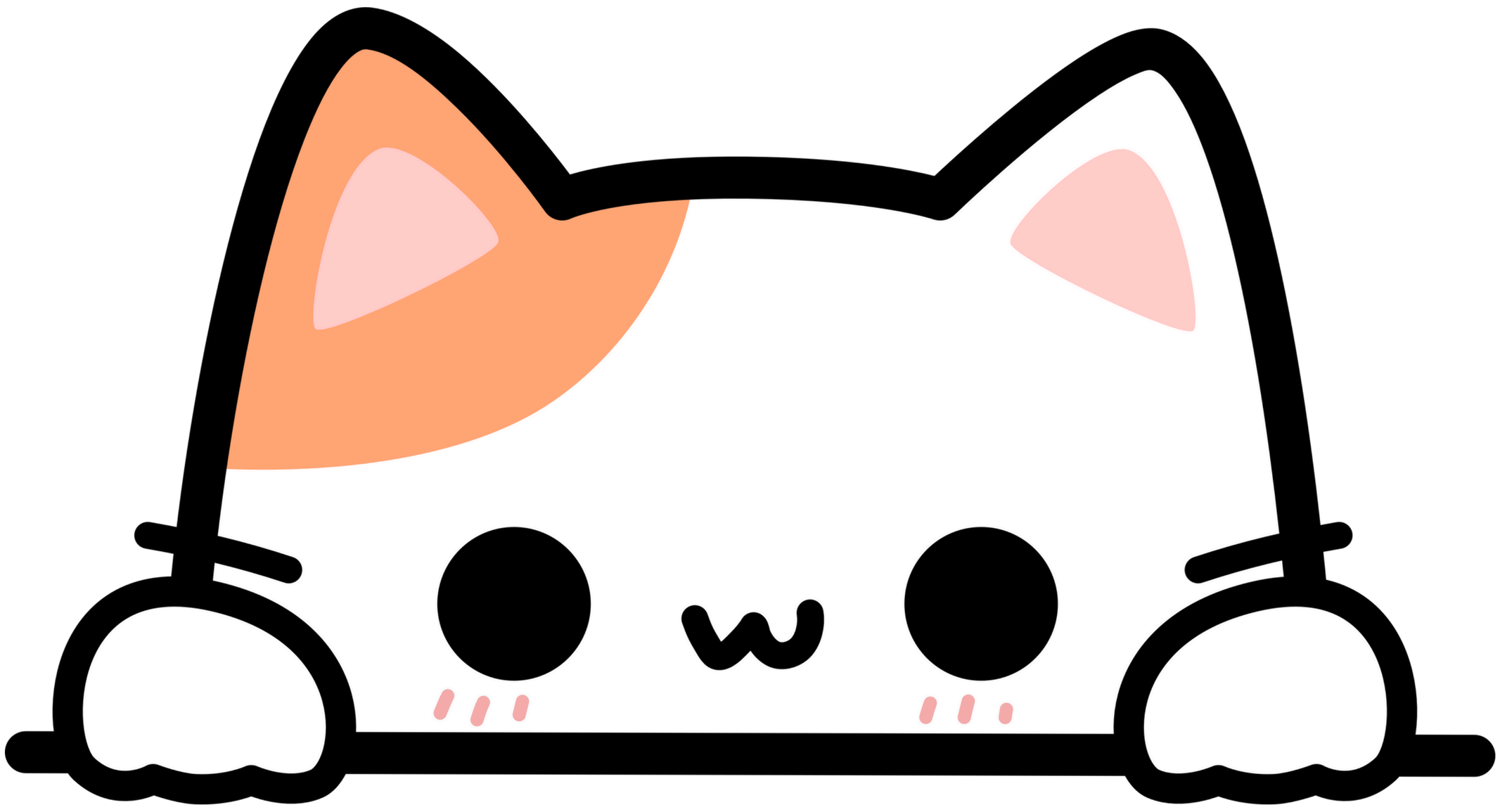
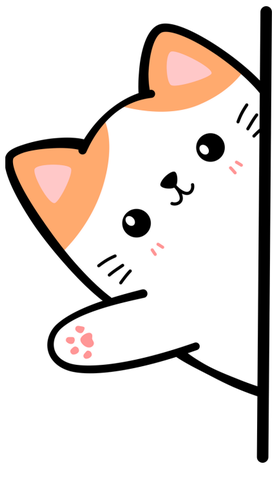
@tauseeffayyaz

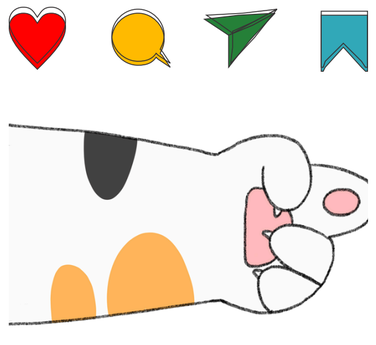


API GUIDE

TERMINOLOGIES

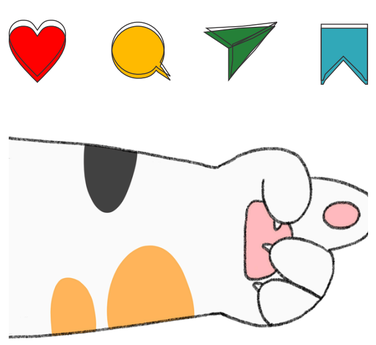


CAT EDITION

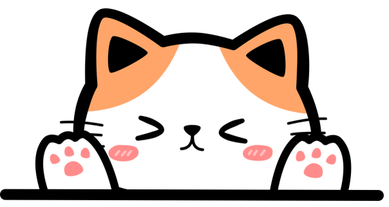


@tauseeffayyaz

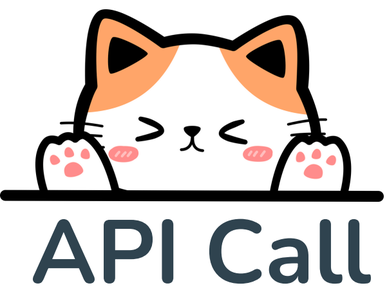
TABLE OF CONTENTS



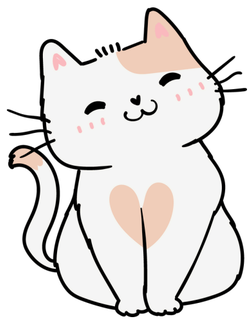
@tauseeffayyaz



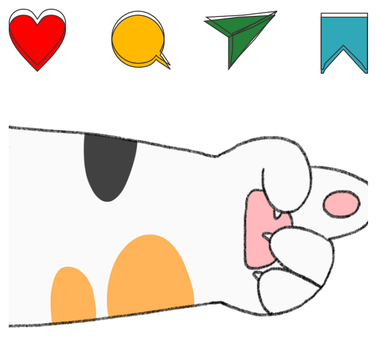
API stands for Application Programming Interface, is a set of communication protocols and routines that allow various services to communicate between them

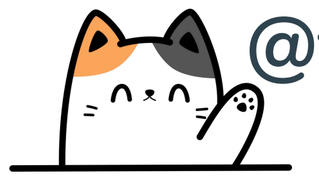


When you send a request to your API endpoint, its called an API Call. That request is processed at API end and you receive your information as feedback



When you login to a site by entering your credentials, you make an API Call





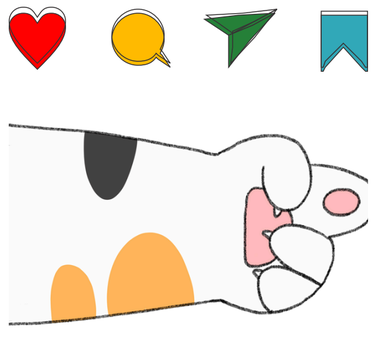
@tauseeffayyaz

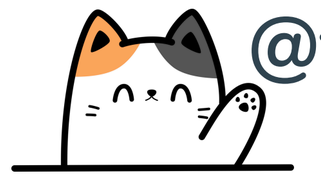
API economy describes the exchange of value between a user and a organization.

This lets businesses use APIs from other services (like social media) in their own apps.

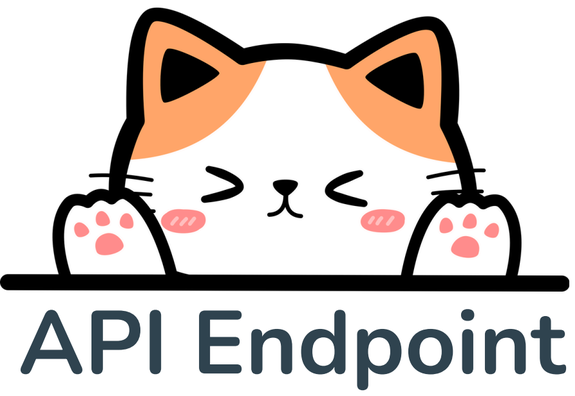
This creates a connection that allows users to benefit from a platform without needing to build the whole app themselves.

