exploit Chain

by Anthony Weems and Dallas Kaman and Michael Weber on March 9, 2021

- What is Jamf Pro?

Effects and Impact of SSRF

Steal Metadata for Cloud Compromise

Remote File Read

Remote Code Execution

Information Disclosure
Internal Hosts

Denial of Service

Why does SSRF happen?

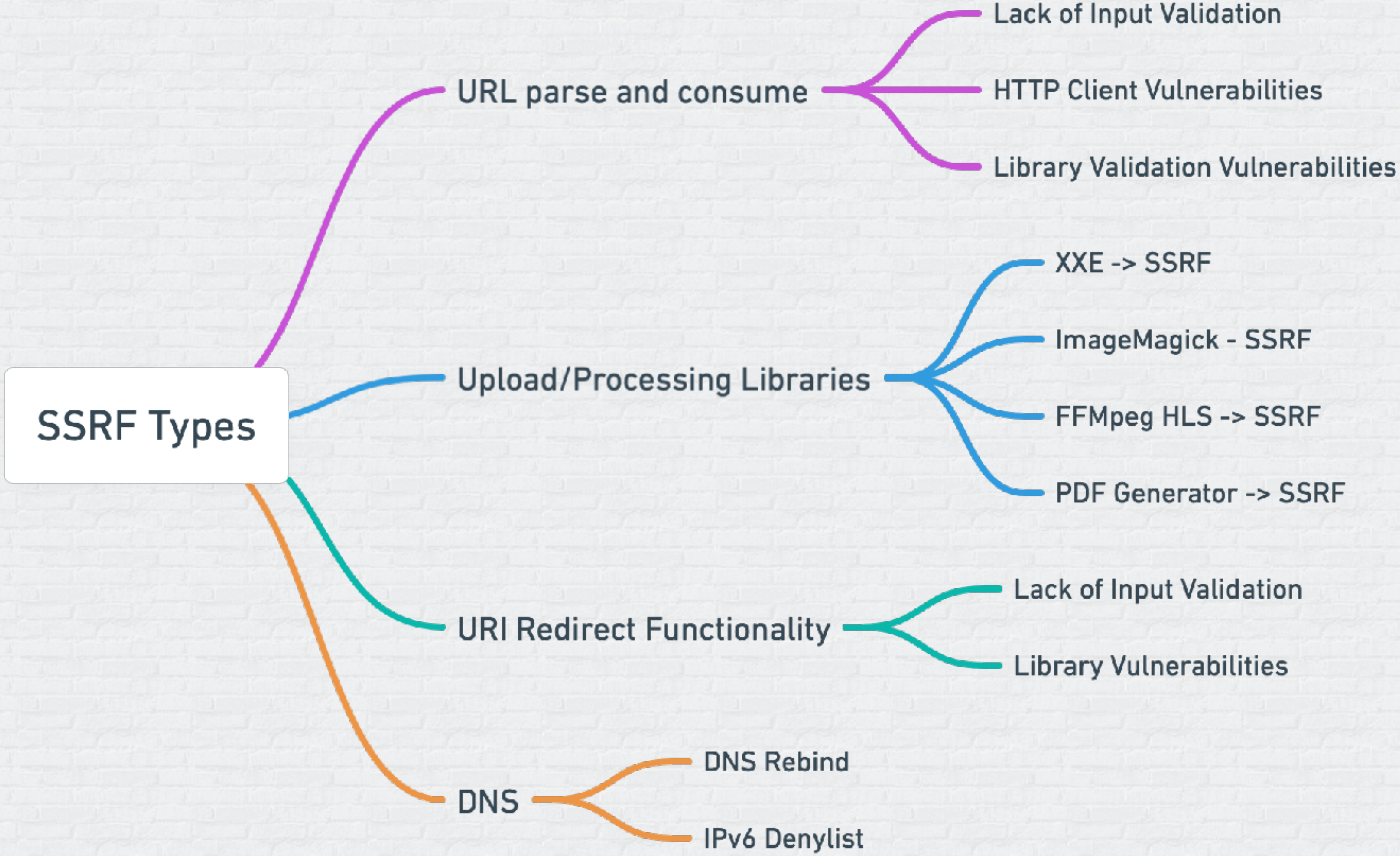
- Application makes HTTP requests based on URIs in Headers and/or Payload => Controlled by attacker
- Application Library makes requests based on URIs in Header and/or Payload => Controlled by attacker
- Application/Library includes content based on URIs from Header and/or payload => Controlled by attacker

Only HTTP?

