# Offensive API security

Dr. Philippe De Ryck

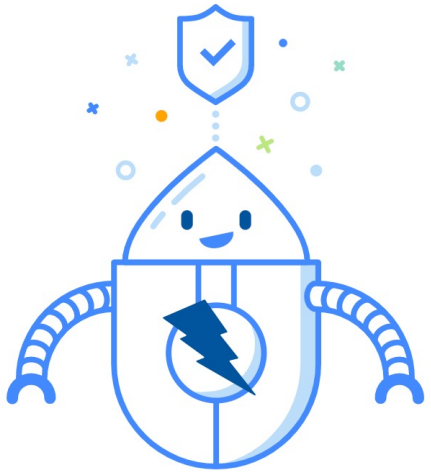
https://Pragmatic Web Security.com

| | |
|---|---|
| 1 | Broken object level authorization |
| 2 | Broken user authentication |
| 3 | Excessive data exposure |
| 4 | Lack of resources & rate limiting |
| 5 | Broken function level authorization |
| 6 | Mass assignment |
| 7 | Security misconfiguration |
| 8 | Injection |
| 9 | Improper assets management |
| 10 | Insufficient logging & monitoring |

# OWASP® Zed Attack Proxy (ZAP)

**The world's most widely used web app scanner. Free and open source. Actively maintained by a dedicated international team of volunteers.**

Quick Start Guide | Download Now



# Burp Suite is the choice of security professionals worldwide

Join the community of over 15,000 organizations using Burp Suite to secure the web and speed up software delivery.

# Introducing Restograde and Burp

# I am *Dr. Philippe De Ryck*

Pragmatic Web Security
Security for developers

**Founder of Pragmatic Web Security**

Google Developers Experts

**Google Developer Expert**

AMBASSADOR PROGRAM

**Auth0 Ambassador**

Secure Application Development

**SecAppDev organizer**

# I help developers with security

- **Hands-on in-depth security training**
- **Advanced online security courses**
- **Security advisory services**

https://pragmaticwebsecurity.com

Business

# Mobile Health Apps Systematically Expose PII and PHI Through APIs, New Findings from Knight Ink and Approov Show

9 February 2021, 12:00 CET

*https://www.bloomberg.com/press-releases/2021-02-09/mobile-health-apps-systematically-expose-pii-and-phi-through-apis-new-findings-from-knight-ink-and-approov-show*

> **Of the 30 popular apps Knight Ink tested, 77 percent contained hardcoded API keys, some which don't expire, and seven percent contained hardcoded usernames and passwords.**

BLOG: VULNERABILITY ADVISORY

# Free BrewDog beer with a side order of shareholder PII?



*https://www.pentestpartners.com/security-blog/free-brewdog-beer-with-a-side-order-of-shareholder-pii/*

"Every mobile app user was given the same hard coded API Bearer Token, rendering request authorisation useless"

# Extracting secrets from the client

# KeyHacks

KeyHacks shows ways in which particular API keys found on a Bug Bounty Program can be used, to check if they are valid.

@Gwen001 has scripted the entire process available here and it can be found here

## Table of Contents



# Key-Checker

## Go scripts for checking API key / access token validity


## Update V1.0.0 🚀

- Added 37 checkers!

## Screenshoot 📷

# Analyze client applications for secrets

*Many clients contain hardcoded secrets, even though it is trivial to extract and abuse such secrets*