Ride sharing apps make calls to Google Maps APIs to provide location based services



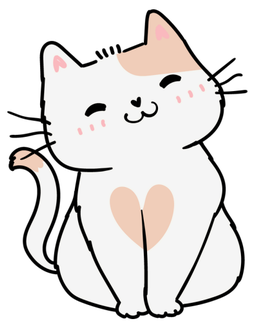


@tauseeffayyaz

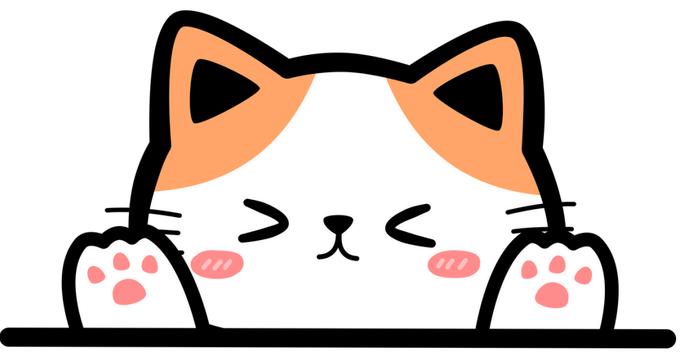


API Endpoint

An endpoint is the end of a communication channel. When APIs interact with other systems, each touchpoint of interaction is considered an endpoint.

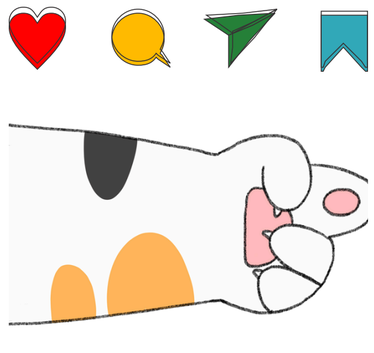


An endpoint is where resource lives such as a server, service or database

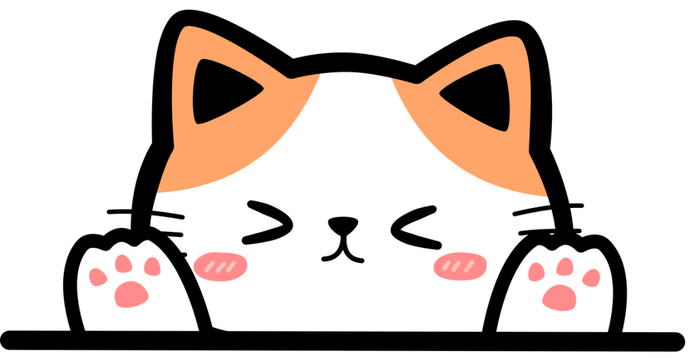


API Integration

In simple terms, API integration connects two or more applications to exchange data between them and connect to the outside world.



@tauseeffayyaz

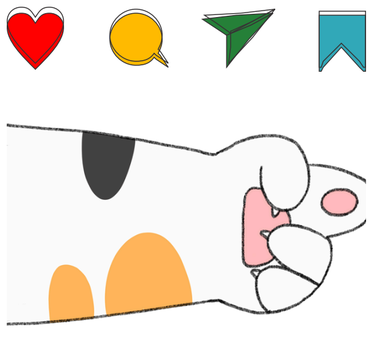


API GATEWAY

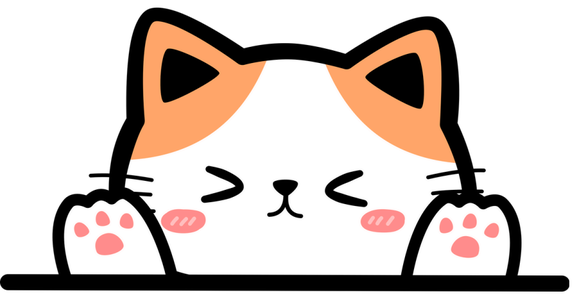
An API **management tool** that serves an **intermediate layer** between the **client** and a set of **backend** services.

It acts as **gatekeepers** and **proxies** that moderate all of your API calls, aggregate the data you need, and return the actual result.

These API Gateways are widely used to handle common tasks such as rate limiting, load balancing and usage metrics.

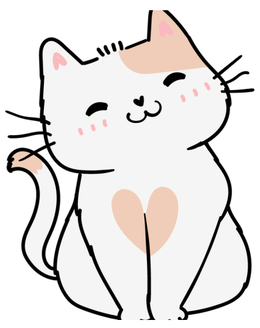


@tauseeffayyaz

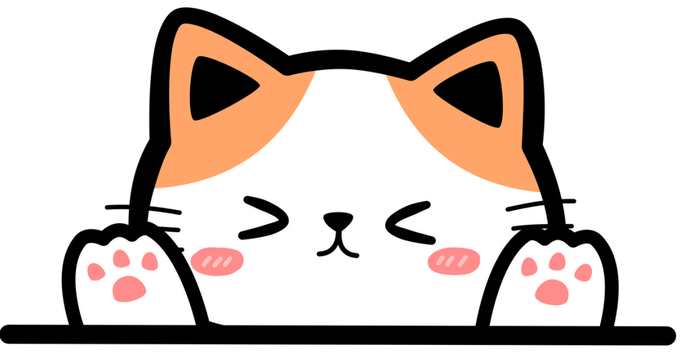


API Lifecycle

API lifecycle is an approach to the API management and development. It aims at providing a holistic view of how to manage APIs across its different stages, from creation to destruction.

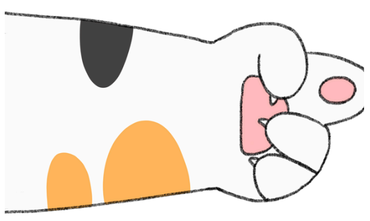


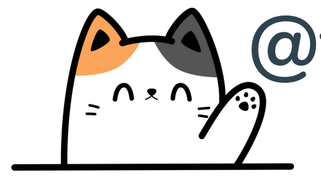
It is often divided into three stages such as creation, control and consumption



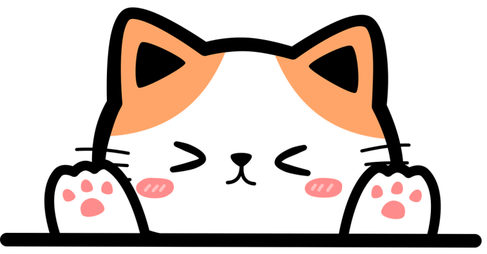
API Request

An API request happens when developer adds an endpoint to a URL and uses that endpoint to call the server or database.



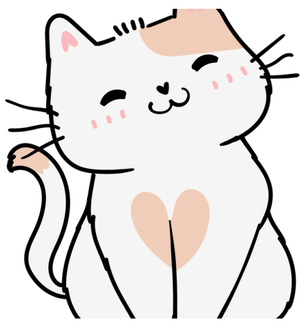


@tauseeffayyaz

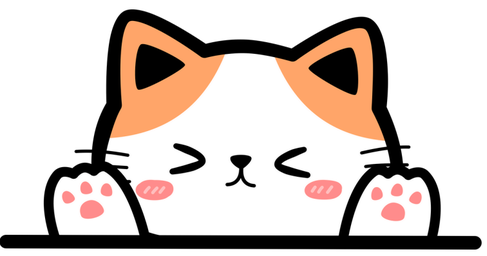


API Keys

API key is a unique identifier that enables other software to authenticate a user or API calling software to an API, to ensure that this person or software is a who it says it is.

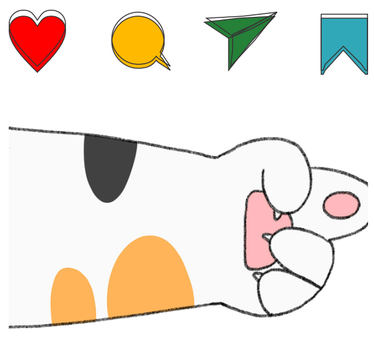


API keys often authenticate the API instead of a user and offer a certain degree of security to API calls.

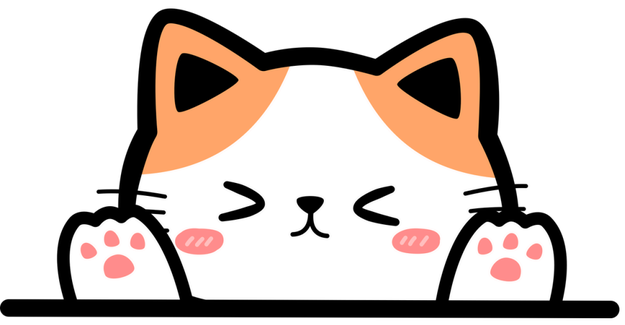


API Layer

API layer is a proxy that joins together all of your service offerings using a graphic UI to provide greater user interactivity. These layers are language-agnostic ways of interacting with apps and help describe the services and data types used to exchange information.



