

Cazando Apis en Aplicaciones Android



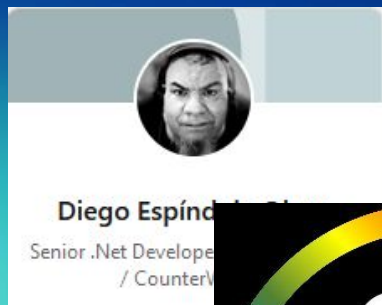
Diego Espíndola

- LinkedIn [Link](#)
- GitHub [Link](#)
- Diplomado UC [Link](#)
- Telegram [Link](#)
- Comunidades



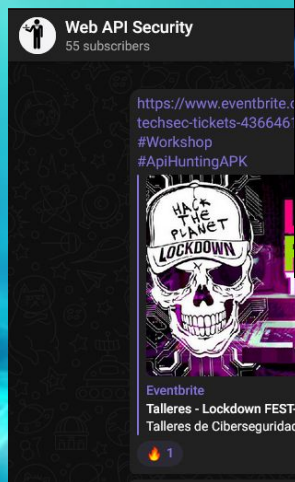
SOCHISI®

SOCIEDAD CHILENA
DE SEGURIDAD
DE LA INFORMACIÓN



Diego Espíndola

Senior .Net Developer
/ Counter...



api-hunting-apk (Public)

☆ 1 Updated 3 days ago

faviconfrenzy (Public)

It find the Favicon of a website, no need to give the exact favicon url, just some url, then send it to shodan to find other websites using the same Favicon

osint favicon recon reconnaissance bugbounty-tool

MIT License Updated on Aug 25

blic

ca de informacion de personas en chile. Basado en web
cosillas mas

Ver más



Diego Espíndola

Experto en desarrollo de soluciones de software



Belisario Martinic

Experto en Mejores Prácticas para la Estrategia, Transformación, Gobierno y Gestión de TIC



Sebastián Vargas

Experto en Seguridad de la Información, Tecnologías de la Información, Gestión y Gobierno TI

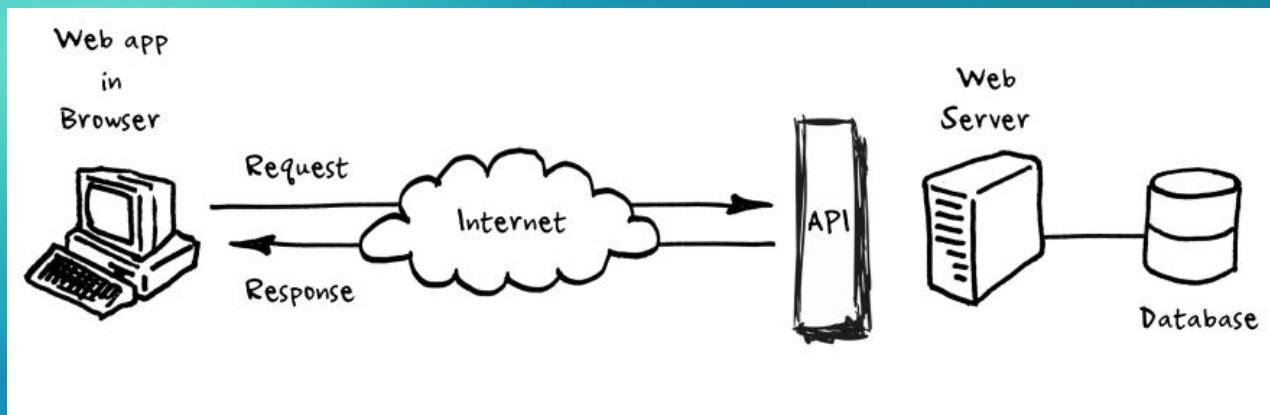
Cristián Rojas

Consultor experto en desarrollo seguro de software, seguridad de la información y en sistemas de gestión de la ciberseguridad

Agenda

- ¿APIs, Que es eso?.
- Manos a la masa.
- Consejos de mitigación.
- Proyectos de OWASP Relacionados.

