# AFRICAHACKON

# WHO AM I?

AFRICAHACKON

## Michael Chesang

> Cyber Security Engineer
> Cyber Guard Africa

## Topic

> API Security

## Pre-requisites

> Postman
> vAPI (docker)
> Burpsuite

## Difficulty

> Easy - Intermediate

vip3.r _vip3rx

# API Security

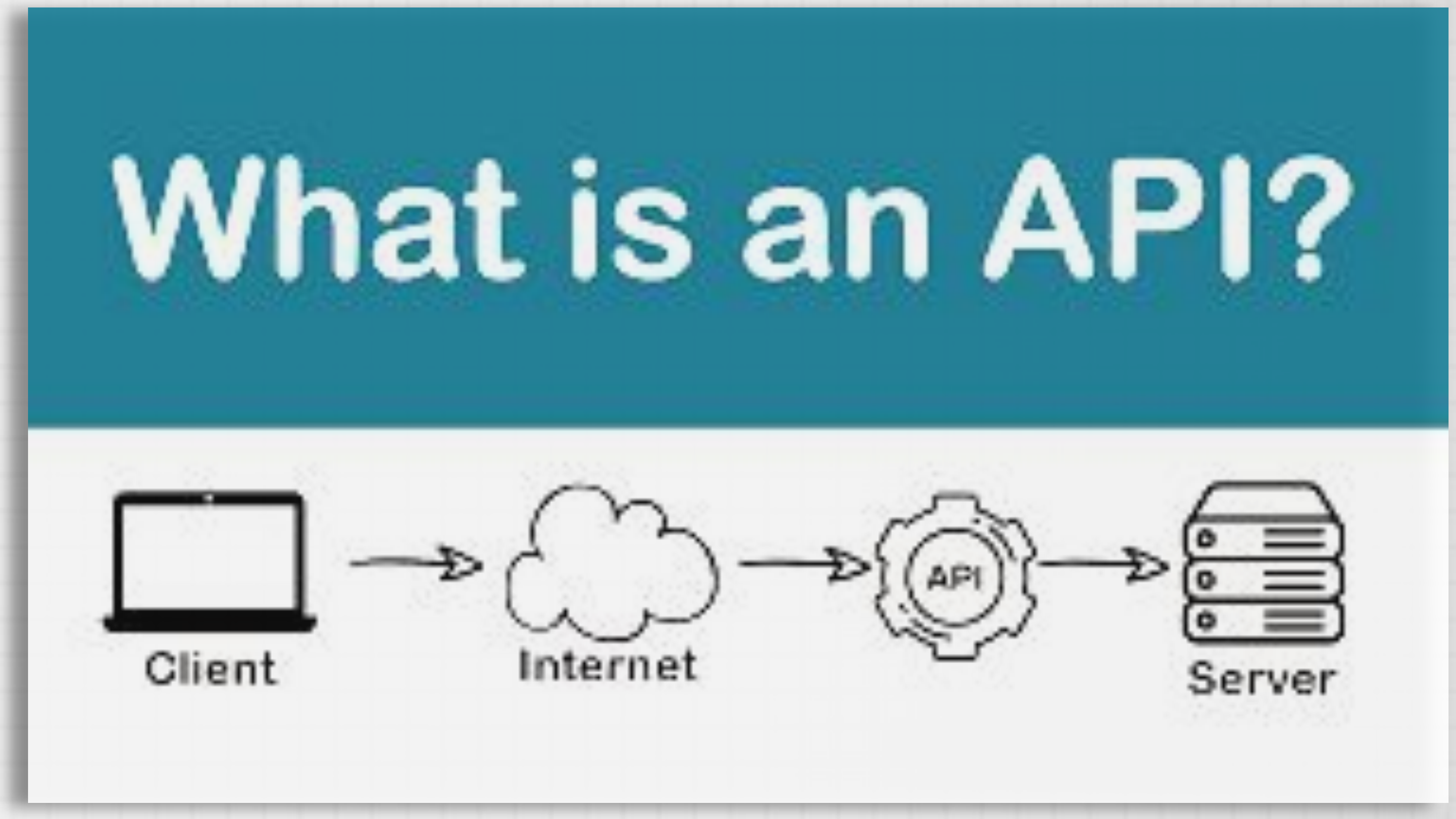
# Basics **First**

## WHAT IS AN API?

- Definition - API stands for Application Programming Interface.

- Function - A set of rules and protocols that allows different software entities to communicate with each other.

- Use case - Powers modern web applications, mobile apps, and integrated tech systems.



# Importance of **API Security?**

## WHY API MATTERS?

- Data Protection: APIs often handle sensitive data like user information, payment details, and more.
- System Integrity: A compromised API can be a gateway for attackers to manipulate systems and applications.
- Business Reputation: Security breaches can erode trust, leading to loss of customers and potential legal consequence.

# OWASP TOP 10 API **VULNERABILITIES**

## KEY THREATS IN THE API LANDSCAPE?

- API1: Broken Object Level Authorization
- API2: Broken User Authentication
- API3: Excessive Data Exposure
- API4: Lack of Resources & Rate Limiting
- API5: Broken Function Level Authorization
- API6: Mass Assignment
- API7: Security Misconfiguration
- API8: Injection
- API9: Improper Assets Management
- API10: Insufficient Logging & Monitoring

# DEMO

# API 1: BROKEN OBJECT LEVEL **AUTHORIZATION**

## THE CONSEQUENCES OF BROKEN OBJECT LEVEL AUTHORIZATION

- Unauthorized data access.
- Exposure of sensitive or private information.
- Potential legal and reputational repercussions.

## REMEDIES???

- Implement fine-grained access controls.
- Use role-based access controls.
- Regularly review and audit authorization configurations.

# API 2: BROKEN USER **AUTHENTICATION**

## THE PERILS OF INADEQUATE USER AUTHENTICATION

- Unauthorized system access.
- Data breaches and leaks.
- Account hijacking or impersonation.

## RESOLVE 😌

- Implement Multi-Factor Authentication (MFA).
- Enforce strong password policies and rotations.
- Ensure secure session management.

# API 3: LACK OF RATE **LIMITING**

## THE DOWNSIDE OF UNCONTROLLED TRAFFIC

- Service disruptions and API downtimes.
- Amplified risk of DDoS attacks.
- System strain leading to performance issues.

## MAGIC FIX 🪄

- Define and enforce API call thresholds.
- Implement token bucket or leaky bucket algorithms.
- Monitor traffic and adjust limits as needed.

# Q&A

# THANK YOU