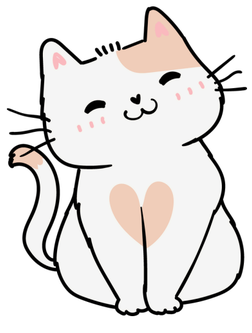
@tauseeffayyaz



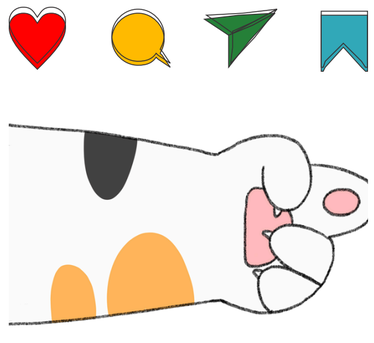
API PORTAL

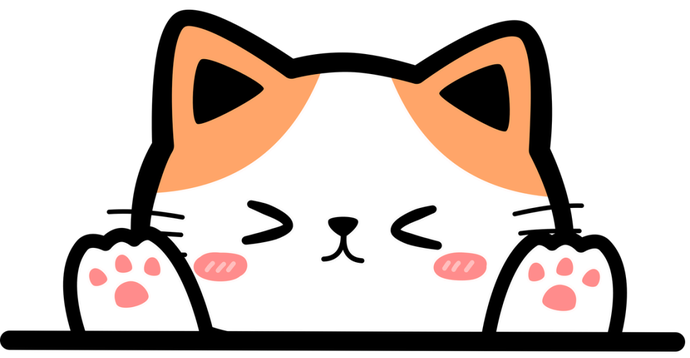
An API portal is a bridge between the API provider and the API consumer.

API portals server to make APIs public and offer content to educate developers about them, their use and how to make the most of them.



An API portal provides the information about the APIs at every stage of the API lifecycle.



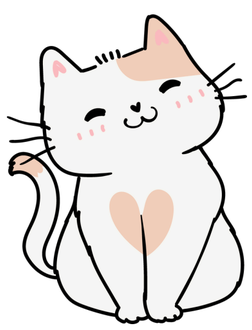


API SECURITY

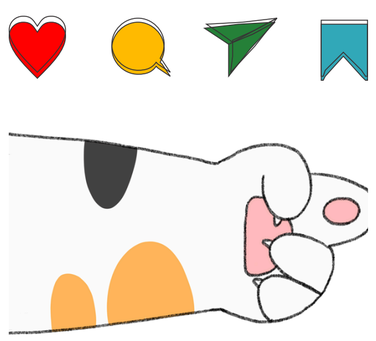
@tauseeffayyaz

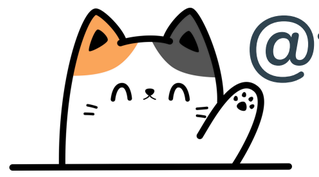
API security defines a set of practices that aim to prevent malicious attacks, misuse and exploit APIs.

It includes basic authentication and authorization, tokens, multi-factor authentication and other advanced security measures.

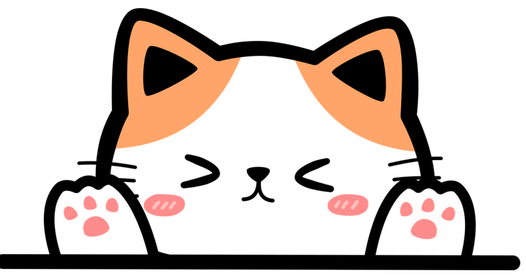


The ubiquitous nature of APIs makes them one of the favourite targets for hackers.





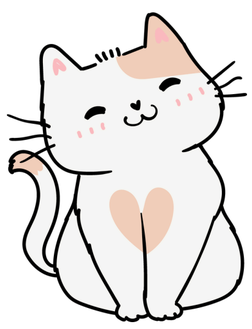
@tauseeffayyaz



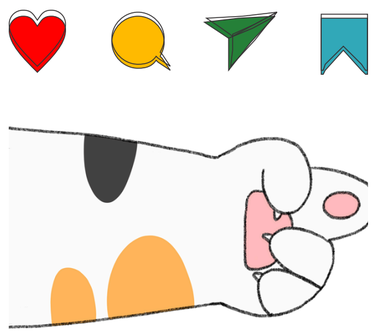
APIGEE

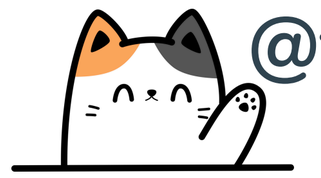
Apigee is an API gateway management tool offered by Google to exchange data across cloud services and applications.

As a proxy layer, Apigee enables you to expose your backend APIs in abstraction or facade and helps protect your APIs, limit their rate and provide analytics and other services.

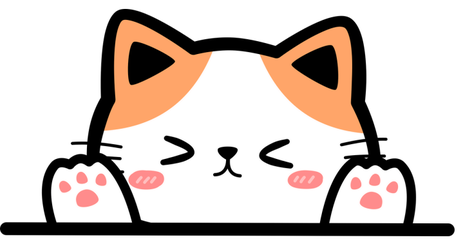


It enables developers to build and manage their APIs in an efficient manner.





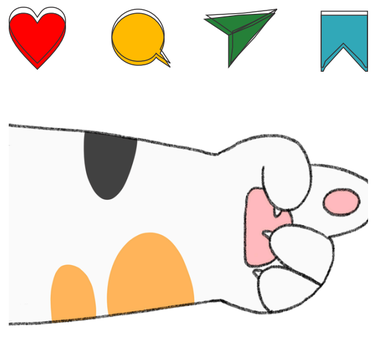
@tauseeffayyaz

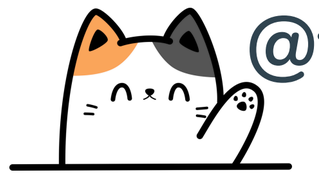


APISEC

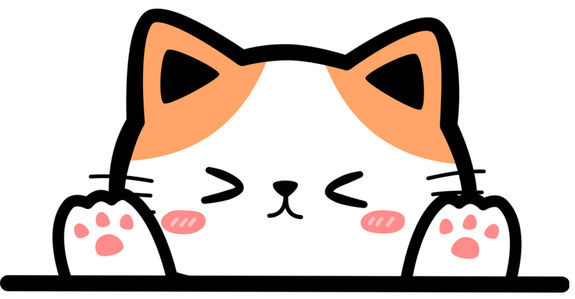
Apisec is an API security company. It leverages automated testing tools to find logic flaws before your code hits the production.

APIsec addresses the business need to secure APIs before they reach production and provides the industry's only automated and continuous API testing platform that uncovers security vulnerabilities in APIs.



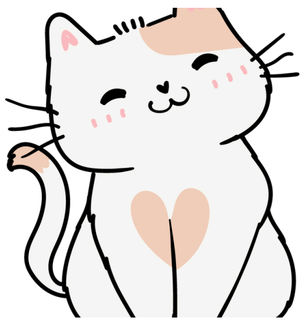


@tauseeffayyaz

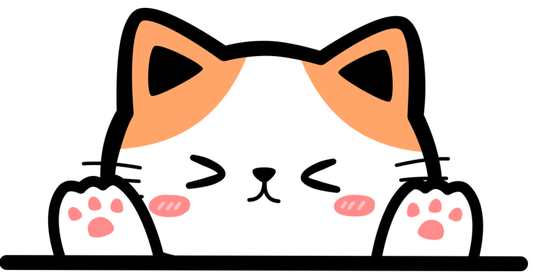


Application

Application software is commonly defined as a program or a bundle of different programs designed for end-users.

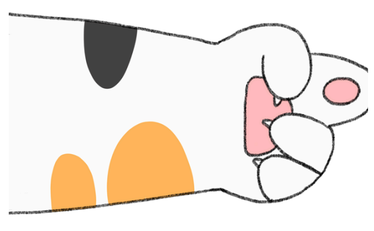


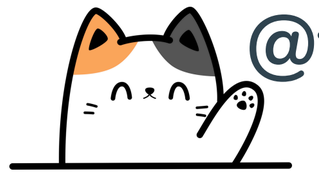
Every program can be called an application and often the terms are used interchangeably.



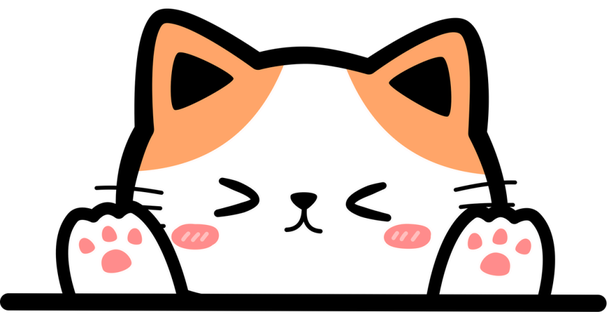
Framework

Framework contains libraries of code, instructions and APIs from which developers and API consumers can obtain information from an app.