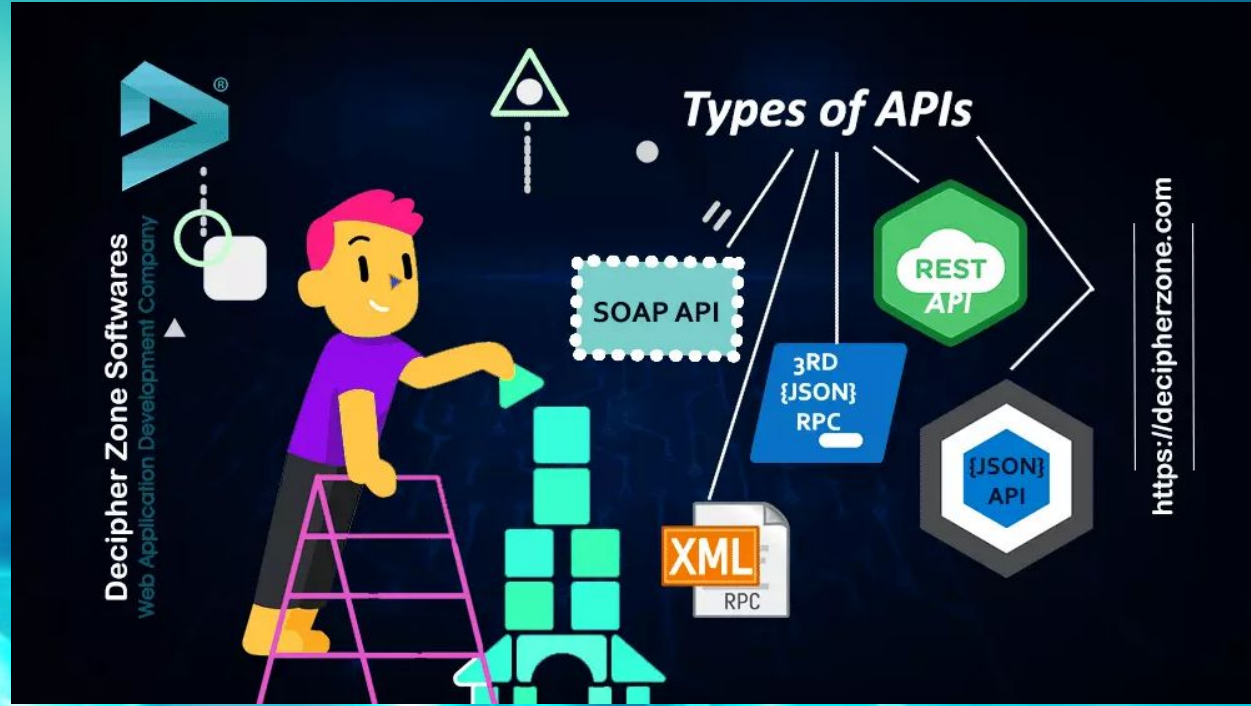
¿APIs, Que es eso?



¿APIs, Que es eso?