# Reverse Engineering Bumble's API

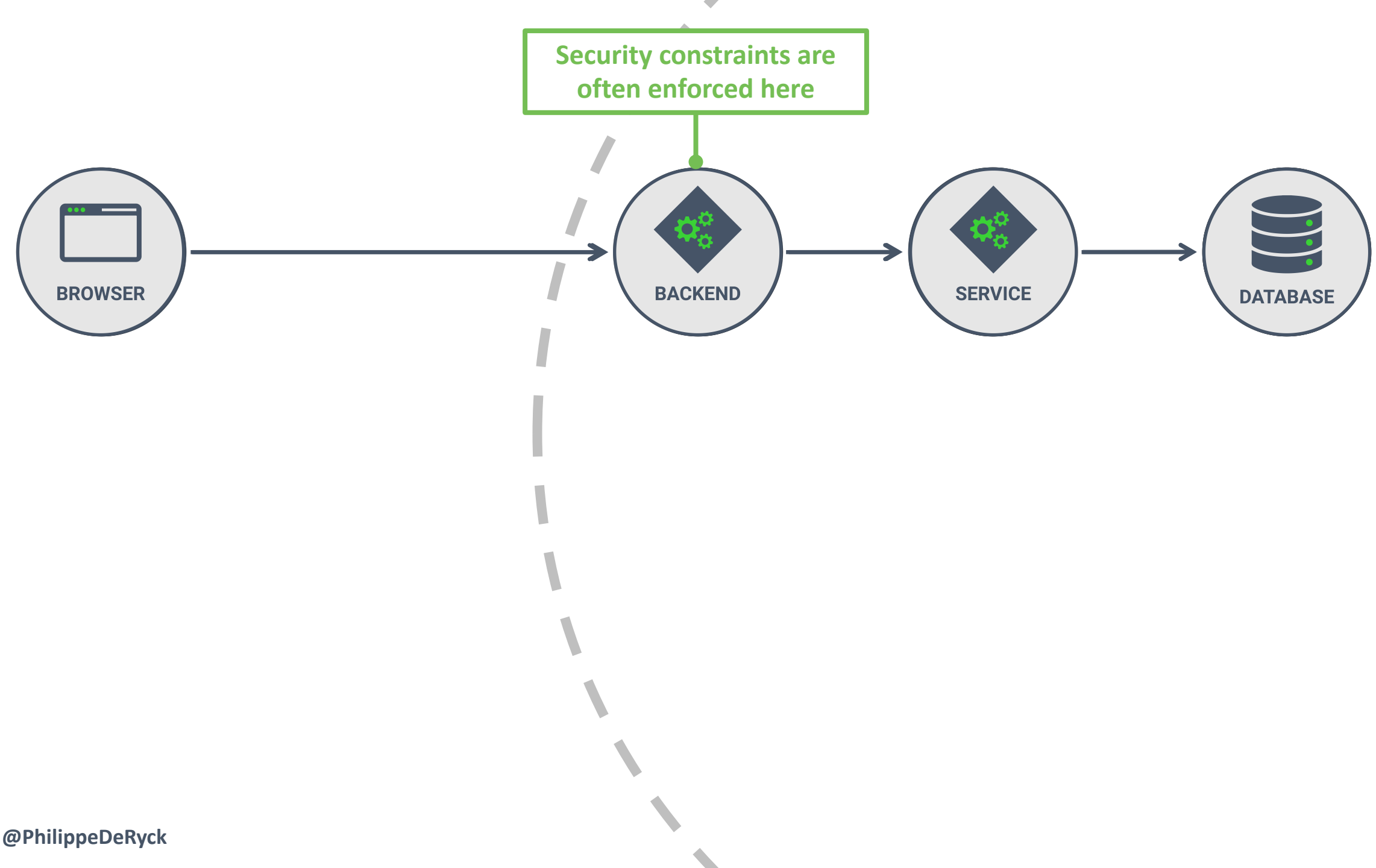
When you have too much time on your hands and want to dump out Bumble's entire user base and bypass paying for premium Bumble Boost features.