- URI?
  - http(s)://
  - file://
  - gopher://
  - ssh://

Depends on the Client

SSRF Attack Types



SSRF Types

- URL parse and consume
  - Lack of Input Validation
  - HTTP Client Vulnerabilities
  - Library Validation Vulnerabilities
- Upload/Processing Libraries
  - XXE -> SSRF
  - ImageMagick - SSRF
  - FFMpeg HLS -> SSRF
  - PDF Generator -> SSRF
- URI Redirect Functionality
  - Lack of Input Validation
  - Library Vulnerabilities
- DNS
  - DNS Rebind
  - IPv6 Denylist

PDF Gen and Libraries

- PDF Generation Libraries - Popular for export, report gen, etc
- PDF Generation Libraries:
  - HTML Rendering => HTML and CSS to PDF
  - Headless Browsers => Webkit/Headless Chrome

Exploiting PDF Libraries

- Typically allow users to load specific HTML tags:
  - <img>
  - <iframe>
  - <style>

WeasyPrint SSRF

- Technique discovered by @NahamSec and CodyBrocious
- Converts HTML to PDF with very support for limited user-generated HTML tags
- Allows you to use <link> tag

Story 2
Maya and the Shopping Spree

The situation

- Maya travels a lot for work. Pre-COVID of course 😄
- She submits expense reports and invoices in an internal expense-management system that her company has developed
- Each expense is reviewed by her Project Manager and approved after review
- Once approved, these bills automatically go into a Payment System where the employee is reimbursed with a bank transfer