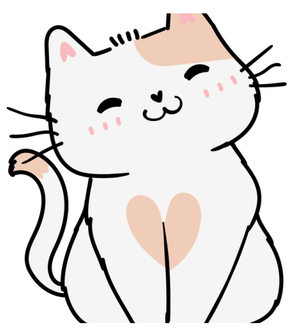
@tauseeffayyaz



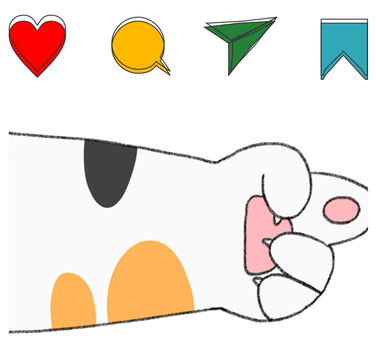
BURP SUITE

Burp or Burp Suite is a set of tools used for penetration testing of web applications.

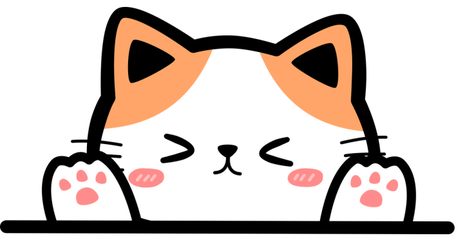
Burp is an all-in-one penetration testing suite that offers users a one-stop shop for all their penetration testing needs.



It contains an intercepting proxy that lets the users see and modify the contents of requests and responses while they are in transit for granular control of your APIs.



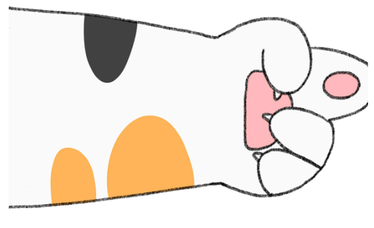
@tauseeffayyaz



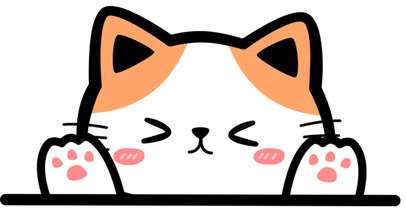
CI / CD

Continuous Integration (CI) and continuous deployment (CD) are a set of operating principles and a collection of practices and agile methodologies that enable development teams to deliver better and faster changes to their code.

CI/CD is one of the most important DevOps practices as it gives teams the tools to focus on meeting their business requirements, code quality and security needs.



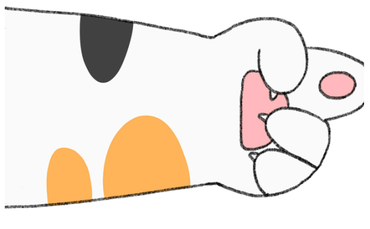
@tauseeffayyaz



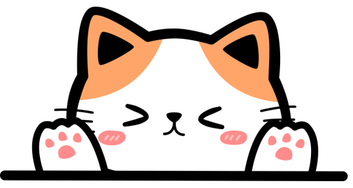
CRUD

CRUD is an acronyms for create, read, update and delete. It refers to the necessary functions to implement a storage application.

Unlike random access memory and internal caching, CRUD data is typically stored and organized into a database, which is simply a collection of data that can be viewed electronically.

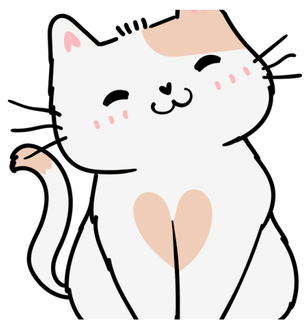


@tauseeffayyaz

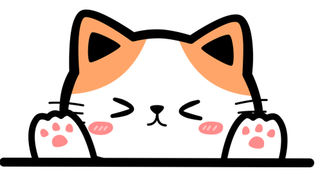


Cache

Cache is a software or hardware component that stores data so users can access and retrieve that data faster. Cached data might be the result of a copy of certain data stored elsewhere.

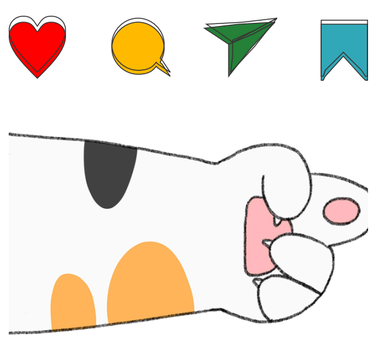


Cache reads data and retrieves it faster than you would otherwise.

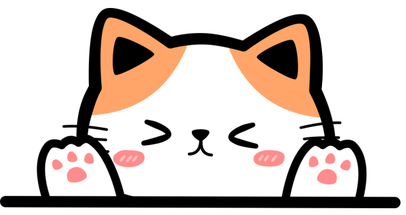


Client

Client is a device that communicates with a server. It can be a desktop, laptop, smartphone or lot-powered device. Most networks allow communication between clients and serveers as it flows through a router or switch.



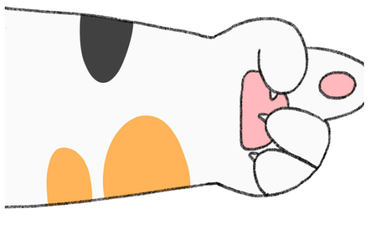
@tauseeffayyaz



DDOS

A distributed denial of service (DDoS) attach is a malicious attack that aims at disrupting the target's traffic.

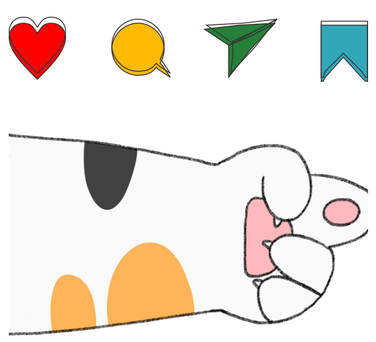
It usually overwhelms the target's infrastructure with a flurry of internet traffic aimed at saturating the servers and causing them to shut the page down.



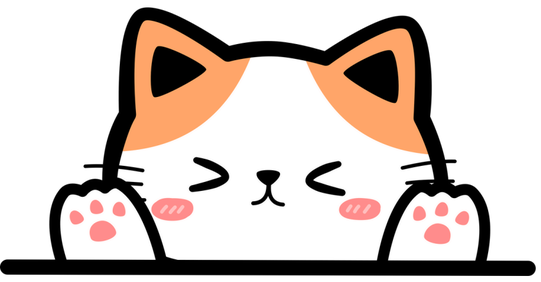
@tauseeffayyaz

Cache is a software or hardware component that stores data so users can access and retrieve that data faster. Cached data might be the result of a copy of certain data stored elsewhere.

An HTTP request sent by a client to a server to retrieve or modify data. A request typically includes a method, a URI and a set of headers and/or a body.

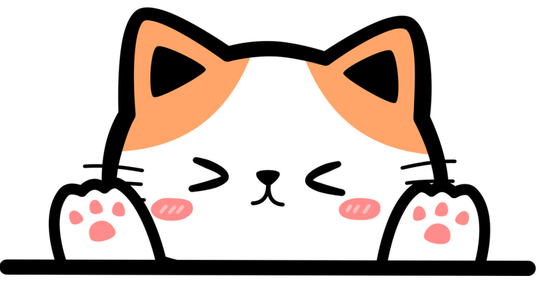


@tauseeffayyaz



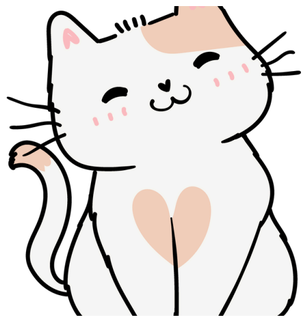
RESPONSE

An HTTP response sent by a server to a client in a response to a request.

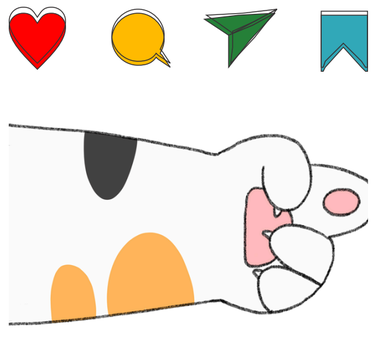


RESPONSE CODE

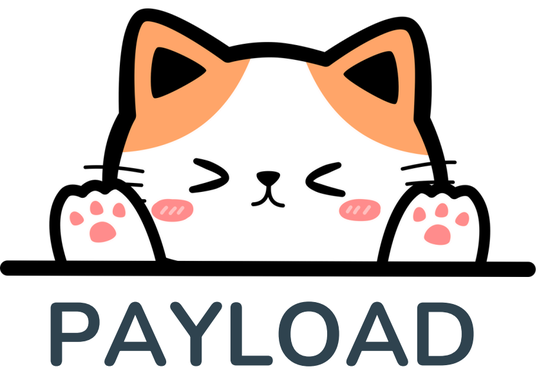
A numerical status code returned in an API response to indicate the success or failure of a request.



Common response codes include 200 (OK), 404 (Not Found) and 500 (Internal Server Error).