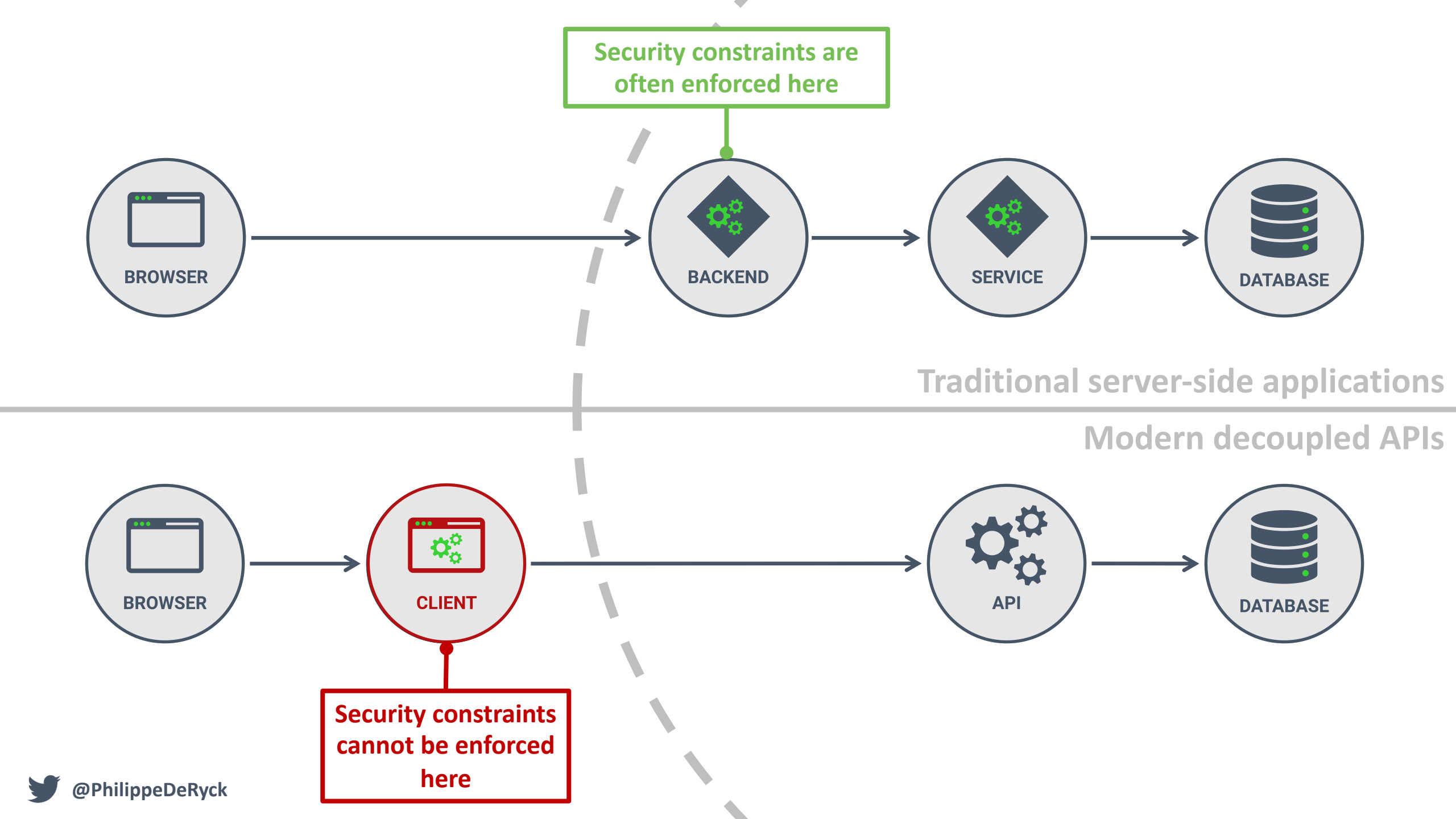
Sanjana Sarda Follow

Nov 14 · 8 min read

> **Our accounts eventually got locked and hidden for more verification requirements. We tested retrieving user data while our account was locked, and it still worked.**

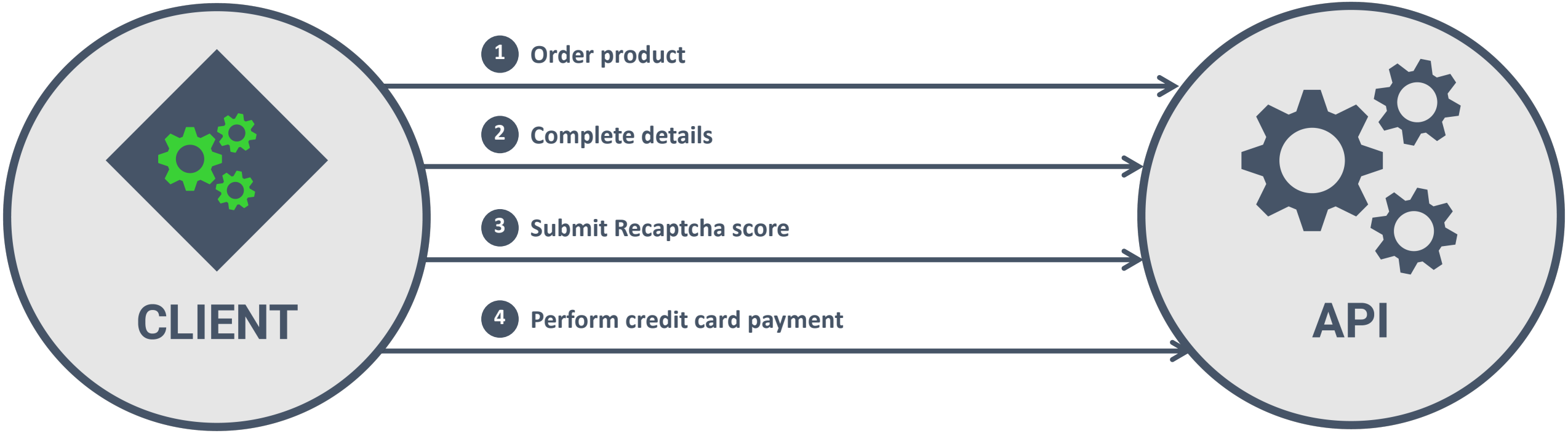
*https://blog.securityevaluators.com/reverse-engineering-bumbles-api-a2a0d39b3a87*

