


# **The Attack Landscape of 2020 – What to look out for and how to protect yourself?**

- 
- *February 27<sup>th</sup>, 2020*

## Persona

- Pascal Schulz
- IT Security Engineer @ Dynatrace
-  PascalSec



*Disclaimer:*

*I am not affiliated to any of the products shown in this presentation*

WHY



## Capital One

**Date:** March 22 and 23, 2019

**Number of records breached:** 106 million

**Information exposed:** Names, addresses, ZIP codes, phone numbers, email addresses, birthdates and self-reported income. Customer credit scores, credit limits, balances, payment history, and contact information.



## Evite

**Date:** February 22, 2019

**Number of records breached:** 100 million

**Information exposed:** Names, email addresses, passwords, and IP addresses of Evite customers.



## American Medical Collection Agency

**Date:** August 1, 2018, to March 30, 2019

**Number of records breached:** More than 20 million

**Information exposed:** Social Security numbers, dates of birth, payment card data, and credit card information.



HOW





# OWASP Top 10 - 2017

The Ten Most Critical Web Application Security Risks



<https://owasp.org>

This work is licensed under a  
[Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/)



## T10

## OWASP Top 10 Application Security Risks – 2017

6

### A1:2017- Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

### A2:2017-Broken Authentication

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

### A3:2017- Sensitive Data Exposure

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

### A4:2017-XML External Entities (XXE)

Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

### A5:2017-Broken Access Control

Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

### A6:2017-Security Misconfiguration

Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.

### A7:2017- Cross-Site Scripting (XSS)

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

### A8:2017- Insecure Deserialization

Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

### A9:2017-Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

### A10:2017- Insufficient Logging & Monitoring

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.



## OWASP 2020 Operating Plan

Draft #4 for Board Review

**Vision: Global and open resource for software security**

**Updated** Mission Statement: OWASP is a nonprofit foundation improving the security of software. Through community-led open source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure our digital lives.

### Goals

1. Promote updated version of OWASP Top 10 set to release in october 2020.
2. Continue to optimize business operations to overachieve financial and membership targets.
3. Manage two successful global conferences planning three in 2021.
4. Launch Project Summits and AppSec Days to over 500 attendees
5. Increase relevance and reputation of OWASP measured by 10% increase in web traffic.
6. Improve satisfaction with OWASP by survey measured a 10% increase.
7. Increase corporate and individual membership by 25%

# The Attack Landscape of 2020 – What to look out for and how to protect yourself?

• February 27<sup>th</sup>, 2020



# Where is my data coming from?

---



Dynatrace

Application Performance, Real-User / Cloud Monitoring Solution [SaaS based]

<http://dynatrace.com>

Reports resolved	Assets in scope	Average bounty
50	7	\$100-\$250

Submit report

Edit Page

Bug Bounty Program

Launched on Apr 2019

Managed by HackerOne

☆ Bookmark

🔔 Subscribe

Rewards

Critical

High

Medium

Low

\$1,500

\$500

\$250

\$100

Last updated on April 8, 2019.

View changes

Credentials

Credentials have been provided for testing

Show Credentials

Response Efficiency

17 hrs

Average time to first response

2 days

Average time to triage

4 days

Average time to bounty

6 days

Average time to resolution

100% of reports

Meet [response standards](#)

Policy

At Dynatrace, the security of our software and solutions is a top priority. We want to invite security researchers from all over the world to participate in our public bug bounty program. If you went ahead and found a security bug in our environment, please proceed and file a bug via Hackerone. We are looking forward to remediating the issue together with you as quickly as possible.

Response Targets

Dynatrace will endeavor to meet the following response SLAs for security researchers participating in our program:

- Time to first response (from report submit) - 2 business days
- Time to triage (from report submit) - 2 business days

# Find out more about the program



<https://www.dynatrace.com/news/blog/dynatrace-incorporates-hackerones-bug-bounty-program-into-their-security-playbook/>

**<https://www.hackerone.com/top-10-vulnerabilities>**

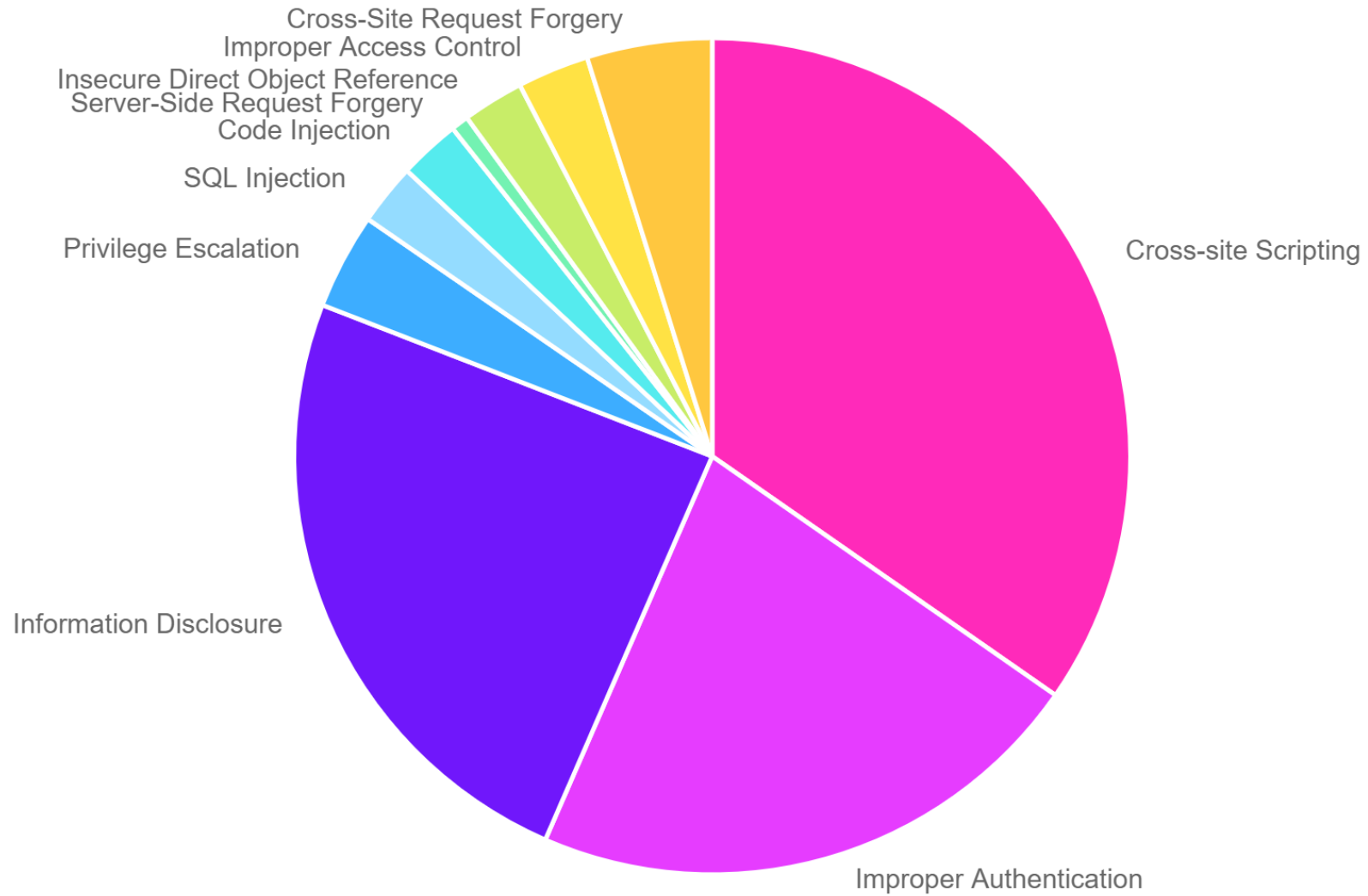


# INTRO

HackerOne has one of the largest and most robust databases of valid vulnerabilities, from across diverse industries and attack surfaces. These resolved vulnerabilities represent the real world risk that existed for over 1,400 organizations including technology unicorns, governments, startups, financial institutions and open source projects. Now, for the first time ever, we're providing our list of the top 10 rewarded vulnerability types as indicated by bounty awards and customer impact.



## TOTAL REPORT VOLUME BY WEAKNESS



**<https://hackerone.com/hacktivity>**



## Hacktivity









See the latest hacker activity on HackerOne

### Sort

☐ Popular☒ New

### Type

☐ All☐ Bug Bounty☐ Published☒ Disclosed

10		<b>No Rate Limit On Forgot Password Page Of NordVPN</b> By <a href="#">th3pr0xyb0y</a> to <a href="#">NordVPN</a>   <span>Resolved</span>   <span>Medium</span>   \$500.00	disclosed 19 hrs ago
6		<b>Content injection via URL parameter.</b> By <a href="#">johnh4x0r</a> to <a href="#">TTS Bug Bounty</a>   <span>Duplicate</span>	disclosed about 1 day ago
41		<b>Bypass Password Authentication for updating email and phone number - Security Vulnerability</b> By <a href="#">jayesh25</a> to <a href="#">Twitter</a>   <span>Resolved</span>   <span>High</span>   \$700.00	disclosed about 1 day ago
3		<b>Bypass to report #280389 [Thinking The issue is not fixed Yet]</b> By <a href="#">4m4n</a> to <a href="#">Infogram</a>   <span>Resolved</span>   <span>Medium</span>	disclosed 2 days ago
2		<b>[jsreport] Remote Code Execution</b> By <a href="#">ermilov</a> to <a href="#">Node.js third-party modules</a>   <span>Resolved</span>   <span>High</span>	disclosed 2 days ago
27		<b>Blind XSS in redtube administering site my.reflected.net</b> By <a href="#">johndoe1492</a> to <a href="#">Redtube</a>   <span>Resolved</span>   <span>High</span>   \$1,000.00	disclosed 2 days ago
2		<b>[script-manager] Unintended require</b> By <a href="#">ermilov</a> to <a href="#">Node.js third-party modules</a>   <span>Resolved</span>   <span>Low</span>	disclosed 2 days ago
10		<b>The password limit is not set, [DoS].</b> By <a href="#">hakmod</a> to <a href="#">Localize</a>   <span>Resolved</span>   <span>Low</span>	disclosed 3 days ago

**<https://portswigger.net/research/top-10-web-hacking-techniques-of-2019>**

---



The results are in!

After **51 nominations** whittled down to 15 finalists by a community vote, an expert panel consisting of **Nicolas Grégoire**, **Soroush Dalili**, **Filedscriptor**, and **myself** have conferred, voted, and selected the Top 10 new web hacking techniques of 2019.

Every year, professional researchers, seasoned pentesters, bug bounty hunters, and academics release a flood of



### 3. Owning The Clout Through Server Side Request Forgery

This presentation from Ben Sadeghipour and Cody Brocious starts out with an overview of existing SSRF techniques, shows how they can be adapted and applied to server-side PDF generators, then brings DNS rebinding into the mix for good measure.

The work targeting PDF generators is an insightful look into a feature-class that's all too easily ignored. We first saw DNS rebinding on server-side browsers appear on the 2018 nomination list, and the release of HTTPRebind should help make this attack more accessible than ever.

Finally, I might be wrong about this but I suspect this presentation may deserve some credit for finally persuading Amazon to think about securing their EC2 metadata endpoint.

### 2. Cross-Site Leaks

Cross-site leaks have been a long time coming. First documented over a decade ago, and creeping into our top 10 last year, it's in 2019 that awareness of this attack class and its sheer number of crazy variations exploded.

It's hard to apportion credit at such a scale but we clearly owe thanks to Eduardo Vela's succinct introduction to the concept with a novel technique, the collaborative effort to build a public list of known XS-Leak vectors, and researchers applying the XS-Leaks technique to great effect.