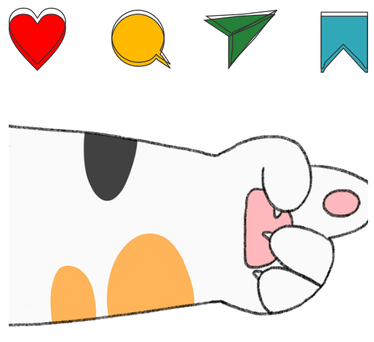


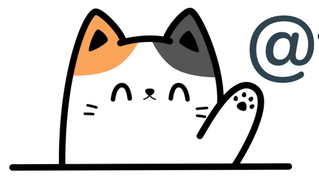
@tauseeffayyaz



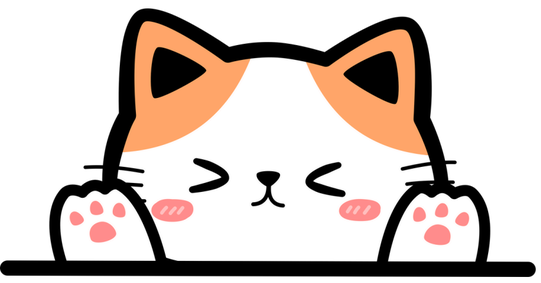
The data sent in an API request or response often in the form of a JSON object.

A technique used in APIs to divide a large dataset into smaller and more manageable chuncks. This allowed client to request a specific page of data rather than receiving



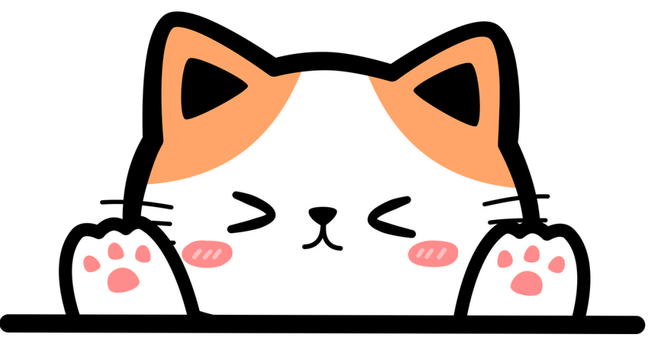


@tauseeffayyaz



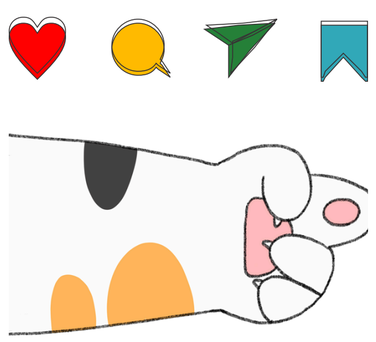
METHOD

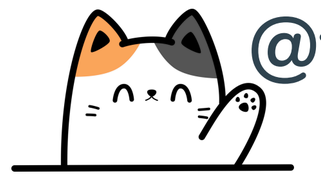
The HTTP verb used in an API request such as GET, POST, PUT or DELETE.



QUERY PARAMETERS

Key-value pairs that are added to the end of an API endpoint URL to specify certain criteria or filters for the data being requested

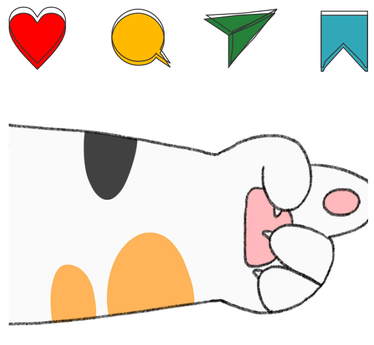


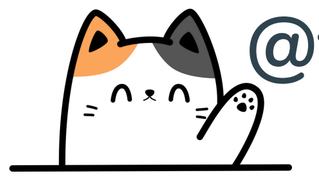


@tauseeffayyaz

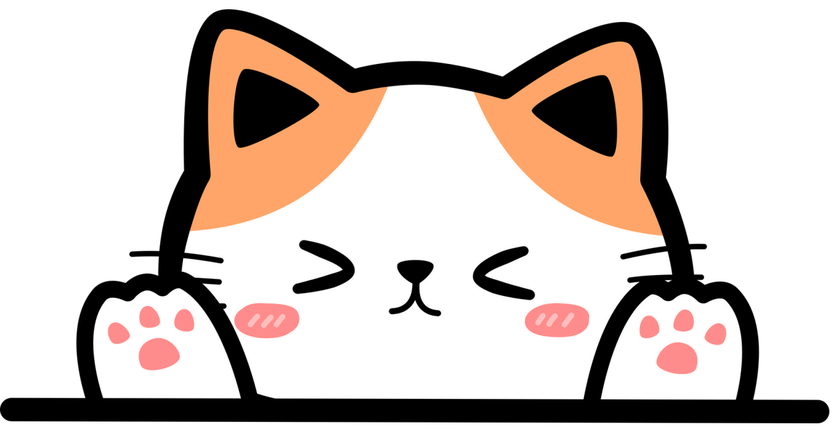
The process of verifying the identity of a client or user before allowing them to access an API. This is often done using an API key or other form of credentials.

The process of limiting the number of API requests that a client can make within a certain timeframe to prevent abuse or overuse of the API.



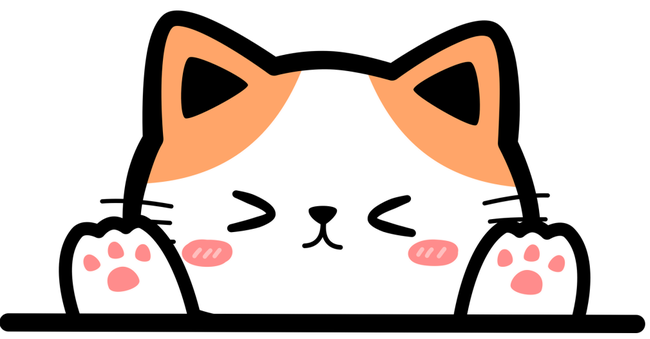


@tauseeffayyaz



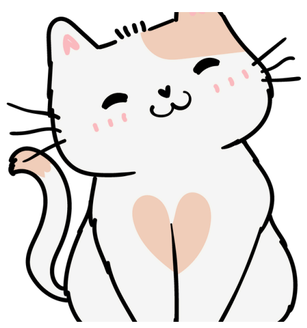
API DOCUMENTATION

Detailed documentation provided by the creator of an API, explaining how to use the API and its various endpoints and parameters.

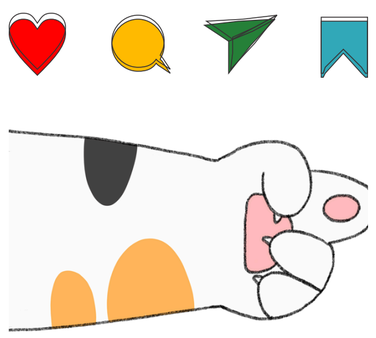


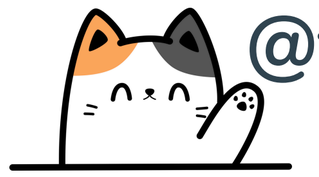
LOGIC FLAW

Business logic flaw result from faulty application logic. It happens when an application behaves unexpectedly.

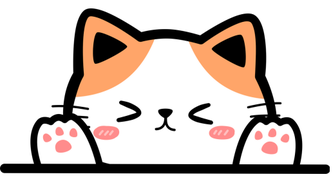


A logic flaw allows attackers to misuse an application and circumvent its rules to change how it performs.





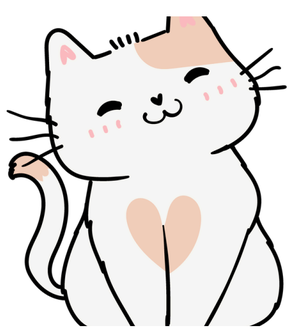
@tauseeffayyaz



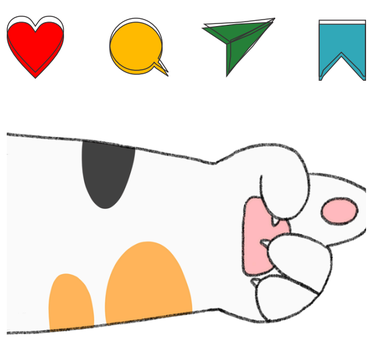
JSON

JSON (JavaScript Object Notation) is a lightweight data-interchange format based on a subset of JavaScript programming language standards.