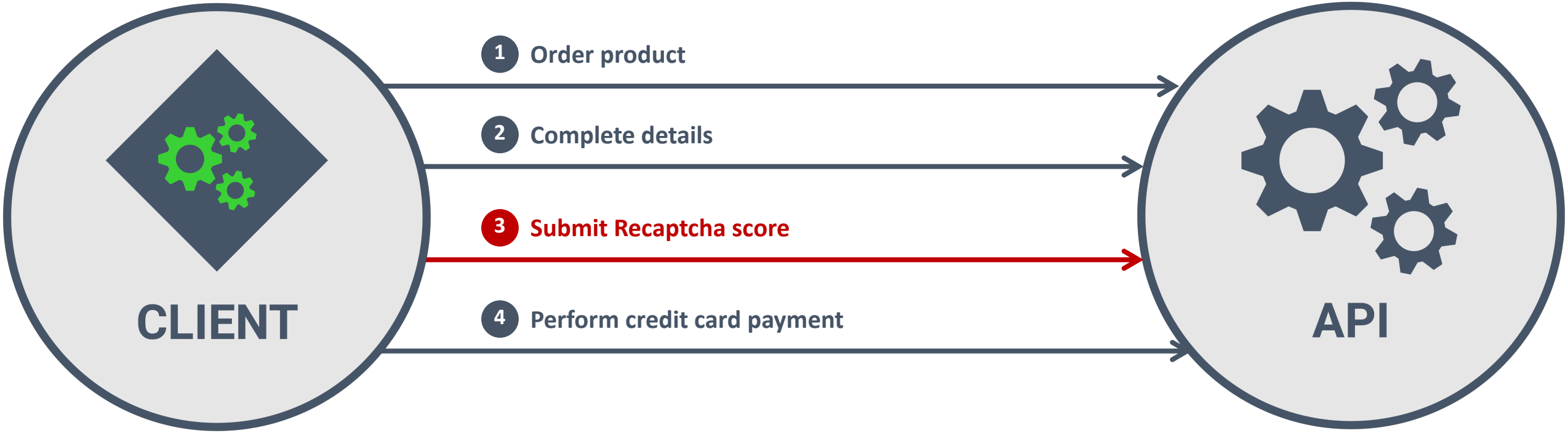

Security constraints are often enforced here
BROWSER
BACKEND
SERVICE
DATABASE

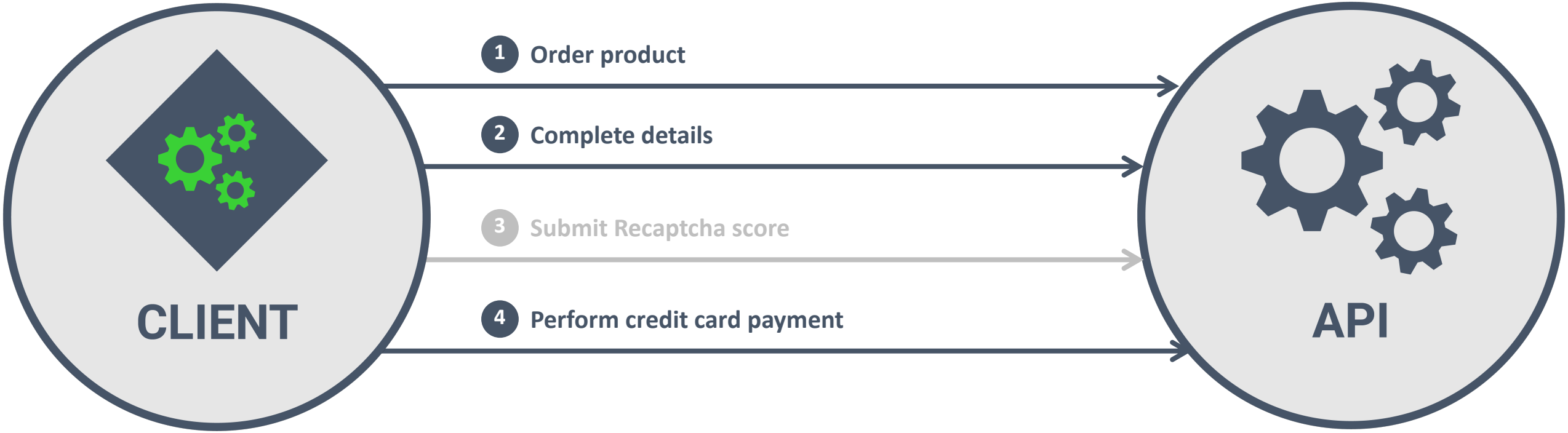



@PhilippeDeRyck

# Bypassing client restrictions


1 Order product
2 Complete details
3 Submit Recaptcha score
4 Perform credit card payment
CLIENT
API


1 Order product
2 Complete details
3 Submit Recaptcha score
4 Perform credit card payment
CLIENT
API


1 Order product
2 Complete details
3 Submit Recaptcha score
4 Perform credit card payment
CLIENT
API

# Bypass restrictions by modifying client behavior

*Clients often enforce certain restrictions, which can be bypassed by modifying the requests going to the API*

# Forget the client, focus on the API

# ILLUMINATE THE OBSCURITY

***APIs often expose sensitive features that are not used by the public client. Scan APIs directly to discover the full attack surface.***

# A security flaw in Grindr let anyone easily hijack user accounts

Zack Whittaker @zackwhittaker / 10:22 PM GMT+2 • October 2, 2020 Comment


Image Credits: SOPA Images / Getty Images

**Grindr,** one of the world's largest dating and social networking apps for gay, bi, trans, and queer people, has fixed a security vulnerability that allowed anyone to hijack and take control of any user's account using only their email address.

https://techcrunch.com/2020/10/02/grindr-account-hijack-flaw/

"

To reset a password, Grindr sends the user an email with a clickable link containing an account password reset token.

Grindr's password reset page was leaking password reset tokens to the browser.

"


*The API response to retrieve online users*

```
[
  {
    "id": 3,
    "name": "John",
    "address": "5 George's Dock, …",
  },
  {
    "id": 6,
    "name": "Jakob",