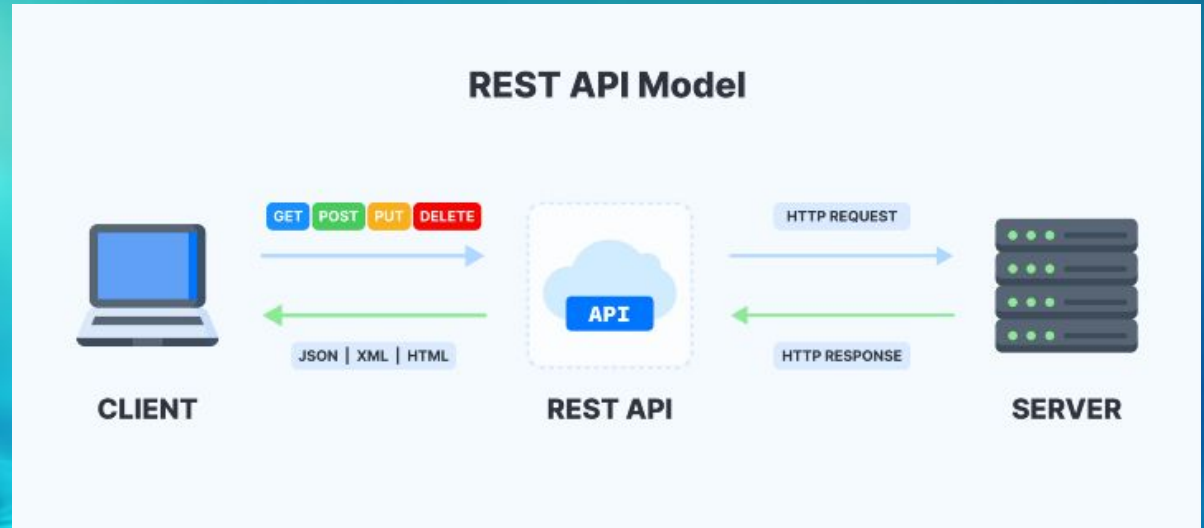
¿APIs, Que es eso?



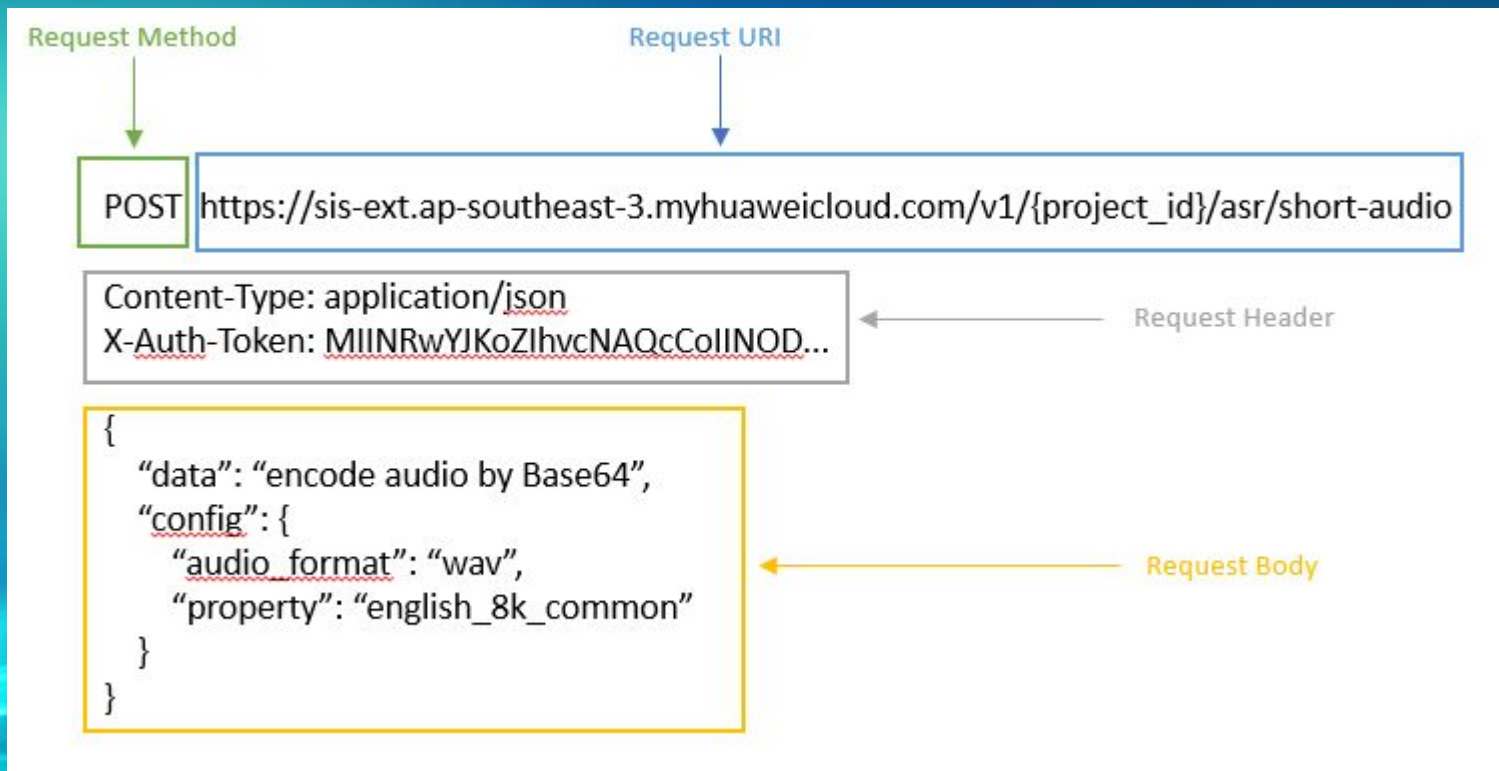
¿APIs, Que es eso?