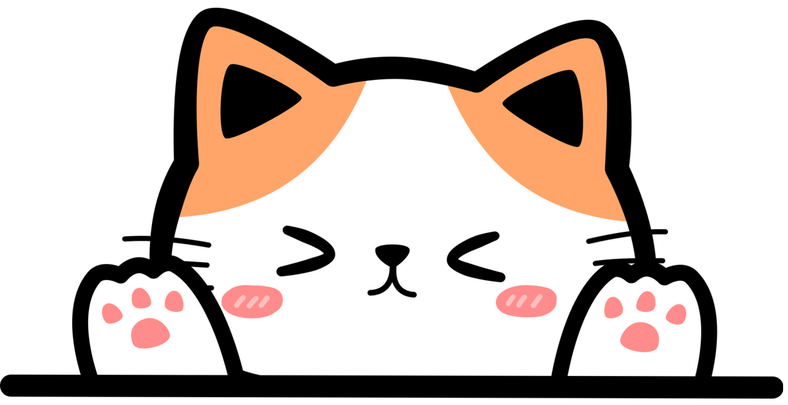
JSON has the advantage that it is both easy for humans to read and write and easy for machines to parse and generate.



JSON format is completely agnostic to languages and uses conventions that are familiar to programmers of C-family languages.



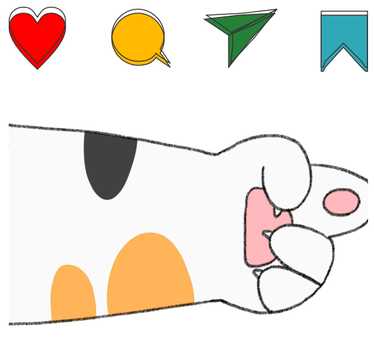
@tauseeffayyaz

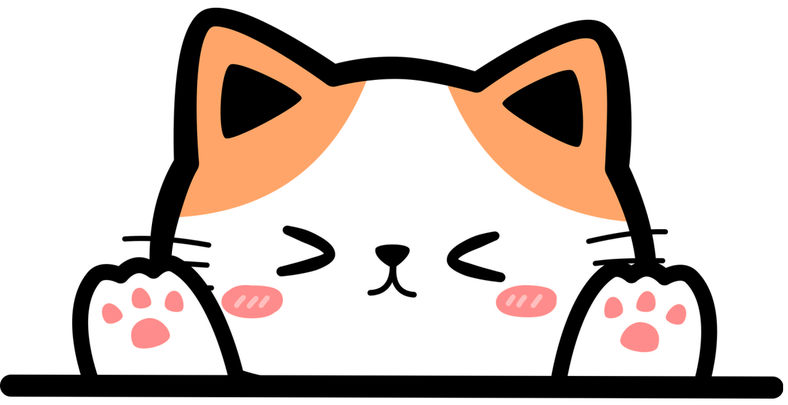


MICROSERVICES

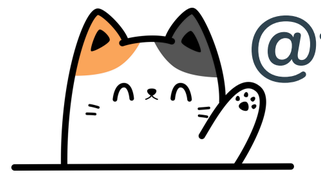
Microservices are also known as microservices architecture. It is a software architecture style that structures apps as a collection of loosely coupled and independent services or sub-apps.

They are highly maintainable services that are organized to enhance an app, website or platform's business capabilities.





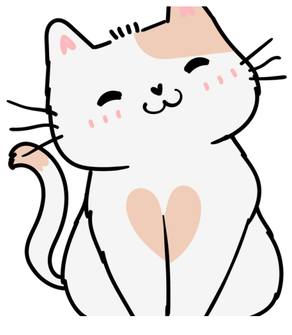
MONETIZATION



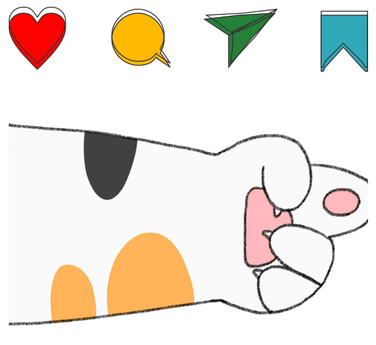
@tauseeffayyaz

API monetization is a process by which a business can generate revenue from its APIs.

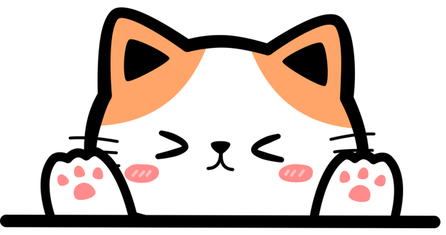
Since APIs enable users to access and integrate data from different sources, they can be used by different developers to integrate relevant services within their products, digital services or applications to become a revenue source.



APIs can be a source of revenue for both public or private services and applications.



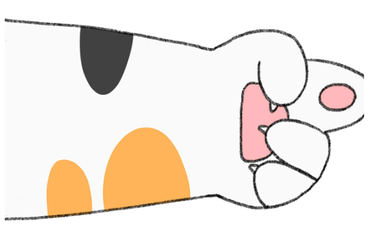
@tauseeffayyaz

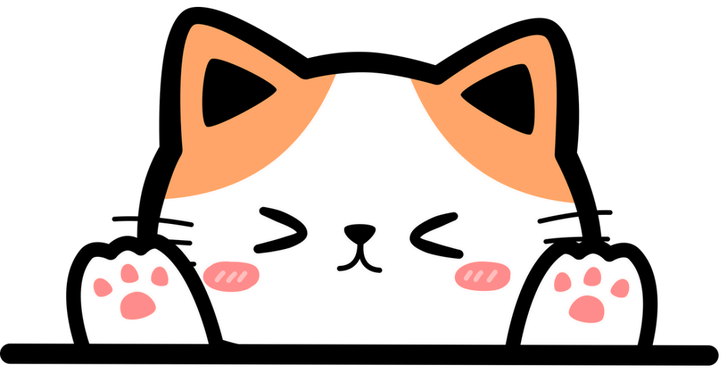


OWASP

OWASP (Open Web Application Security Project) is a non-profit organization dedicated to enhancing software security.

OWASP offers a range of tools to help developers and programmers secure the web through open-source software projects, hundreds of local chapters worldwide and educational, training events.



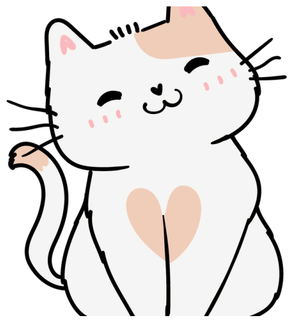


OVER PERMISSIONED CONTAINER

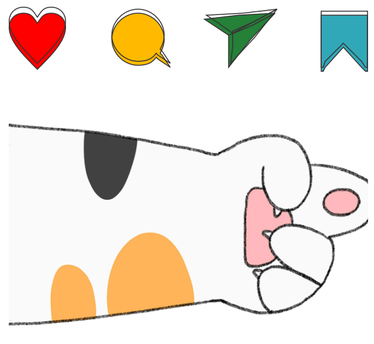
@tauseeffayyaz

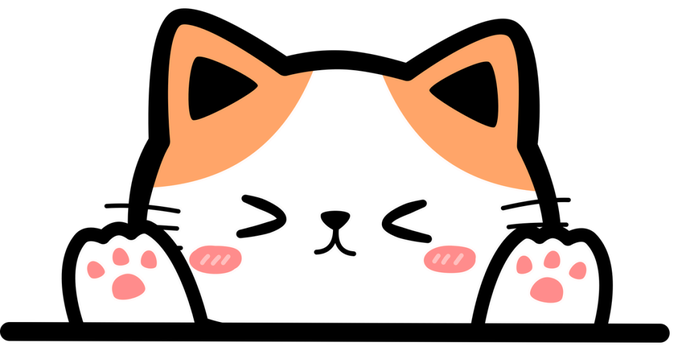
An over-permissioned container is a container that has all the root capabilites of a host machine.

It can access resources that aren't accessible to ordinary containers and users.

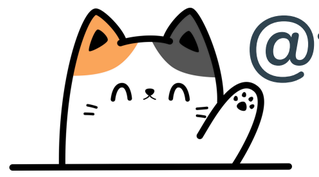


Over-permissioning can give malicious actors a point where they can attack your infrastructure and compromise your implementation of APIs.





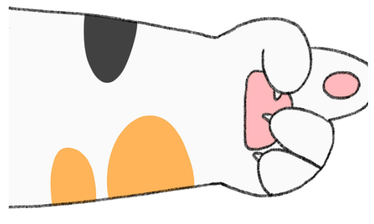
PARAMETERS

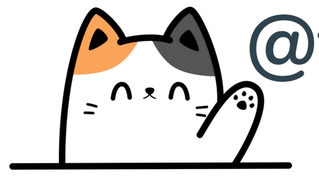


@tauseeffayyaz

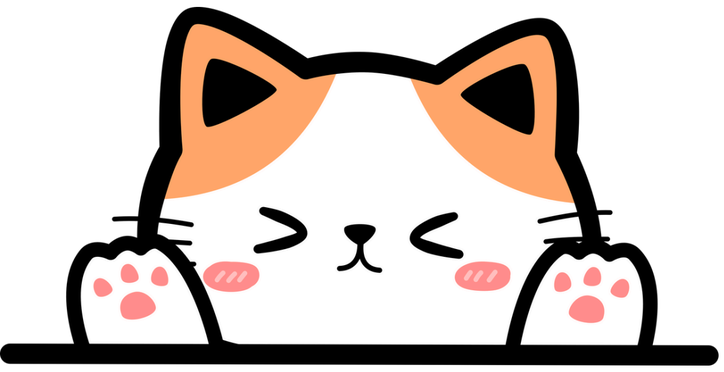
Parameters are special types of variables used in computer programming to pass information betwee procedures and functions.