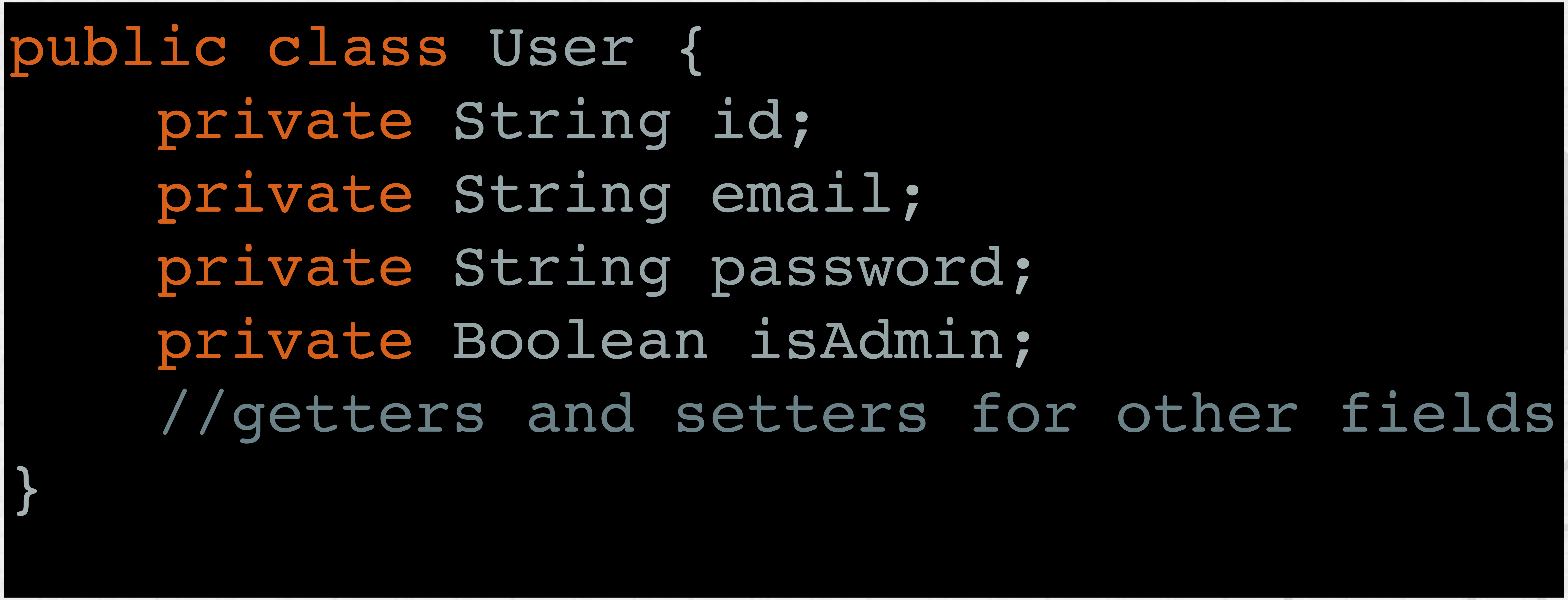
The Problem

- Maya has run into a bit of a debt problem. She has bills she can’t pay.
- She’d love nothing more than getting “larger” approvals for all the bills submitted
- But how does she do that?

What is an IDOR?

- Authorization Bypass (some cases for Elevation of Privileges)
- Adversary is able to leverage a vulnerable authorization system to gain access to records that should be unauthorized to access