    "address": "71–75 Shelton Street, …",
  },
  {
    "id": 17,
    "name": "Philippe",
    "address": "Holsbeeksesteenweg 143, …",
  }
]
```

# Looking under the hood

# Look for data under the hood

*APIs often provide more data in the response than is used by the client. This data exposure can result in a leak or support additional attacks.*

INTERNET INSECURITY | By Lorenzo Franceschi-Bicchierai | Oct 10 2017, 8:03pm

# T-Mobile Website Allowed Hackers to Access Your Account Data With Just Your Phone Number

> he could query for someone else's phone number and the API would simply send back a response containing the other person's data.

# Extracting information

# ORS Patient Portal —Digital India initiative put at risk the leakage of millions of patients' health information

# A Twitter app bug was used to match 17 million phone numbers to user accounts

Zack Whittaker @zackwh

Marcos Ferreira

Published On: 14 Sep 2020

Change the username for any Facebook Page

IDOR

Facebook | Web

---

HIGH VALID

$15,000

@PhilippeDeRyck

https://techcrunch.com/2019/12/24/twitter-android-bug-phone-numbers/
https://bugreader.com/marcos@change-the-username-for-any-facebook-page-219
https://medium.com/@logicbomb_1/ors-patient-portal-digital-india-initiative-put-at-risk-the-leakage-of-millions-of-patients-7f093a1768e2

# Enumerate API endpoints

*API endpoints are often enumerable, even when they don't use sequential identifiers. Enumeration attacks become even more powerful in combination with BOLA vulnerabilities.*

*The Java Spring endpoint updating a user*

```
1  @RequestMapping(path = "/user/{id}", method = PATCH, consumes = "application/json")
2  public void updateUser(String id, @RequestBody User user) {
3    UserService.updateUser(id, user);
4  }
```