XS-Leaks have already had a lasting impact on the web security landscape, as they played a major role in the death of browser XSS filters. Block-mode XSS filtering was a major source of XS-Leak vectors, and this combined with even worse issues with filter-mode to persuade Edge and later Chrome to both discard their filters in a victory for web security and a disaster for web security researchers alike.

### 1. Cached and Confused: Web Cache Deception in the Wild

In this academic whitepaper, Sajjad Arshad et al take Omer Gil's Web Cache Deception technique (which premiered at #2 in our top 10 back in 2017), and share a systematic exploration of Web Cache Deception vulnerabilities across the Alexa Top 5000 websites.

For legal reasons, most offensive security research is conducted during professional audits or on websites with bug bounty programs, but through careful ethical footwork this research offers a glimpse into the state of security on the wider web. With the help of a well-crafted methodology that could easily be adapted for other techniques, they prove that Web Cache Deception is still a prevalent threat.



WHAT



*Disclaimer:*

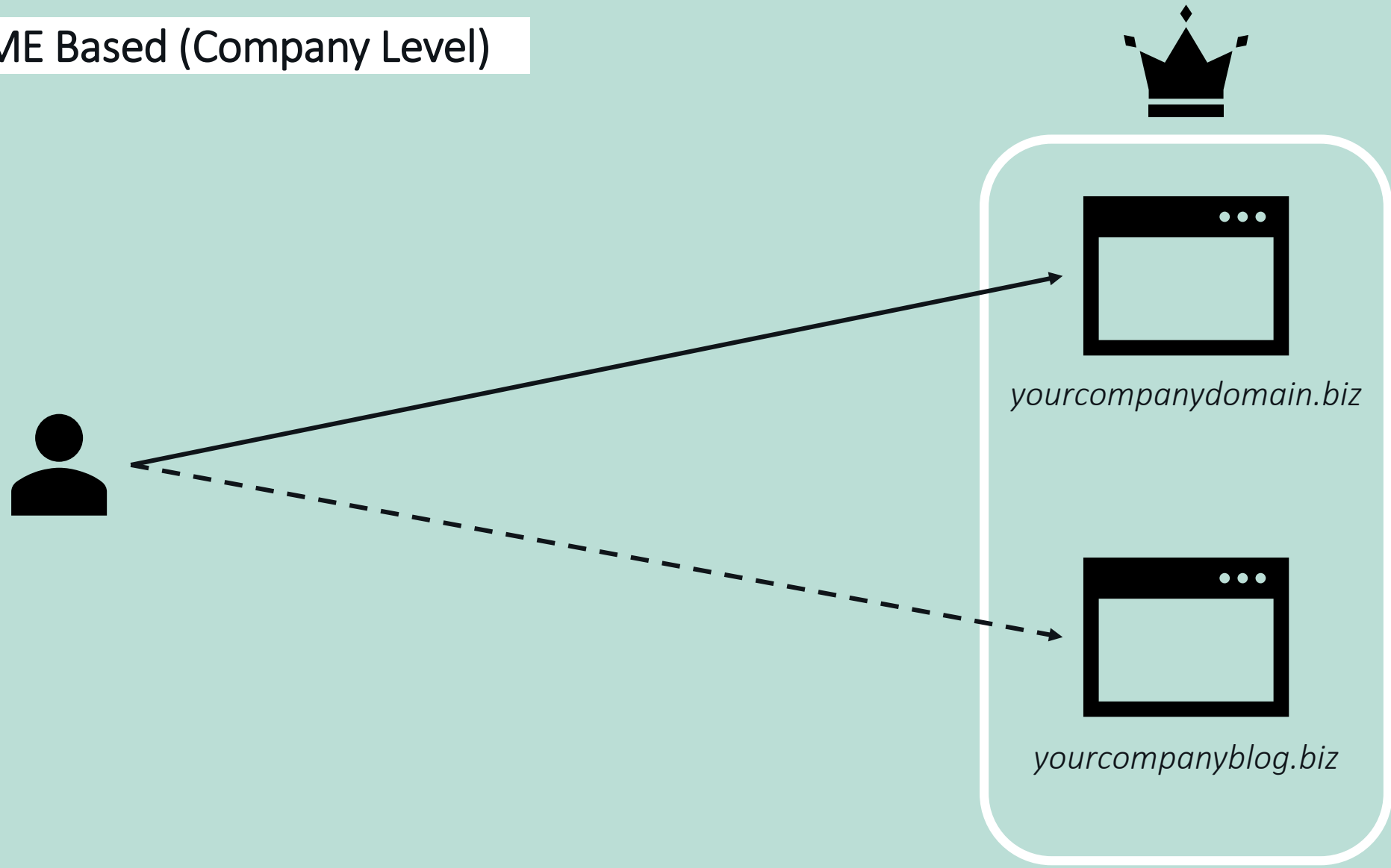
*Some of the vulnerabilities shown have been existing for quite a while now.*

*However, we have seen more and more whitehat hackers concentrating on the ones to follow throughout the last two years.*

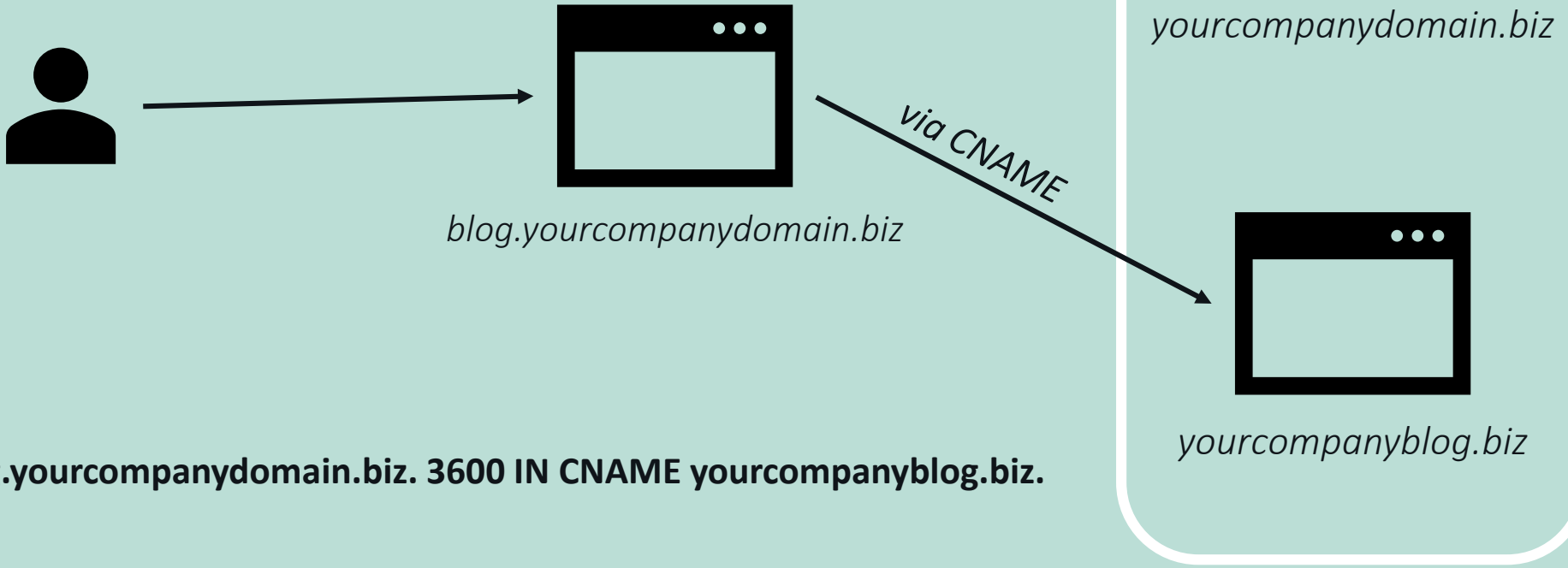
# Subdomain Takeover

---

## CNAME Based (Company Level)

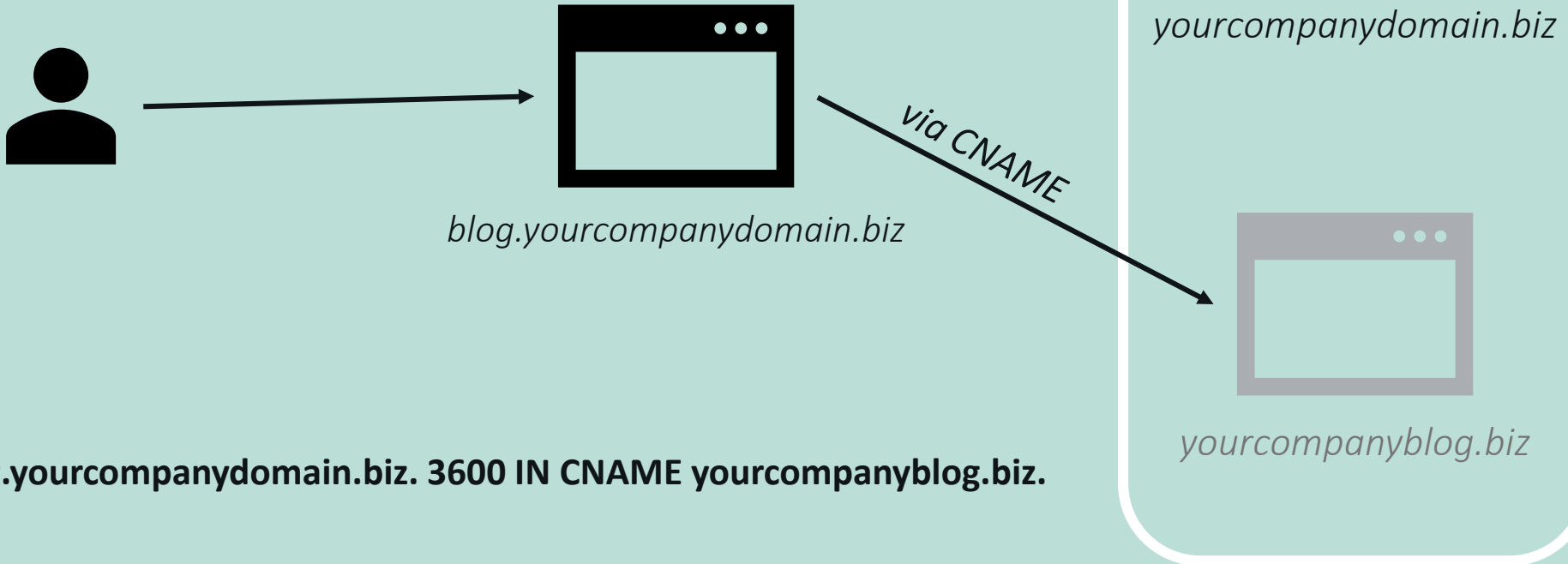


## CNAME Based (Company Level)



**blog.yourcompanydomain.biz. 3600 IN CNAME yourcompanyblog.biz.**

## CNAME Based (Company Level)



**blog.yourcompanydomain.biz. 3600 IN CNAME yourcompanyblog.biz.**

# Search results

Q

Continue to Cart

All domains include Basic Privacy Protection

Domain Available

Call 020 7084 1810 for buying assistance

yourcompanyblog.biz is available

£7.10

~~£20.10~~

for the first year

☐

yourcompanyblog.com Add this: £0.99

when you register for 2 years or more, 1st year price £0.99 Additional years £16.10

Why it's great.

✓ "Your" and "Blog" are widely used keywords.

✓ "Yourcompanyblog" is 15 characters or less.