- Two Modes:
  - Primary Key
  - Mass-Assignment

Mass Assignment



```java
public class User {
    private String id;
    private String email;
    private String password;
    private Boolean isAdmin;
    //getters and setters for other fields
}
```

Exploiting Mass Assignment

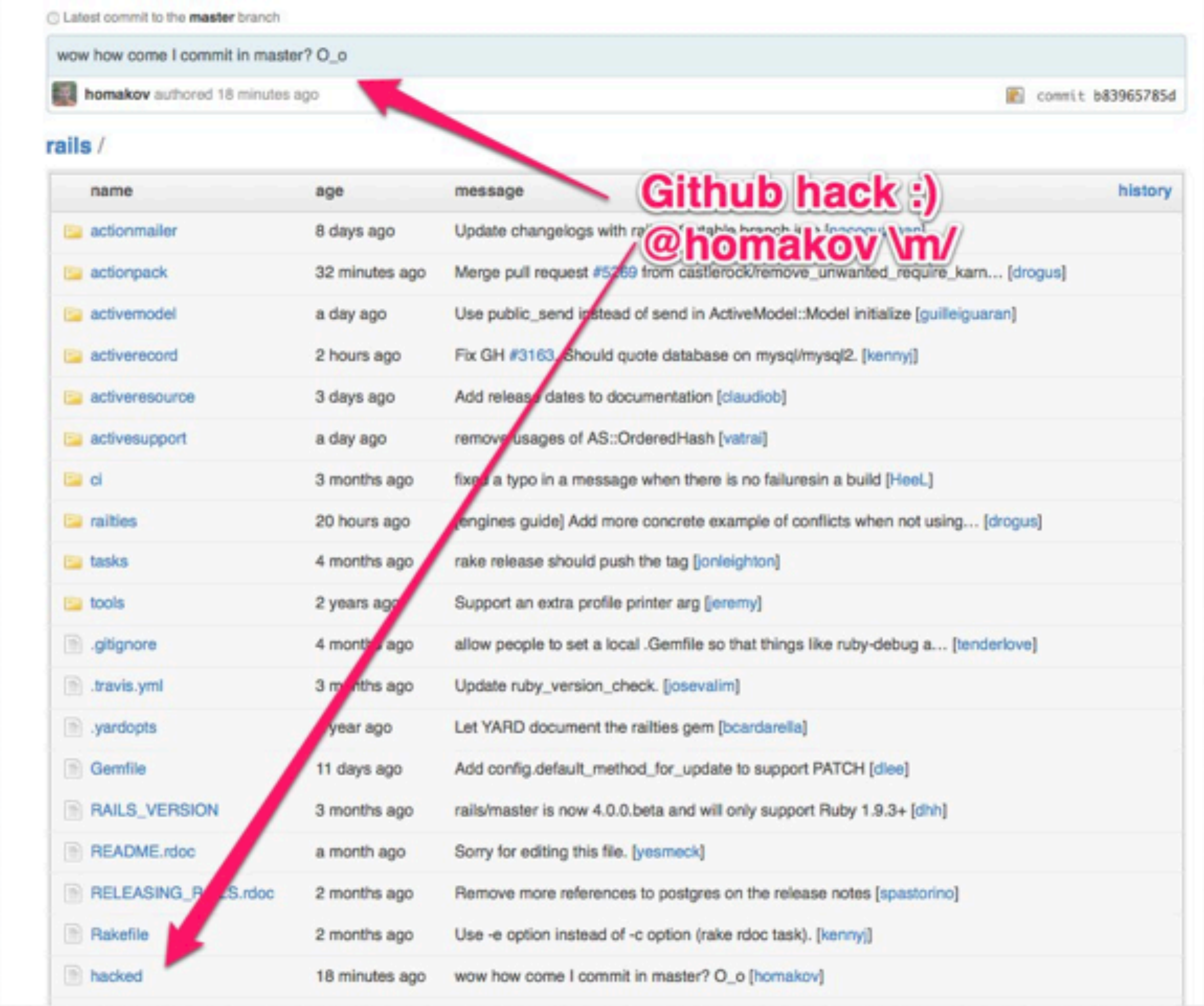
```
public static Result form(){
    Form<User> filledForm  =
newUserForm.bindFromRequest();
}
```