An argument to a function is referred to as a parameter. Adding four numbers may require four parameters.





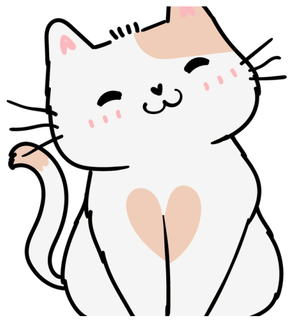
@tauseeffayyaz



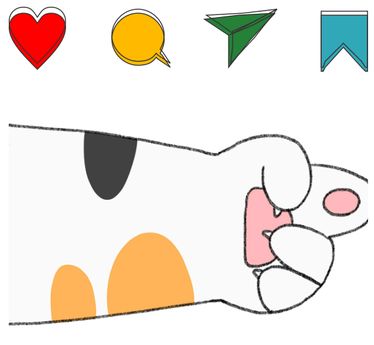
PENETRATION TESTING

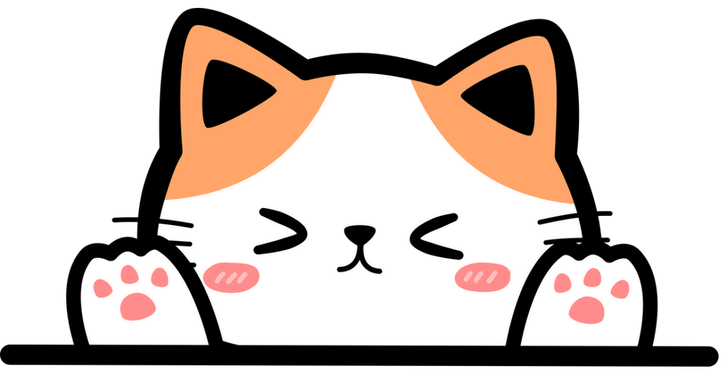
Penetration testing stimulates attacks on your computer system to identify exploitable vulnerabilities.

It identifies, tests and highlights vulnerabilities in an organization's security posture.

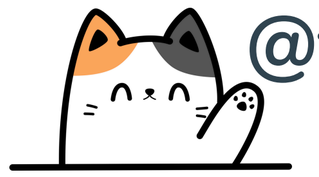


Web application firewals (WAF) are generally augmented by penetration testing in the context of web application security.





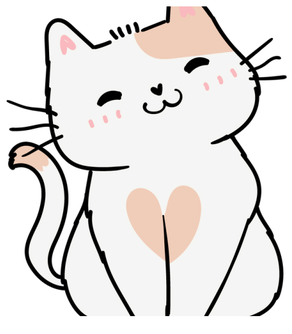
PRODUCTION ENVIRONMENT



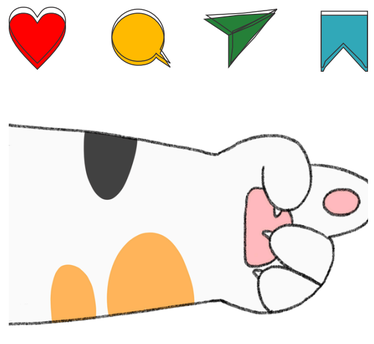
@tauseeffayyaz

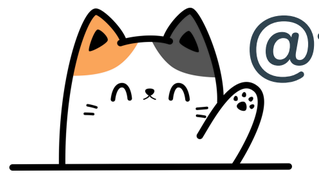
A production environment is where **software** and other products are **actually put into operation** in how their intended users intend them to be used.

Developers generally use this term to refer to the setting where **end-users** will actually **use the products.**

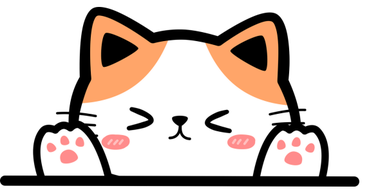


In production, software programs and hardware are run in real-time. They are relied on daily by organizations and companies for their daily operations





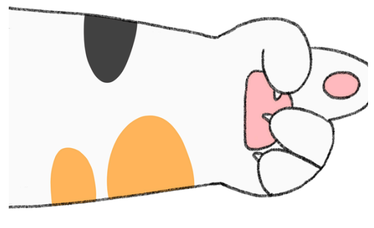
@tauseeffayyaz



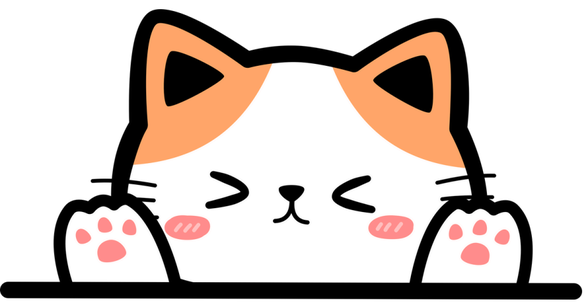
REST

REST (REpresentational State Transfer) is an application programming interface that conforms o the constraints of REST architectural style and enables a quicker interaction between different RESTful web services.

A stateless Web service must be able to read and modify its resource using a predefined set of operations and a textual representation.



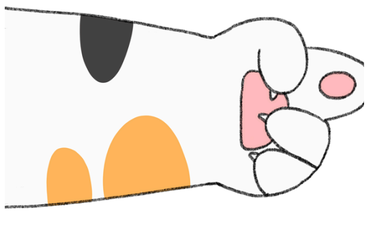
@tauseeffayyaz

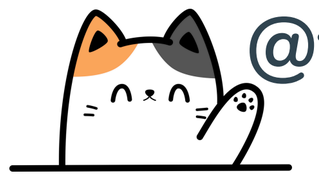


RED TEAMS

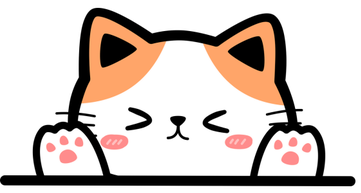
Red teams are cybersecurity professionals trained in attacking systems and breaking into them by finding compromised entry points or exploitable logic flaws.

Red team’s objective is to improve a company’s cybersecurity standing by showing it how they managed to gain access and exploit their system vulnerabilities.





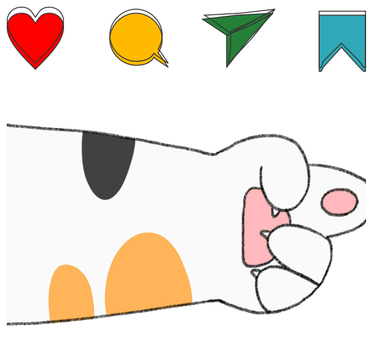
@tauseeffayyaz



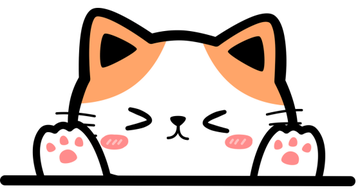
SDK

SDK (Software Development Kit) is a set of instructions, integrated practices, code samples and documentation that enables developers to create software applications on a specific platform.

SDKs can be seen as workshops with everything developers need to build specific software for a specific platform.



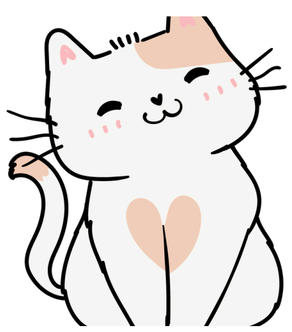
@tauseeffayyaz



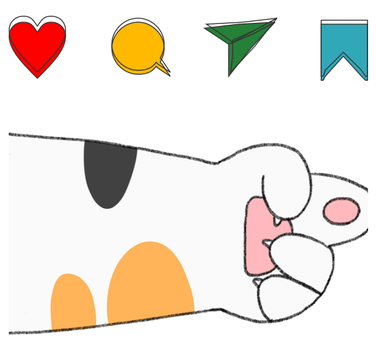
SDLC

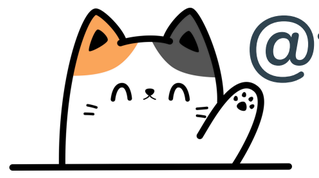
SDLC (Software Development Lifecycle) is a process for planning, creating, testing and deploying an information system.

It aims at producing quality software at the lowest cost in the shortest time possible.

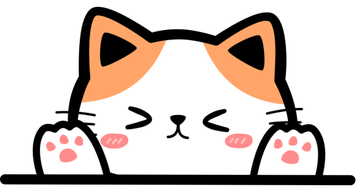


It gives developers a structured flow divided into phases to help companies produce high-quality software products.