✓ Includes Basic Privacy Protection

▶ How to choose a great domain name?

Add to Cart

Buy 3 and Save 56%

yourcompanyblog.com  
yourcompanyblog.net  
yourcompanyblog.org

~~£50.30~~ £22.00

for the first year

Add to Cart

Available Alternate Domains

.com £0.99

.co.uk £0.01

.eu £4.99

.net £11.99

.info £2.99

yourcompany.blog

~~£31.10~~ £9.10

for the first year

Add to Cart

## CNAME Based (Company Level)

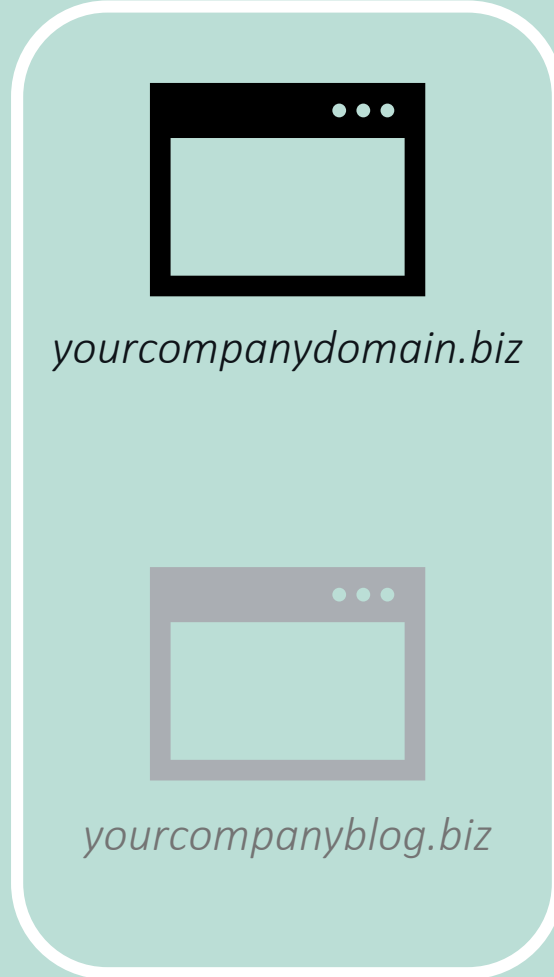
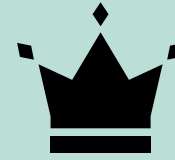


*blog.yourcompanydomain.biz*

*via CNAME*



*yourcompanyblog.biz*



*yourcompanydomain.biz*

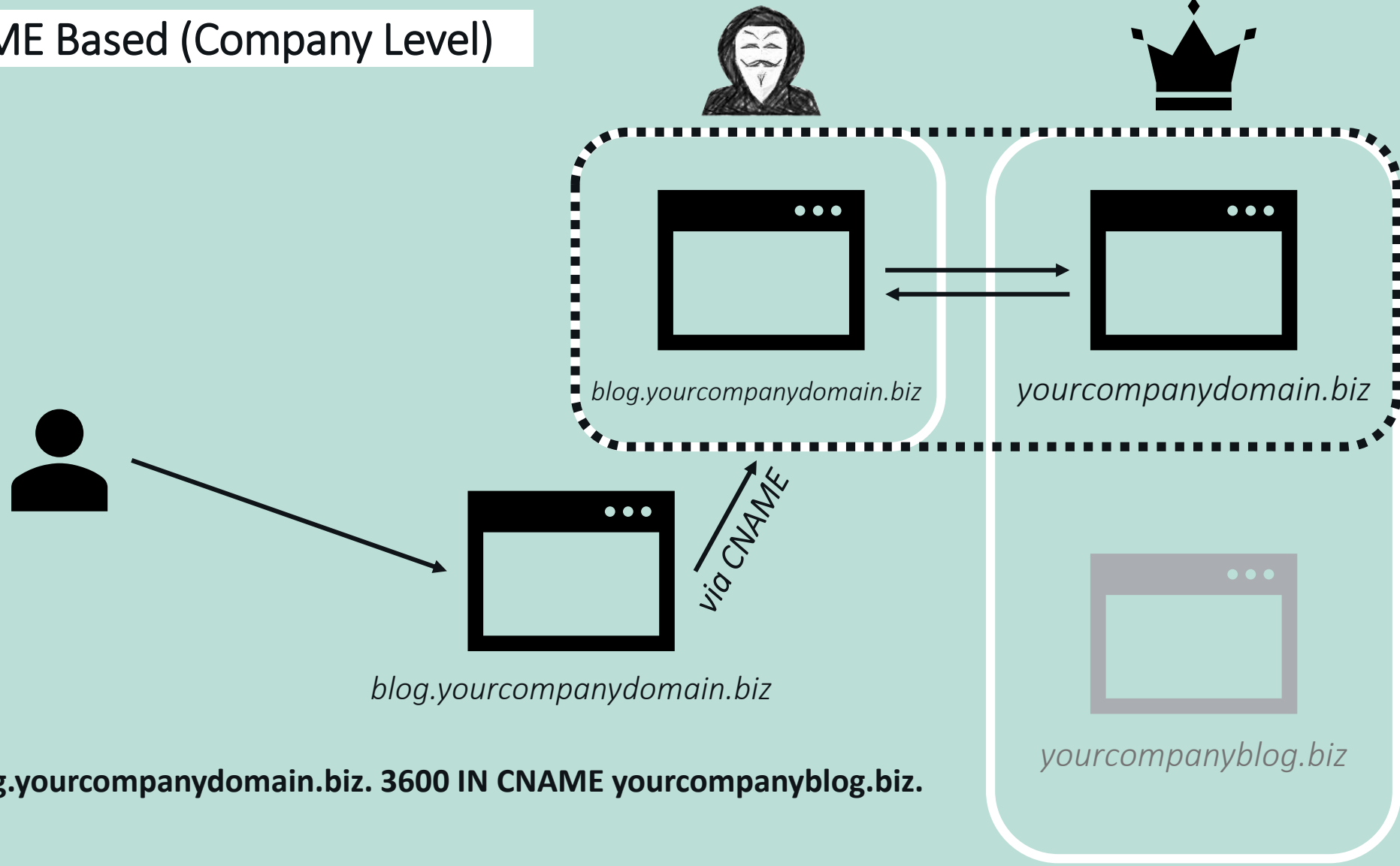


*yourcompanyblog.biz*

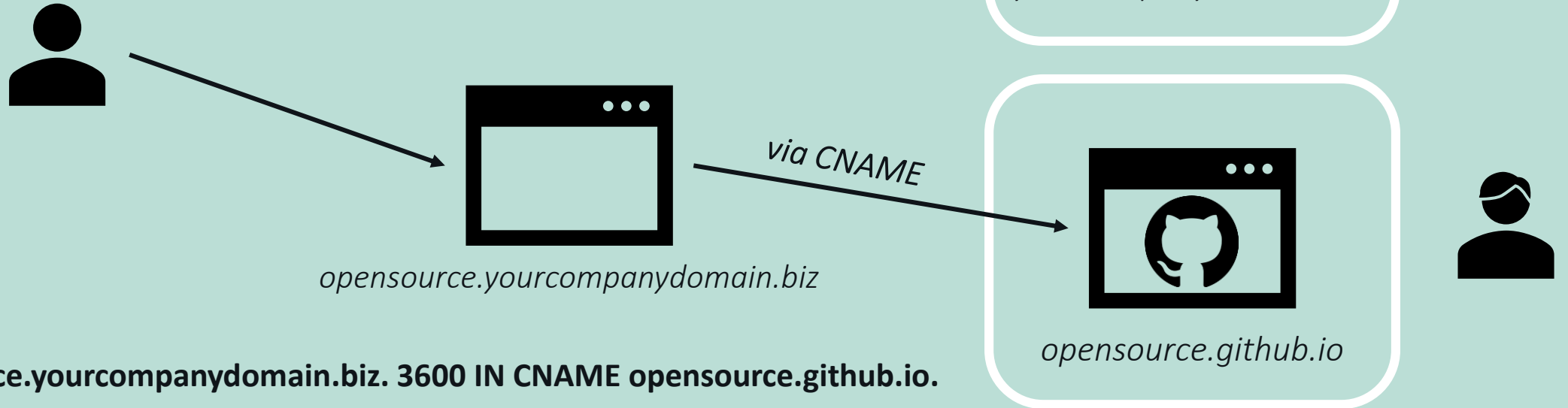
**blog.yourcompanydomain.biz. 3600 IN CNAME yourcompanyblog.biz.**



## CNAME Based (Company Level)



## CNAME Based (Dev Level)



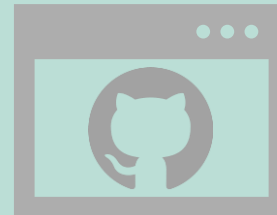
## CNAME Based (Dev Level)



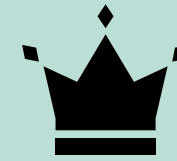
*opensource.yourcompanydomain.biz*



*via CNAME*



*opensource.github.io*



*yourcompanydomain.biz*

**opensource.yourcompanydomain.biz. 3600 IN CNAME opensource.github.io.**

# 404

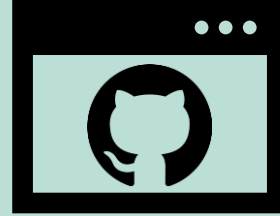
There isn't a GitHub Pages site here.

If you're trying to publish one, [read the full documentation](#) to learn how to set up **GitHub Pages** for your repository, organization, or user account.