**Updates the DB with new field values for the user with the given ID**

*The User data class*

```
1  public class User {
2    private String id, name, role;
3    …
4    public void setName(String name) {
5      this.name = name;
6    }
7
8    public String setRole(String role) {
9      this. role = role;
10   }
11 }
```

*A legitimate request payload to update the user's name*

```
1  {
2    "name": "Dr. Phil"
3  }
```

*A malicious request payload to update restricted fields*

```
1 {
2   "name": ”Philippe becomes admin",
3   "role": "admin"
4 }
```

# "Accidentally" changing information

# Automated IDOR Discovery through Stateful Swagger Fuzzing

**Aaron Loo, Engineering Manager**
Jan 16, 2020

Scaling security coverage in a growing co
empower front-line developers to be able
they make it to production servers.

Today, we're excited to announce that we
we've developed to identify Insecure Direc
stateful Swagger fuzzing, tailored to supp
integrates with our Continuous Integration
coverage as web applications evolve.

Microsoft Research Blog

# RESTler finds security and reliability bugs through automated fuzzing

Published November 16, 2020

**Research Area**

Security, privacy, and cryptography

@PhilippeDeRyck

*https://engineeringblog.yelp.com/2020/01/automated-idor-discovery-through-stateful-swagger-fuzzing.html*
*https://www.microsoft.com/en-us/research/blog/restler-finds-security-and-reliability-bugs-through-automated-fuzzing/*

# Discover and use API data models

***Reconstructing data models from requests and responses empowers the exploitation of mass assignment vulnerabilities.***