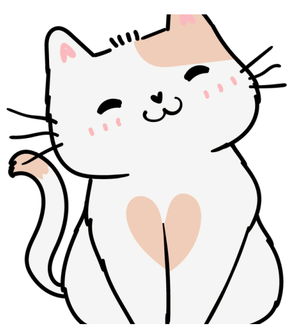
@tauseeffayyaz



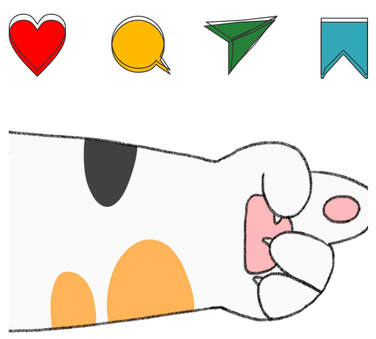
SOAP

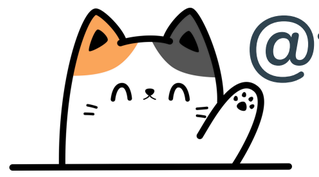
SOAP (Simple Object Access Protocol) is a protocol specification for exchanging structured information to implement web services.

It leverages XML information set for message format and other application-layer protocols such as HTTP or SMTP for message transmission. The messaging services provided by SOAP are exclusively XML-based.

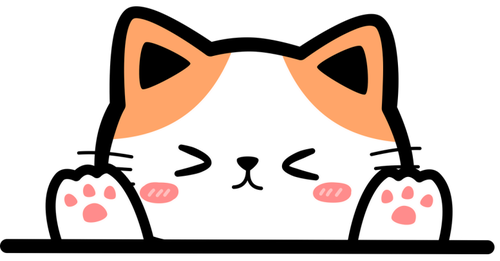


SOAP was originally developed by Microsoft to replace old technologies that cannot work over internet such as DCOM and COBRA.





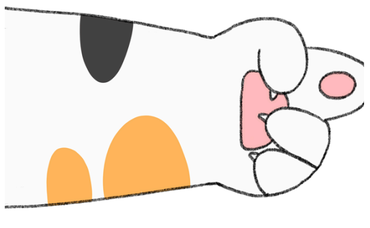
@tauseeffayyaz

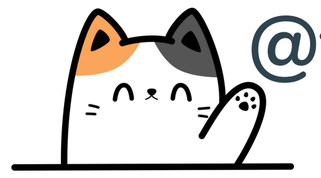


SQL INJECTION

An SQL injection technique is a way to inject malicious code into a databse that may damage it.

These are on of the most common hacking techniques and rely on the placement of malicious SQL code statements via web input using forms or other editable fields.

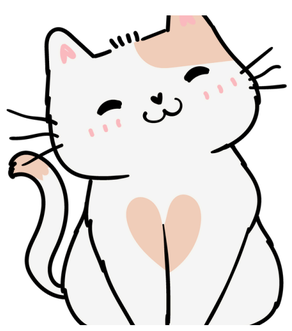




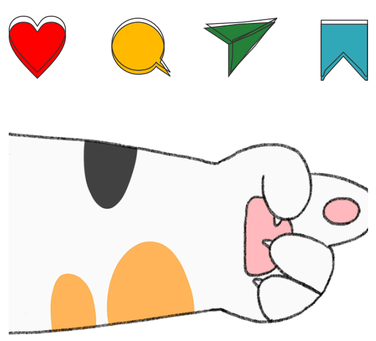
@tauseeffayyaz

Webhook or web callback or HTTP push API is a way for an app to provide other applications with real-time information.

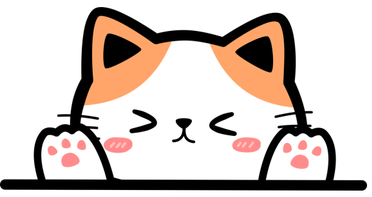
They deliver data directly to other applications so data is available immediately instead of standard APIs requiring frequent polling for real-time data.



Webhooks are beneficial to both consumers and providers but their only drawback is the difficulty of setting them up first.



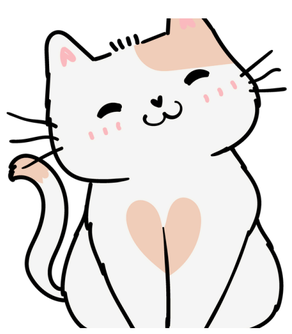
@tauseeffayyaz



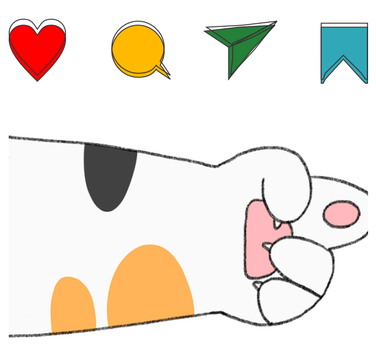
ZAP

ZAP or OWASP Zed Attack Proxy is one of the world's most popular free security tools which ets delivers automatically find security vulnerabilities in their applications.

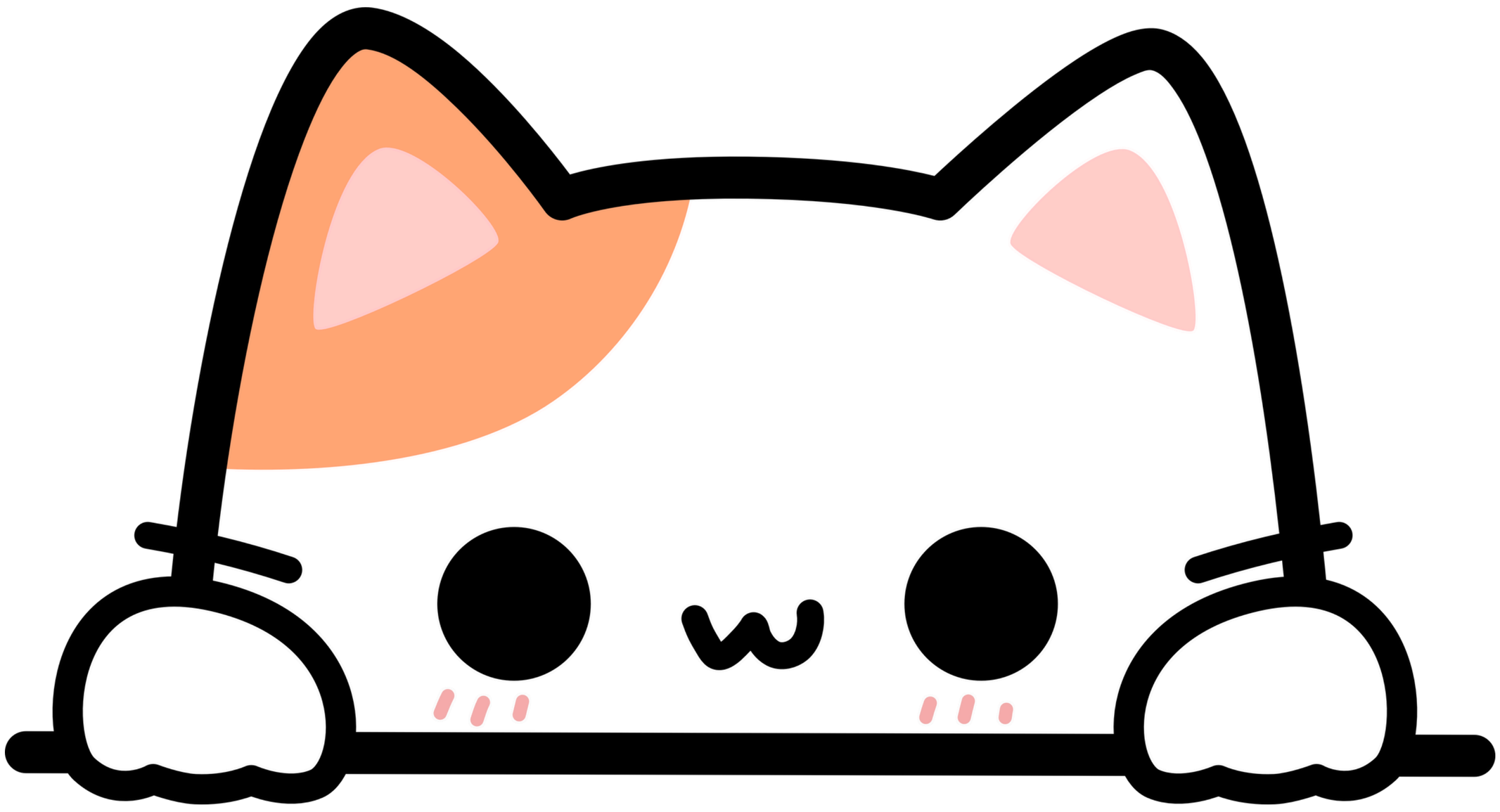
By automating penetration testing and security regression testing, developers can automate an application's security testing during the CI/CD process.



Zap lets you do nearly everything you can do with the desktop interface using its powerful API.



@tauseeffayyaz



THANK YOU

LIKE & REPOST

Follow @tauseeffayyaz for more helpful content!