GitHub Status — @githubstatus



## CNAME Based (Dev Level)



*opensource.github.io*

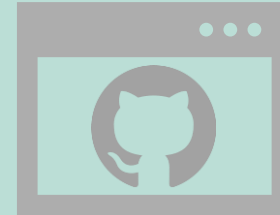


*yourcompanydomain.biz*



*opensource.yourcompanydomain.biz*

*via CNAME*

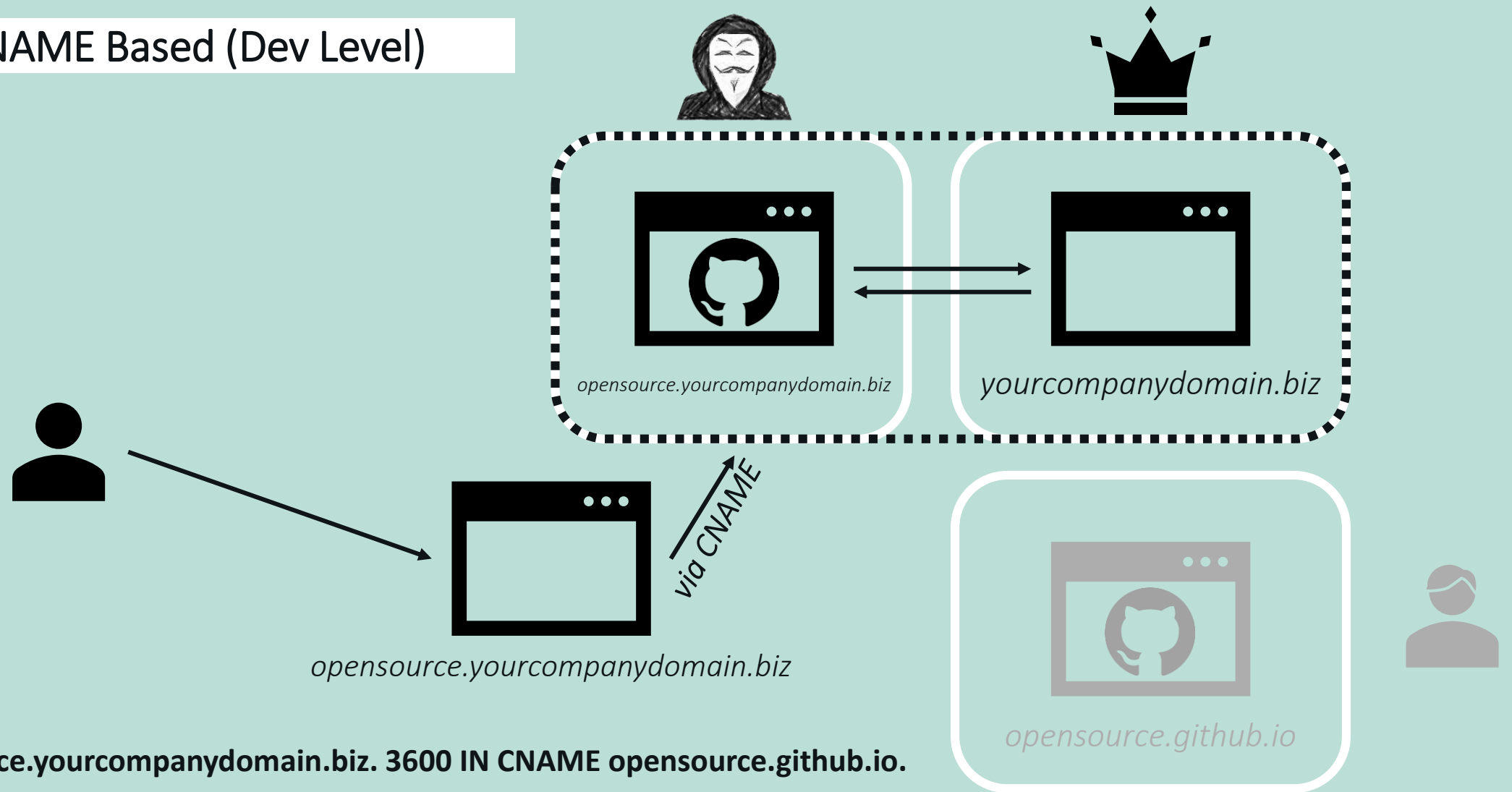


*opensource.github.io*



**opensource.yourcompanydomain.biz. 3600 IN CNAME opensource.github.io.**

## CNAME Based (Dev Level)



## Similar Behaviour With

- Amazon S3
- Heroku
- Shopify
- Microsoft Azure
- Statuspage
- Tumblr
- Wordpress
- And more...



Be aware that this also works  
with NS and MX DNS entries

# What I Need You To Do



Paid Service

# Asset Monitoring

We'd love to show you what Detectify can do for your business!

## What is subdomain takeover?

One common security threat is exposing old subdomain names. Subdomains pointing to third party services no longer being used make it possible for malicious hackers to register the subdomain on that third party and (effectively) hijack the subdomain. Some issues have already been published on our [blog](#).

Detectify provides a tool that allows you to monitor subdomains for such vulnerabilities based on your domain names. Asset Monitoring continuously monitors changes within public DNS resolvers and warns you as soon as it detects any anomalies.



# Self-Service



# Can I takeover XYZ?

A list of services and how to claim (sub)domains with dangling DNS records.

## Disclaimer

The authors of this document take no responsibility for correctness. This project is merely here to help guide security researchers towards determining whether something is vulnerable or not, but does not guarantee accuracy. This project heavily relies on contributions from the public; therefore, proving that something is vulnerable is the security researcher and bug bounty program's sole discretion. On top of that, it is worth noting that some bug bounty programs may accept dangling DNS record reports without requiring proof of compromise.

## What is a subdomain takeover?

Subdomain takeover vulnerabilities occur when a subdomain (subdomain.example.com) is pointing to a service (e.g. GitHub pages, Heroku, etc.) that has been removed or deleted. This allows an attacker to set up a page on the service that was being used and point their page to that subdomain. For example, if subdomain.example.com was pointing to a GitHub page and the user decided to delete their GitHub page, an attacker can now create a GitHub page, add a CNAME file containing subdomain.example.com, and claim subdomain.example.com.

You can read up more about subdomain takeovers here:

- <https://labs.detectify.com/2014/10/31/hostile-subdomain-takeover-using-herokugithubdeck-more/>

## All entries

Engine	Status	Fingerprint	Discussion	Documentation
Airee.ru	Vulnerable		<a href="#">Issue #104</a>	
Akamai	Not vulnerable		<a href="#">Issue #13</a>	
AWS/S3	Vulnerable	The specified bucket does not exist	<a href="#">Issue #36</a>	
Bitbucket	Vulnerable	Repository not found		
Campaign Monitor	Vulnerable	'Trying to access your account?'		<a href="#">Support Page</a>
Cargo Collective	Vulnerable	404 Not Found		<a href="#">Cargo Support Page</a>
Cloudfront	Not vulnerable	ViewerCertificateException	<a href="#">Issue #29</a>	<a href="#">Domain Security on Amazon CloudFront</a>
Desk	Not vulnerable	Please try again or try Desk.com free for 14 days.	<a href="#">Issue #9</a>	
Digital Ocean	Vulnerable	Domain uses DO name serves with no records in DO.		
Fastly	Edge case	Fastly error: unknown domain:	<a href="#">Issue #22</a>	
Feedpress	Vulnerable	The feed has not been found.	<a href="#">HackerOne #195350</a>	
Fly.io	Vulnerable	404 Not Found	<a href="#">Issue #101</a>	
Freshdesk	Not vulnerable			<a href="#">Freshdesk Support Page</a>
Ghost	Vulnerable	The thing you were looking for is no longer here, or never was.		

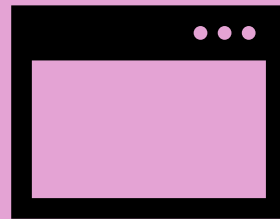
# Metadata SSRF

---





*PORT 80,443  
ALLOWED*



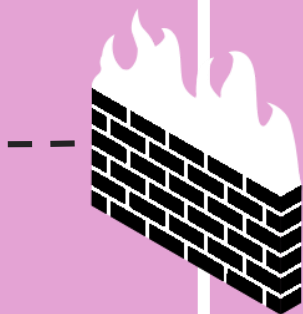
*AWS*



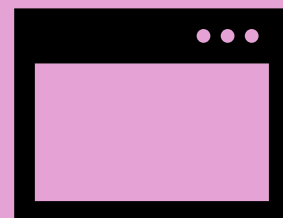
*GCP*



*AZURE*



*PORT 80,443  
ALLOWED*



*e.g. <http://169.254.169.254/latest/user-data>*



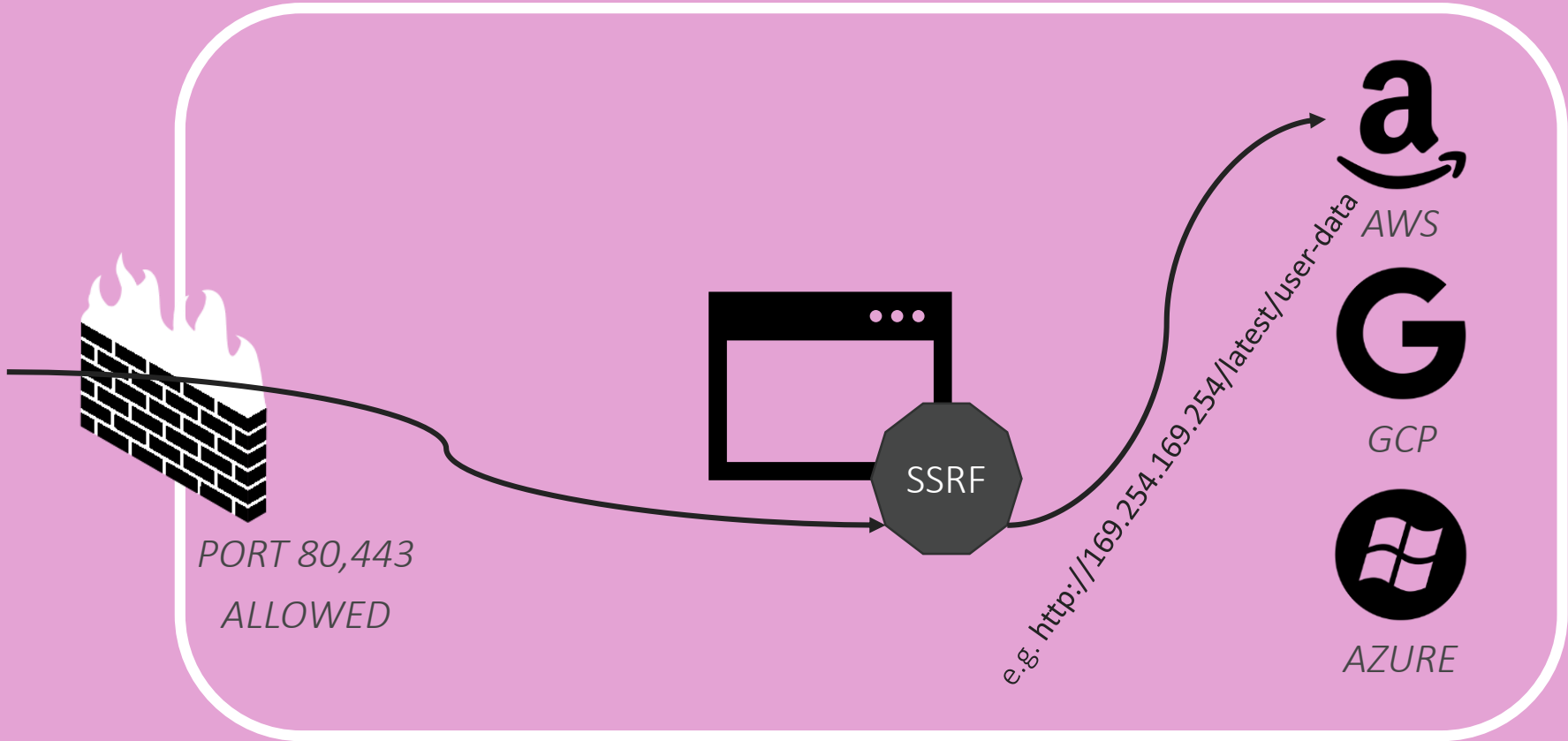
*AWS*



*GCP*



*AZURE*



## Examples:

### AWS

`http://169.254.169.254/latest/user-data`  
`http://169.254.169.254/latest/user-data/iam/security-credentials/[ROLE NAME]`  
`http://169.254.169.254/latest/meta-data/iam/security-credentials/[ROLE NAME]`  
`http://169.254.169.254/latest/meta-data/ami-id`  
`http://169.254.169.254/latest/meta-data/reservation-id`  
`http://169.254.169.254/latest/meta-data/hostname`  
`http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key`  
`http://169.254.169.254/latest/meta-data/public-keys/[ID]/openssh-key`

### GCP

Requires the header "Metadata-Flavor: Google" or "X-Google-Metadata-Request: True"

`http://169.254.169.254/computeMetadata/v1/`  
`http://metadata.google.internal/computeMetadata/v1/`  
`http://metadata/computeMetadata/v1/`  
`http://metadata.google.internal/computeMetadata/v1/instance/hostname`  
`http://metadata.google.internal/computeMetadata/v1/instance/id`  
`http://metadata.google.internal/computeMetadata/v1/project/project-id`

### Digital Ocean

`http://169.254.169.254/metadata/v1.json`  
`http://169.254.169.254/metadata/v1/`  
`http://169.254.169.254/metadata/v1/id`  
`http://169.254.169.254/metadata/v1/user-data`  
`http://169.254.169.254/metadata/v1/hostname`  
`http://169.254.169.254/metadata/v1/region`  
`http://169.254.169.254/metadata/v1/interfaces/public/0/ipv6/address`