Adversary can guess isAdmin=True and change user privileges

Ruby – Mass Assignment

```ruby
def signup
  params[:user]
  @user = User.new(params[:user])
end
```

Github's Mass Assignment Flaw – 2013



○ Latest commit to the **master** branch

wow how come I commit in master? O_o

homakov authored 18 minutes ago — commit b83965785d

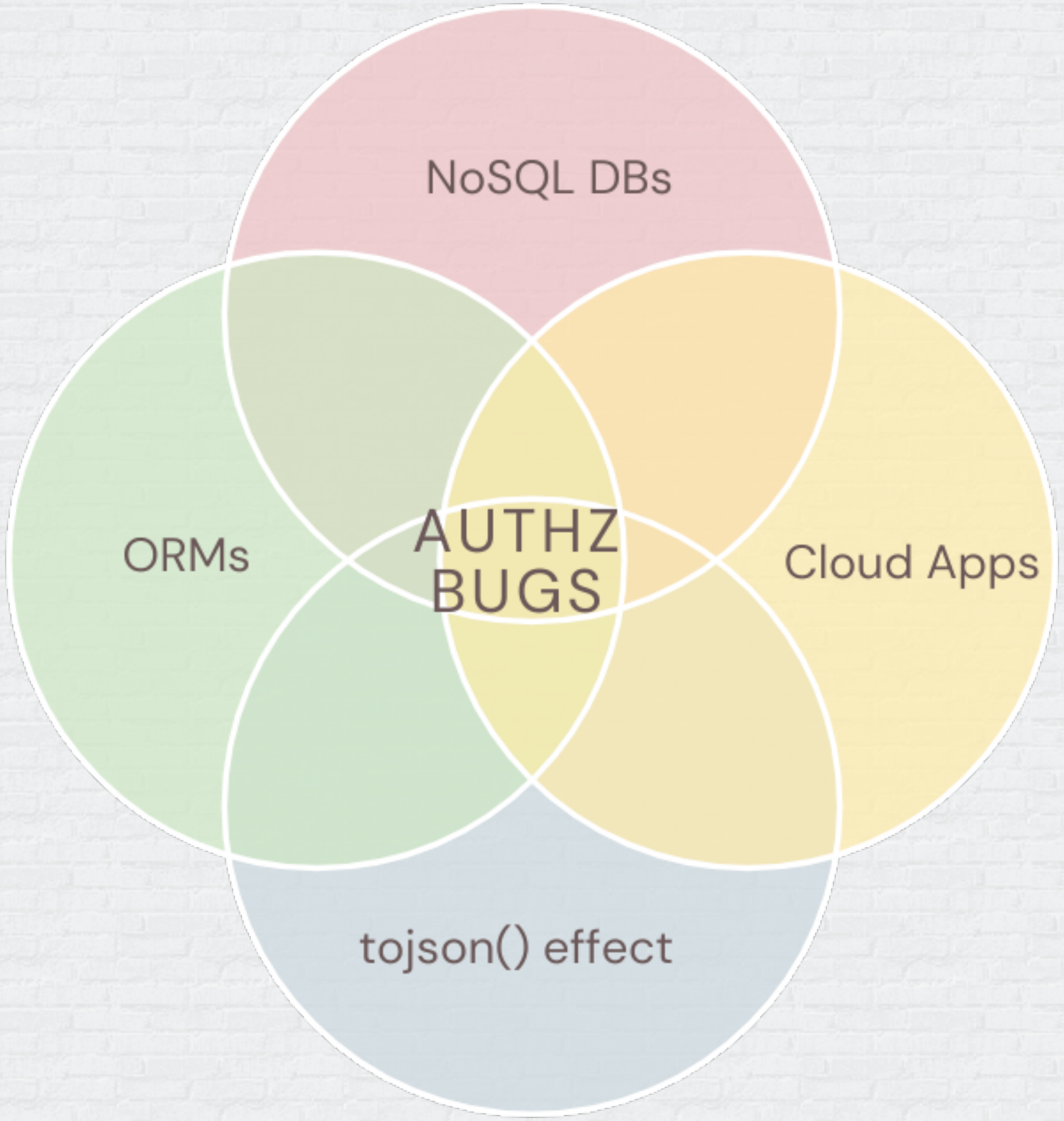
rails /

Github hack :)
@homakov \m/

name	age	message
actionmailer	8 days ago	Update changelogs with ra[illegible]
actionpack	32 minutes ago	Merge pull request #5269 from castlerock/remove_unwanted_require_karn... [drogus]
activemodel	a day ago	Use public_send instead of send in ActiveModel::Model initialize [guilleiguaran]
activerecord	2 hours ago	Fix GH #3163. Should quote database on mysql/mysql2. [kennyj]
activeresource	3 days ago	Add release dates to documentation [claudiob]
activesupport	a day ago	remove usages of AS::OrderedHash [vatrai]
ci	3 months ago	fixed a typo in a message when there is no failuresin a build [HeeL]
railties	20 hours ago	[engines guide] Add more concrete example of conflicts when not using... [drogus]
tasks	4 months ago	rake release should push the tag [jonleighton]
tools	2 years ago	Support an extra profile printer arg [jeremy]
.gitignore	4 months ago	allow people to set a local .Gemfile so that things like ruby-debug a... [tenderlove]
.travis.yml	3 months ago	Update ruby_version_check. [josevalim]
.yardopts	a year ago	Let YARD document the railties gem [bcardarella]
Gemfile	11 days ago	Add config.default_method_for_update to support PATCH [dlee]
RAILS_VERSION	3 months ago	rails/master is now 4.0.0.beta and will only support Ruby 1.9.3+ [dhh]
README.rdoc	a month ago	Sorry for editing this file. [yesmeck]
RELEASING_RAILS.rdoc	2 months ago	Remove more references to postgres on the release notes [spastorino]
Rakefile	2 months ago	Use -e option instead of -c option (rake rdoc task). [kennyj]
hacked	18 minutes ago	wow how come I commit in master? O_o [homakov]

The exploit

Why?



Defense