# Apache Pulsar bug allowed account takeovers in certain configurations

Ben Dickson 02 June 2021 at 11:43 UTC
Updated: 02 June 2021 at 14:32 UTC

GitHub | Open Source Software | Secure Development

*Software maintainers downplay real-world impact of JWT vulnerability*

## Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "user": "e72d1a26f40e4e879967",
  "tenant": "d8cf3fa301a34c968502a7051bfdc0a8",
  "iat": 1620192644914,
  "exp": 1620196244914
}
```

# alg: none

# alg: none

eyJhbGciOiJub25lIiwidHlwIjoiSldUIn0
.
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4
gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ
.

**Ben Knight** Senior Security Consultant

April 16, 2020

## JSON Web Token Validation Bypass in Auth0 Authentication API

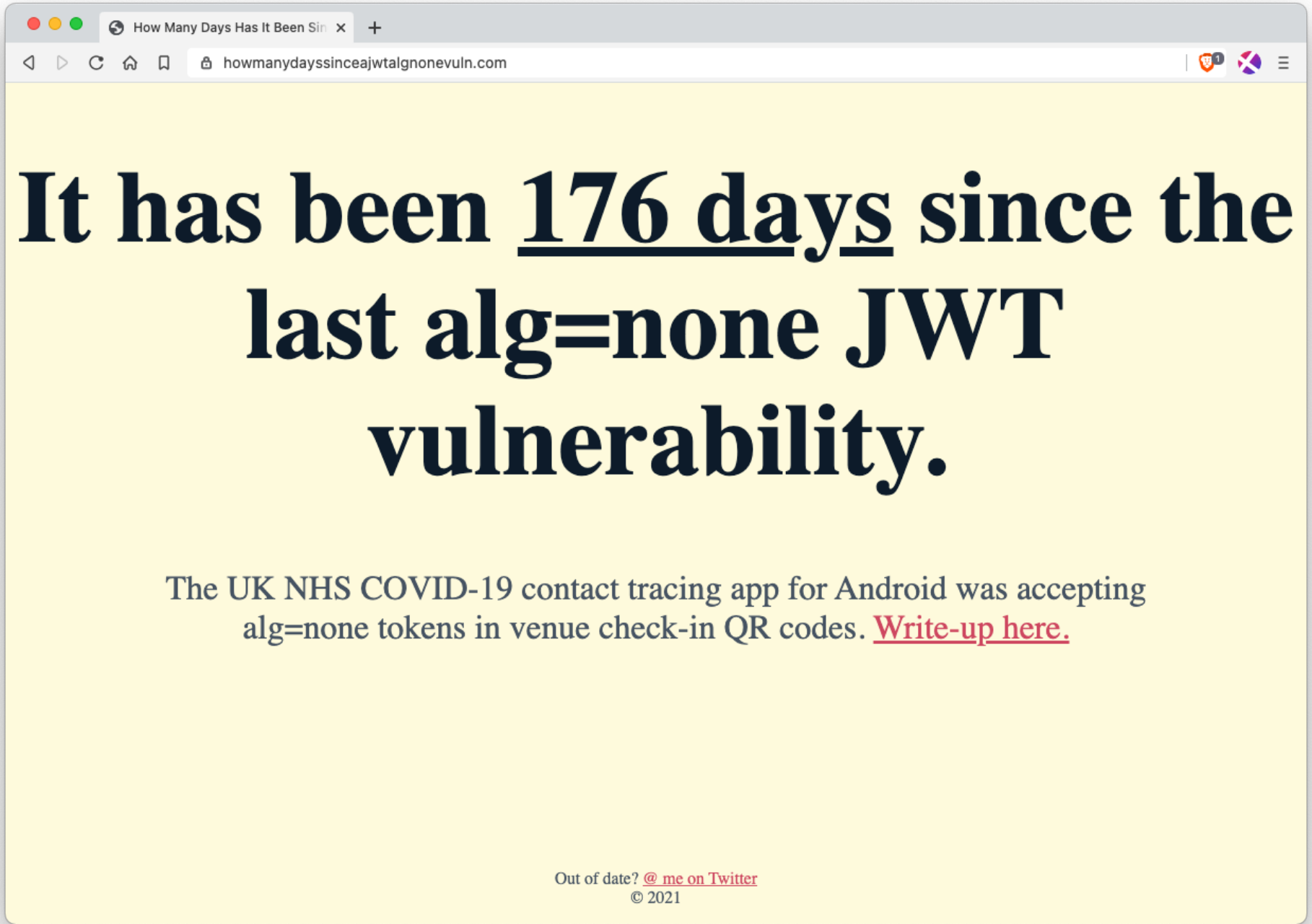
Ben discusses a JSON Web Token validation bypass issue disclosed to Auth0 in their Authentication API.

**alg: NoNe**

**alg: NONe**

**alg: nOnE**

*https://insomniasec.com/blog/auth0-jwt-validation-bypass*




*https://www.howmanydayssinceajwtalgnonevuln.com/*

# TAMPER WITH AUTHORIZATION INFORMATION

***Clients often include authorization objects, such as JWT tokens. When an API fails to properly verify this object, it often results in a high-impact privilege escalation issue.***

# Attacking your APIs ...

The attack surface is your entire API

Go off the "common path" used by the client

Don't assume the API gets it right, verify!

...

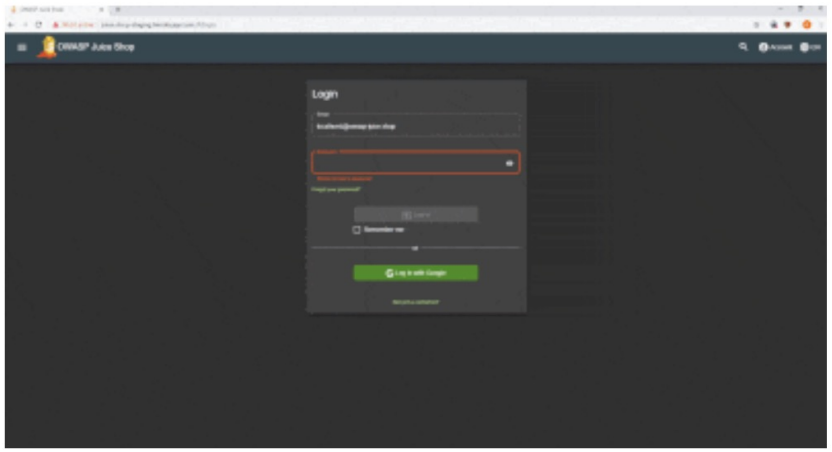
# OWASP Juice Shop

Main | Overview | News | Challenges | Learning | CTF | Ecosystem | Supporters

owasp flagship project | release v13.3.0 | GitHub ★ 6.7k | Follow 4.6k

openssf best practices gold | Contributor Covenant v2.0 adopted

OWASP Juice Shop is probably the most modern and sophisticated insecure web application! It can be used in security trainings, awareness demos, CTFs and as a guinea pig for security tools! Juice Shop encompasses vulnerabilities from the entire OWASP Top Ten along with many other security flaws found in real-world applications!



# Thank you!

Reach out for hands-on training to learn how to avoid these vulnerabilities in your APIs

@PhilippeDeRyck

/in/PhilippeDeRyck