### Oracle Cloud

`http://192.0.0.192/latest/`  
`http://192.0.0.192/latest/user-data/`  
`http://192.0.0.192/latest/meta-data/`  
`http://192.0.0.192/latest/attributes/`

Src: <https://gist.github.com/jhaddix/78cece26c91c6263653f31ba453e273b>

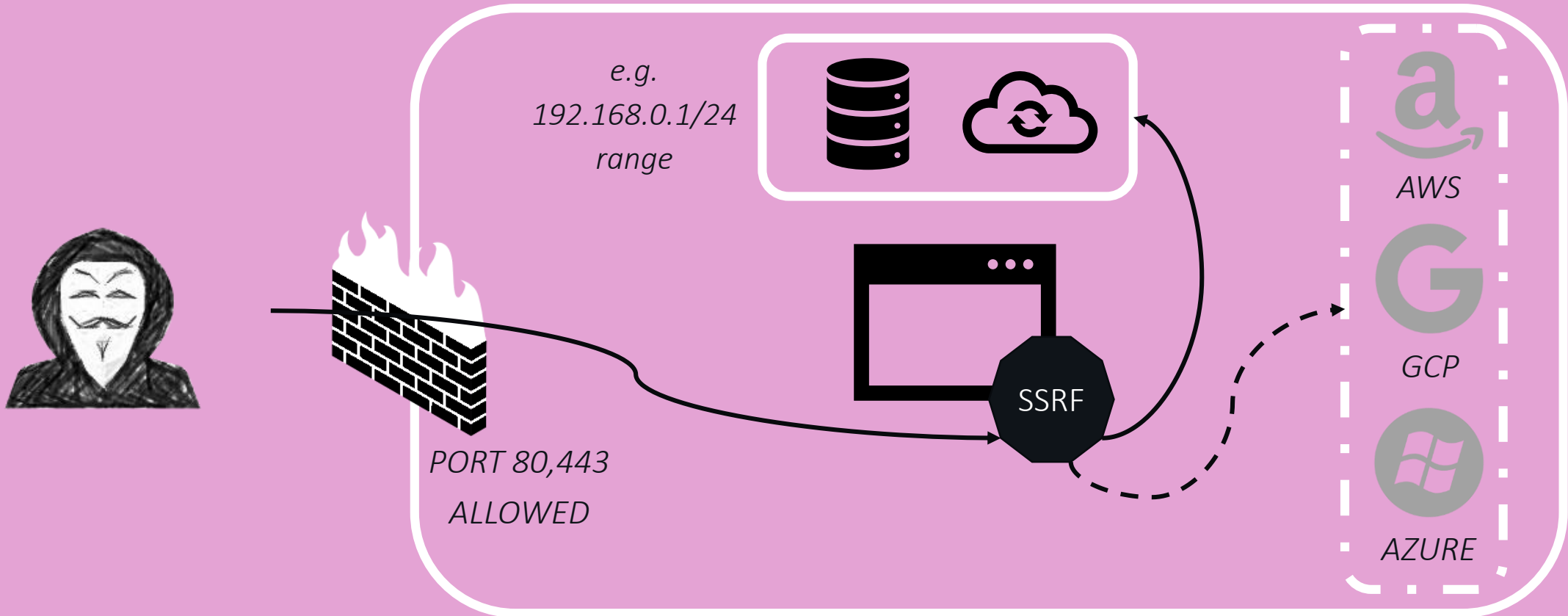
Demo



# What I Need You To Do

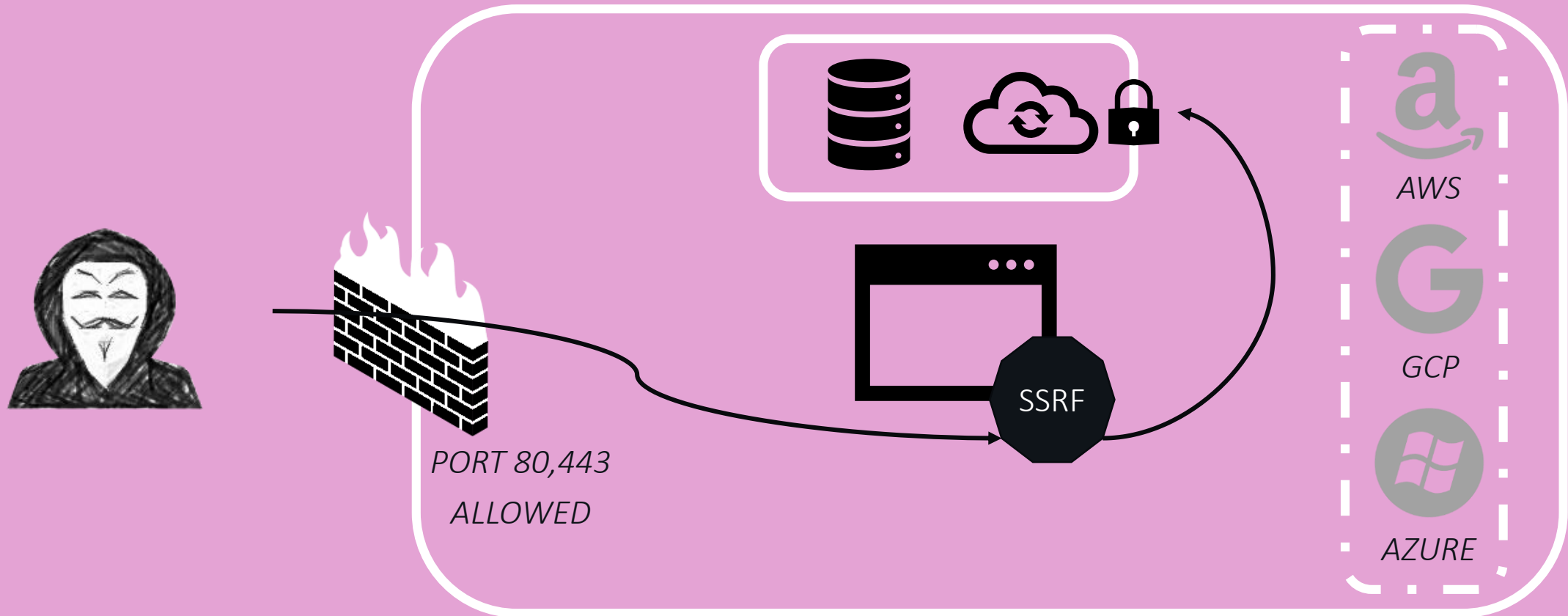


## Whitelist IP Ranges / DNS Names

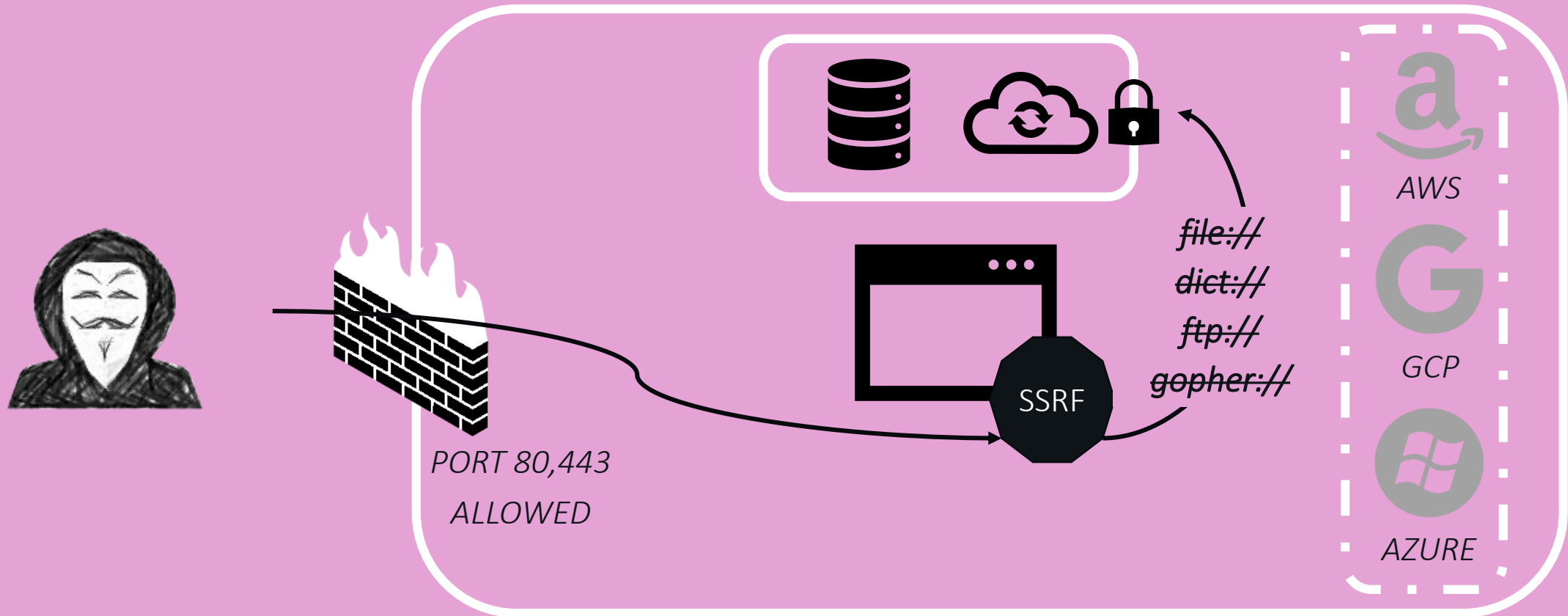




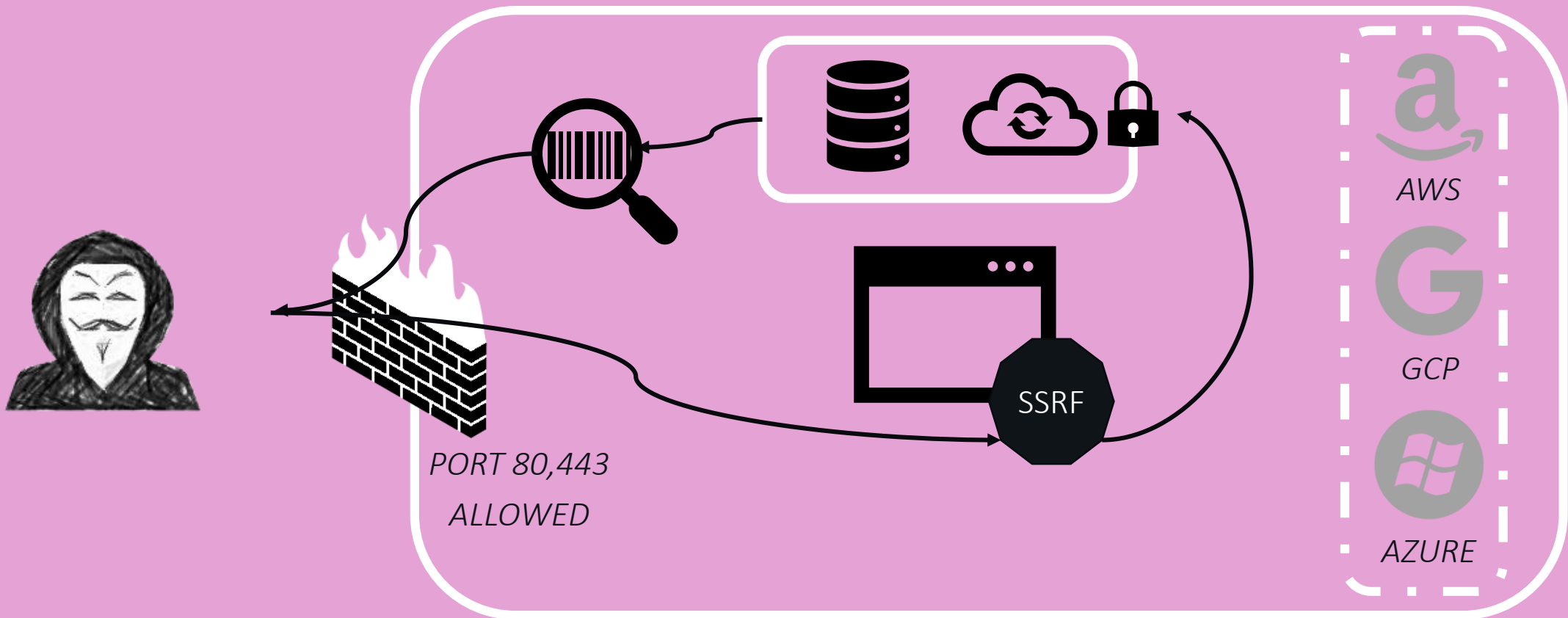
## Use Authentication Also for Internal Services



## Disable Unnecessary URL Schemes

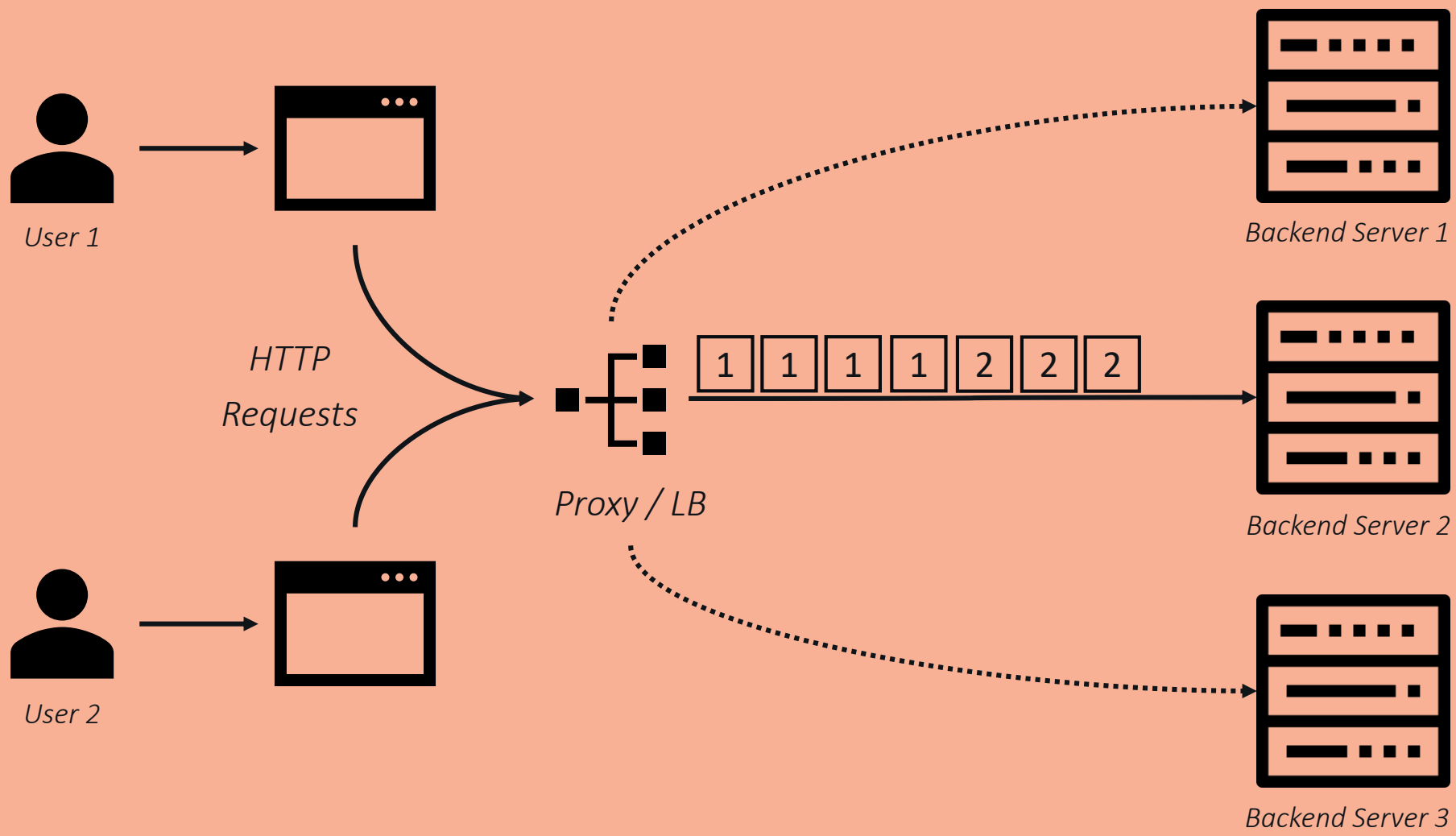


## Monitor Response Sent Back to the User



# HTTP Desync Attacks

---





User 1



HTTP  
Requests



User 2





User 1



HTTP  
Requests



User 2





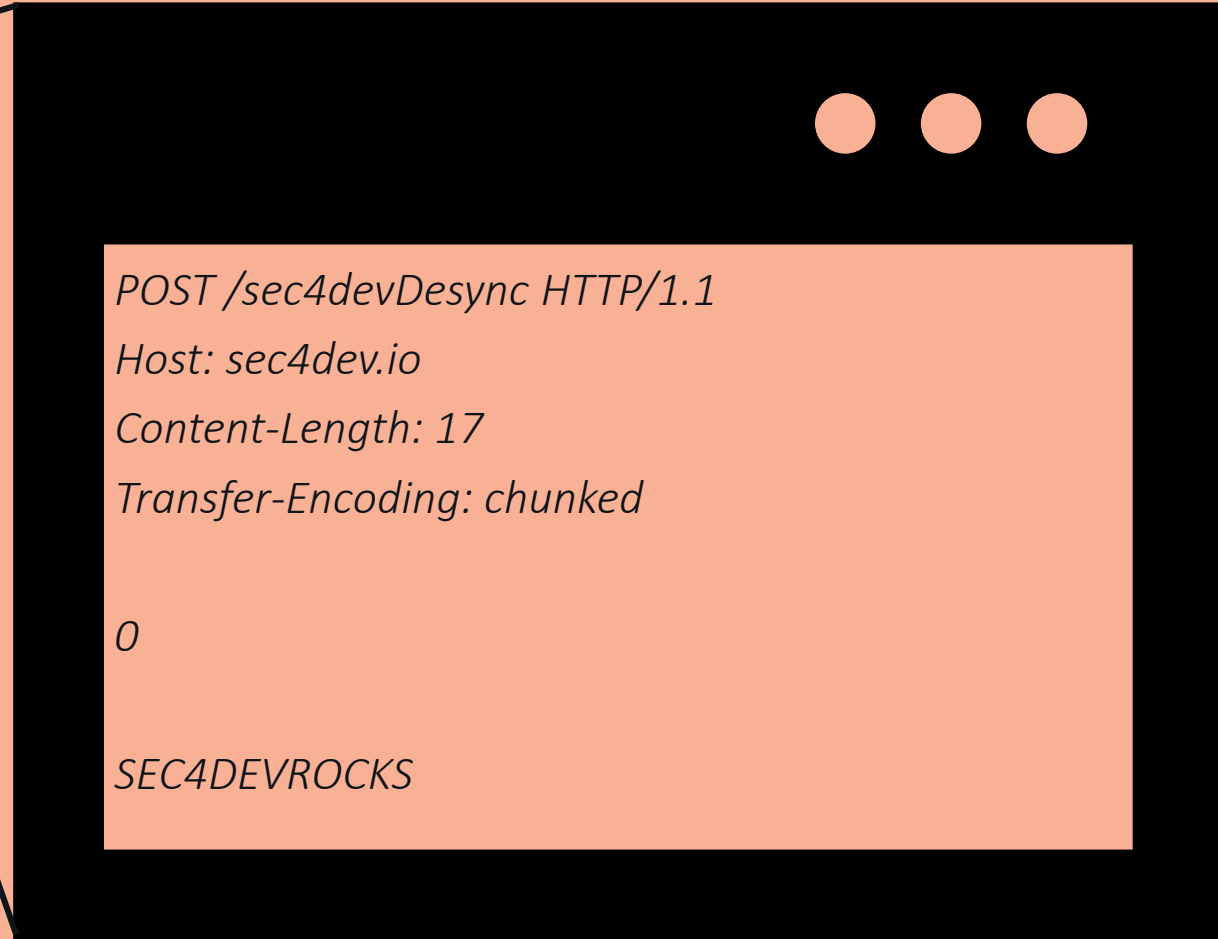
User 1



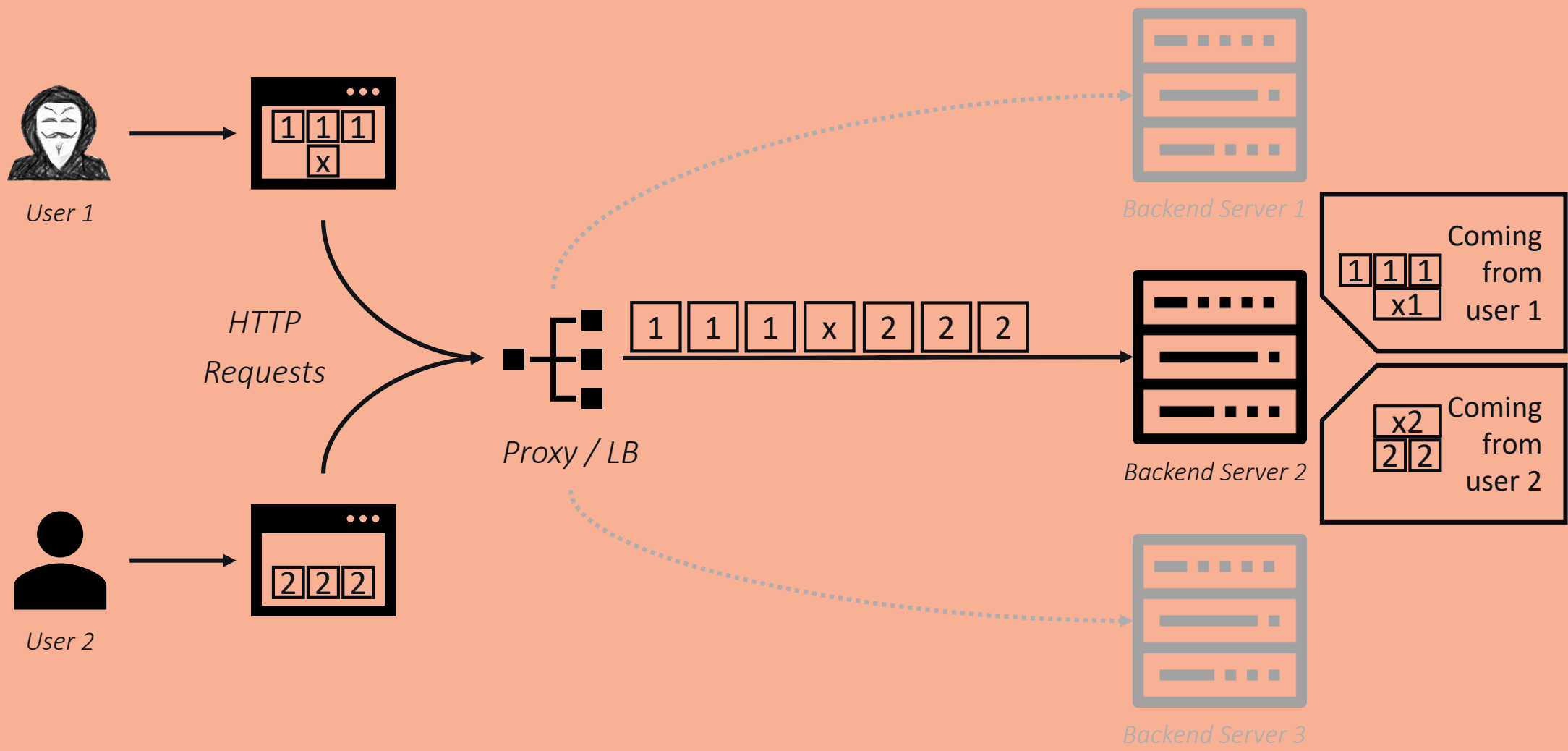
HTTP  
Requests



User 2







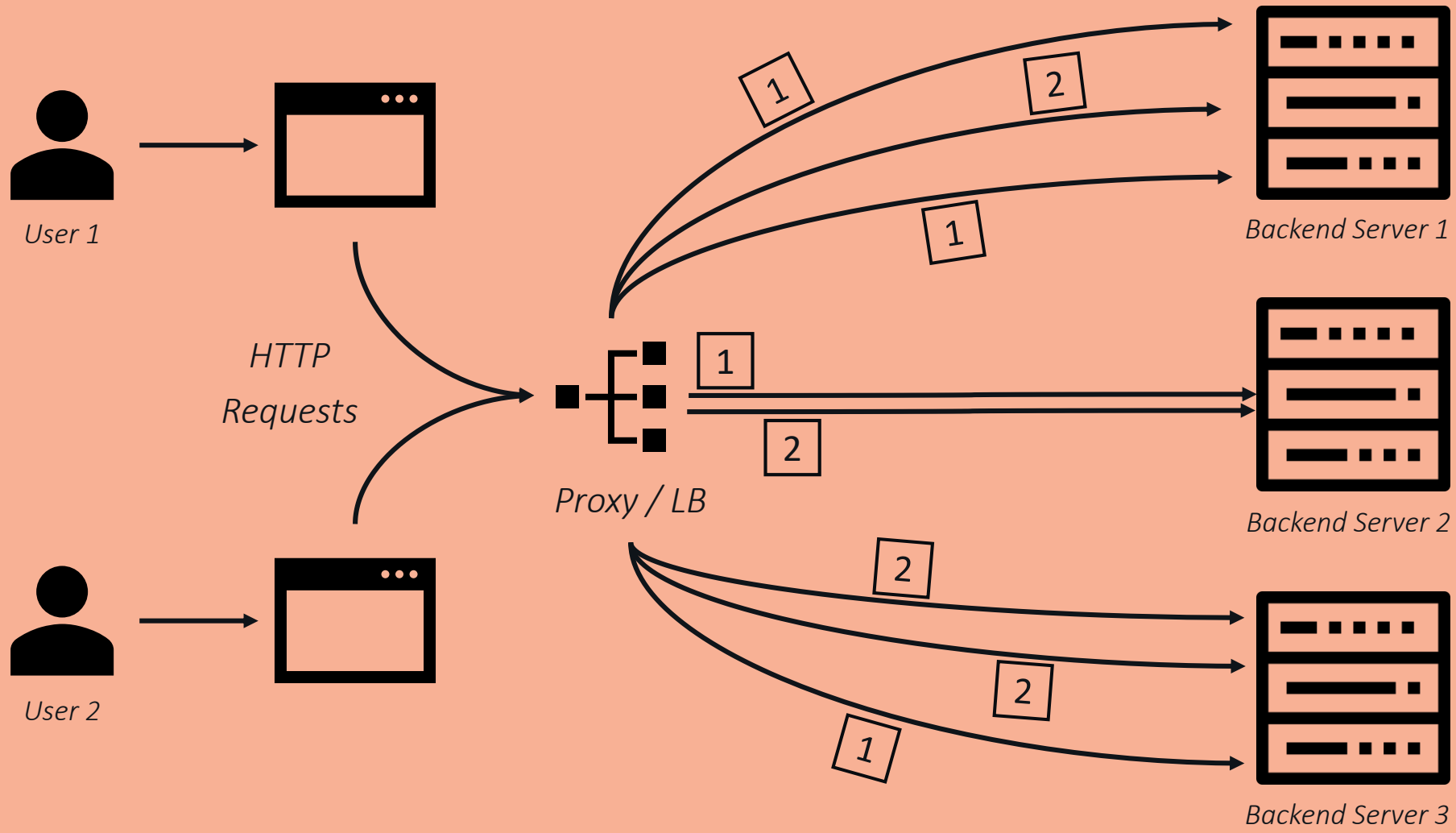
Demo



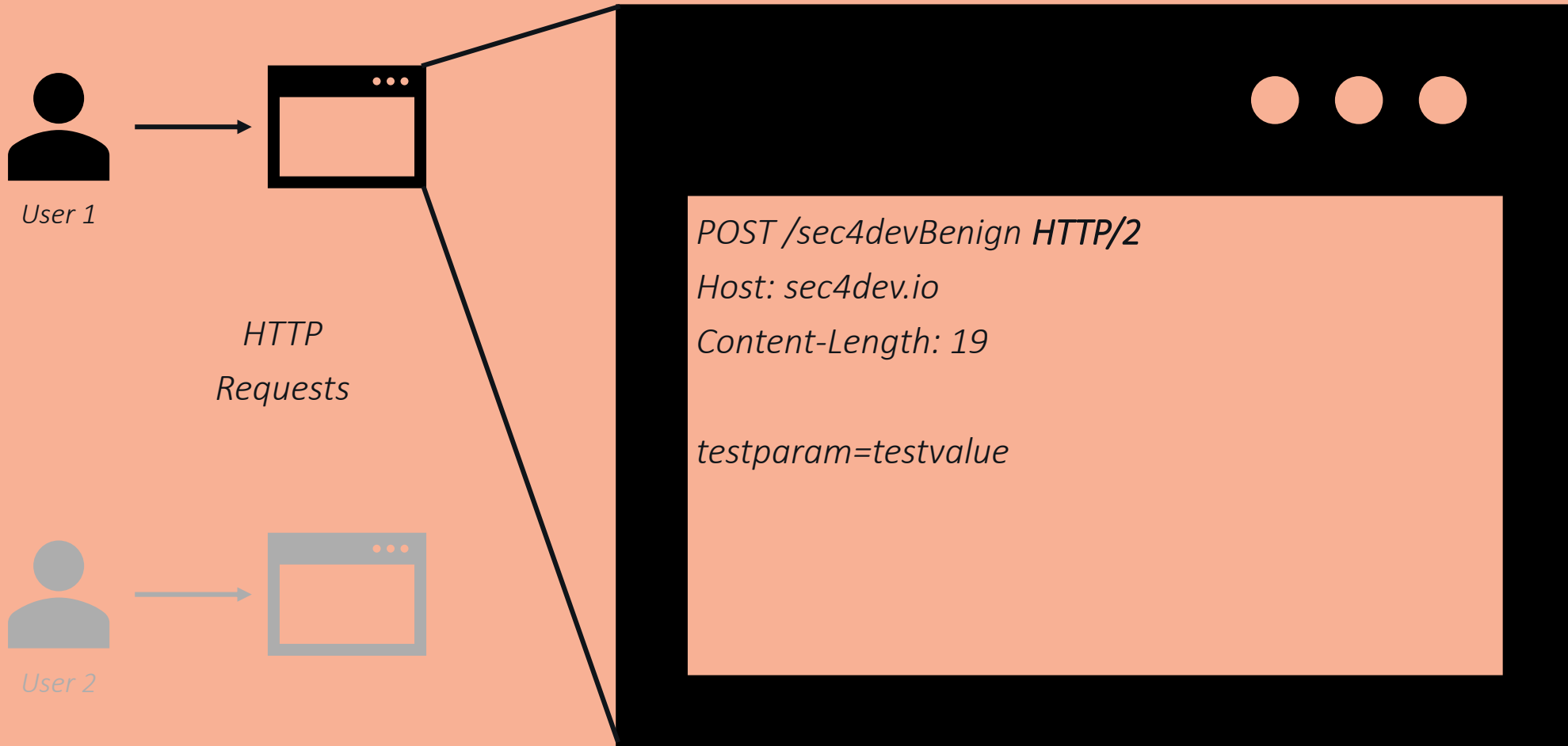
# What I Need You To Do



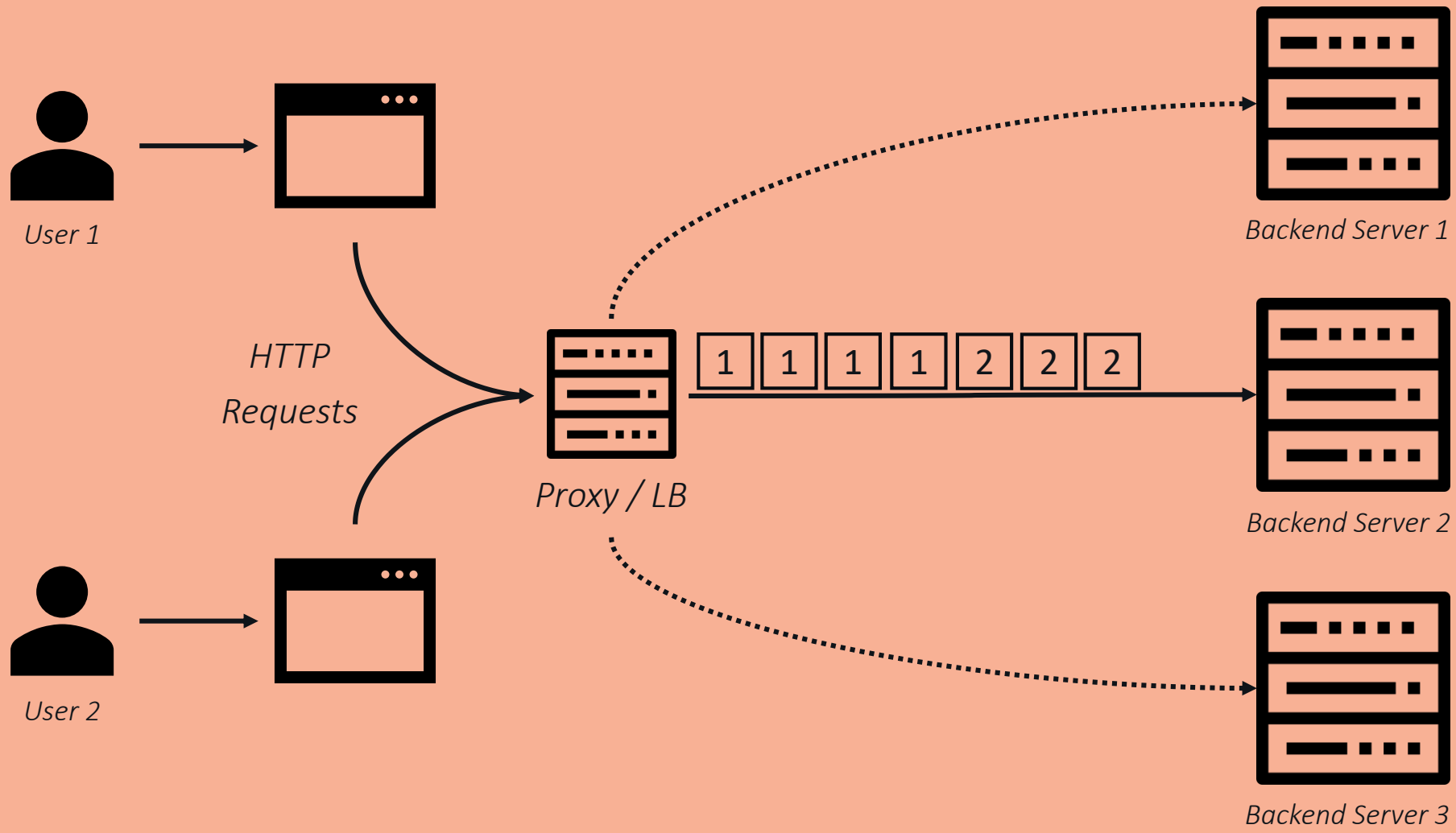
## Use Separate Network Connections For Each Request



## Use HTTP/2 For Backend Connections



## Use Exact Same Software for Frontend / Backend



# Public Secrets Disclosure

---





shhgit live! v0.3

51 matches 0 filters

High entropy string 20

Google OAuth Key 8

Django configuration file 7

Environment configuration 5

Google Cloud API Key 3

Log file 2

Potential private key (.pem) 1

NPM configuration file 1

PHP configuration file 1

SQLite3 database file 1

Shell configuration file (.ba) 1

Potential private key (.pfx) 1

1Password password man...

Amazon MWS Auth Token

Apache htpasswd file

Apple Keychain database file

Artifactory

AWS Access Key ID

AWS Access Key ID Value

AWS Account ID

AWS CLI credentials file

AWS Secret Access Key

AWS Session Token

Azure service configuratio...

Carrierwave configuration ...

Chef Knife configuration file

☒ Interesting file extensions ☒ High entropy strings ☐ Notify on match

@darkp0rt blog

Read the corresponding [blog post](#) that inspired this tool.

Found	Signature Name	Matches	File	★
7:20:11 PM	Potential private key (.pfx)	—	/prime-dotnet-webapi-tests/Utils/Auth/prime-api-test.pfx	7
7:19:46 PM	Google OAuth Key	422156404885-9qilmhj7eium3943mh54f96svu781dm6.apps.googleusercontent.com	/src/config/config.js	0
7:19:45 PM	Google OAuth Key	422156404885-9qilmhj7eium3943mh54f96svu781dm6.apps.googleusercontent.com	/src/components/navigation/Header.js	0
7:19:45 PM	Google OAuth Key	422156404885-9qilmhj7eium3943mh54f96svu781dm6.apps.googleusercontent.com	/src/components/modals/SessionModal.js	0
7:19:43 PM	Google OAuth Key	422156404885-9qilmhj7eium3943mh54f96svu781dm6.apps.googleusercontent.com	/Dockerfile	0
7:18:58 PM	Environment configuration file	—	./env	0
7:18:48 PM	Google OAuth Key	639403125587-ue3c18da1qidqehs1n1p5rjvgn15f7qu.apps.googleusercontent.com	/python/neuroglancer/default_credentials_manager.py	468
7:18:29 PM	High entropy string	JSON.stringify('639403125587-4k5hgdfumtrvur8v48e3pr7oo91d765k.apps.googleusercontent.com'),	/config/webpack_helpers.js	468
7:18:29 PM	Google OAuth Key	639403125587-4k5hgdfumtrvur8v48e3pr7oo91d765k.apps.googleusercontent.com	/config/webpack_helpers.js	468
7:18:19 PM	High entropy string	16 verbose cwd d:\CLOUD_SANDBOX\GORILLA_TEST\timeoff-management-application	/npm-debug.log	0
7:18:19 PM	Log file	—	/npm-debug.log	0
7:16:25 PM	High entropy string	SECRET_KEY = 'ilb^go0t#1%4\$fk9tu\$@46k*g*m6#b())j_ung-drlkeryfz6e'	/superlists/settings.py	-1
7:16:25 PM	Django configuration file	—	/superlists/settings.py	-1
7:15:20 PM	Shell configuration file (.bashrc, .zshrc, .cshrc)	—	/windows/bashrc	0
7:15:10 PM	High entropy string	integrity sha1-3F5pjL0Hkmw8c+A3doGk50g/YW4=	/yarn-error.log	0
7:15:10 PM	High entropy string	integrity sha1-fSKbH8xjfkZsoIEYCDanqr/4P0M=	/yarn-error.log	0
7:15:10 PM	High entropy string	integrity sha1-bVuTSkVpk7I9N/QKOC1vFmao5cY=	/yarn-error.log	0
7:15:10 PM	High entropy string	integrity sha1-YrEQ4omkcUGOPsNqYX1HLjAd/Ik=	/yarn-error.log	0
7:15:10 PM	High entropy string	integrity sha1-GLK82lhbHFxR3vJHkw7SmgvmsXc=	/yarn-error.log	0

# What I Need You To Do

---

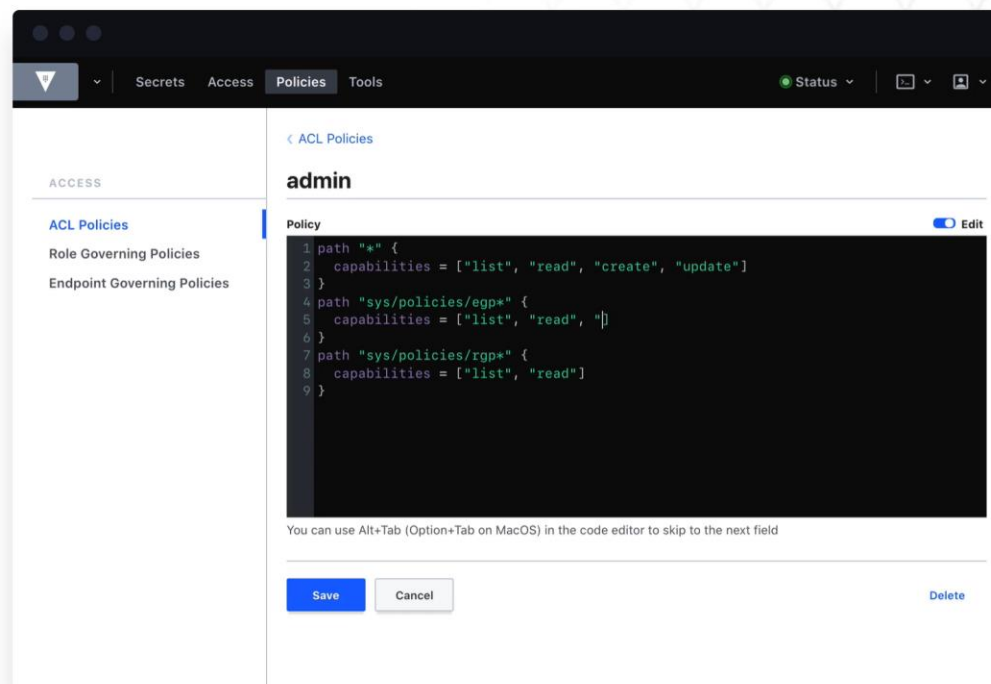
Build Awareness  
Enable Employees

Use Secrets Vault /  
Manager

[Overview](#)[Use Cases](#) ▾[Enterprise](#)[Whitepaper](#)[Learn](#)[Docs](#)[API](#)[Community](#)[Download](#)

# Manage Secrets and Protect Sensitive Data

Secure, store and tightly control access to tokens, passwords, certificates, encryption keys for protecting secrets and other sensitive data using a UI, CLI, or HTTP API.

[Download](#)[Get Started with Vault](#)

UI

CLI

# AWS Secrets Manager

Easily rotate, manage, and retrieve database credentials, API keys, and other secrets through their lifecycle

[Get started with AWS Secrets Manager](#)

AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text. Secrets Manager offers secret rotation with built-in integration for Amazon RDS, Amazon Redshift, and Amazon DocumentDB. Also, the service is extensible to other types of secrets, including API keys and OAuth tokens. In addition, Secrets Manager enables you to control access to secrets using fine-grained permissions and audit secret rotation centrally for resources in the AWS Cloud, third-party services, and on-premises.

## Benefits

### Rotate secrets safely

AWS Secrets Manager helps you meet your security and compliance requirements by

### Manage access with fine-grained policies

With Secrets Manager, you can manage access to secrets using fine-grained AWS Identity

pre-commit hooks

# git-secrets

---

Prevents you from committing passwords and other sensitive information to a git repository.

---

## Contents

- [Synopsis](#)
- [Description](#)
- [Installing git-secrets](#)
  - [\\*nix \(Linux/macOS\)](#)
  - [Windows](#)
  - [Homebrew \(for macOS users\)](#)
- [Advanced configuration](#)
- [Before making public a repository](#)
- [Options](#)
  - [Operation Modes](#)
  - [Options for `--install`](#)
  - [Options for `--scan`](#)
  - [Options for `--list`](#)
  - [Options for `--add`](#)
  - [Options for `--register-aws`](#)
  - [Options for `--aws-provider`](#)
  - [Options for `--add-provider`](#)
- [Defining prohibited patterns](#)
- [Ignoring false positives](#)
- [Secret providers](#)
- [Example walkthrough](#)



# Github Token Scanning Service

## About token scanning

GitHub scans public repositories for known token formats, to prevent fraudulent use of credentials that were committed accidentally.

When you push commits to a public repository, or switch a private repository to public, GitHub scans the contents of the commits or repository for tokens issued by the following service providers:

- Alibaba Cloud
- Amazon Web Services (AWS)
- Atlassian
- Azure
- CloudBees CodeShip
- Discord
- Dropbox
- GitHub
- GoCardless
- Google Cloud
- Hashicorp Terraform
- Mailgun
- npm
- Postman
- Proctorio
- Pulumi
- Slack

## Valuable Sources (Subdomain Takeover)

- <https://0xpatrik.com/subdomain-takeover-basics/>
- <https://www.hackerone.com/blog/Guide-Subdomain-Takeovers>
- <https://help.github.com/en/github/working-with-github-pages>
- <https://0xpatrik.com/takeover-proofs/>
- <https://github.com/EdOverflow/can-i-take-over-xyz>

## Valuable Sources (Metadata SSRF)

- <https://www.acunetix.com/blog/articles/server-side-request-forgery-vulnerability/>
- <https://gist.github.com/jhaddix/78cece26c91c6263653f31ba453e273b>
- <https://aws.amazon.com/blogs/security/defense-in-depth-open-firewalls-reverse-proxies-ssrf-vulnerabilities-ec2-instance-metadata-service/>
- <https://portswigger.net/web-security/xxe/lab-exploiting-xxe-to-perform-ssrf>
- <https://portswigger.net/web-security/ssrf>

## Valuable Sources (HTTP Desync Attacks)

- <https://portswigger.net/web-security/request-smuggling>
- <https://portswigger.net/research/http-desync-attacks-request-smuggling-reborn>

## Valuable Sources (Public Secrets Disclosure)

- <https://shhgit.darkport.co.uk/>
- <https://www.vaultproject.io/>
- <https://aws.amazon.com/secrets-manager/>
- <https://github.com/awslabs/git-secrets>



- Any questions / feedback?
- Please contact me via PM to <https://twitter.com/PascalSec>



- Any questions / feedback?
- Please contact me via DM to <https://twitter.com/PascalSec>

- WE ARE HIRING

[https://jobs.lever.co/dynatrace?lever-via=qMV\\_Evjulm](https://jobs.lever.co/dynatrace?lever-via=qMV_Evjulm)