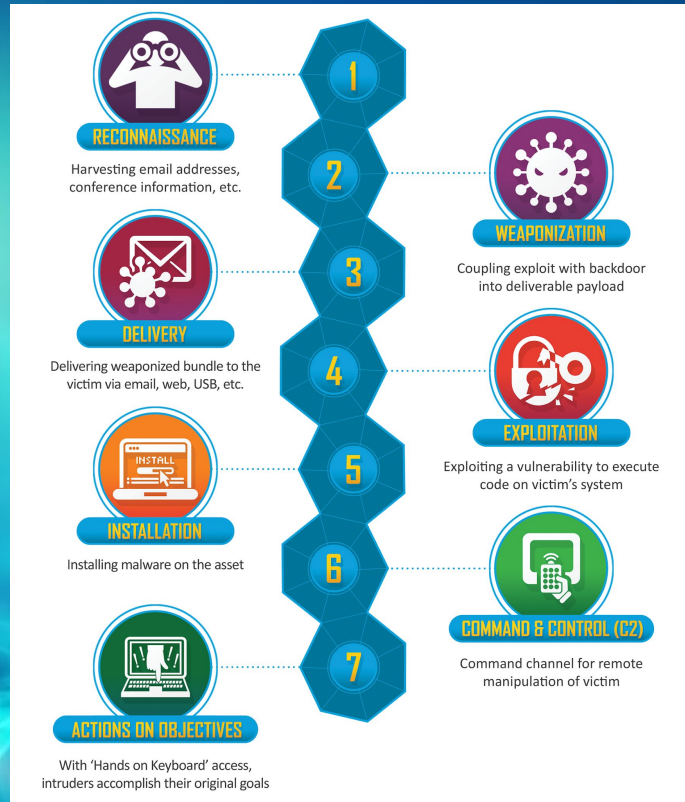
¿APIs, Que es eso?



¿APIs, Que es eso?



Manos a la masa



Manos a la masa



Consejos de mitigación

Primer caso (Api Key a simple vista)

- Restricciones de cliente en apikeys de google Cloud (servidor)
- No Almacenar Api Keys en el código fuente, Usar credenciales de usuario para obtener Api Key en tiempo real.
- Almacenar Api Key en librería nativa en C++
- Android Keystore System

Consejos de mitigación

Segundo Caso (MITM)

- Certificate Pining
- Certificate Transparency
- Obligar Android 7+

Proyectos OWASP relacionados

- OWASP Top 10 Mobile

Top 10 Mobile Risks - Final List 2016

- M1: Improper Platform Usage
- M2: Insecure Data Storage
- M3: Insecure Communication
- M4: Insecure Authentication
- M5: Insufficient Cryptography
- M6: Insecure Authorization
- M7: Client Code Quality
- M8: Code Tampering
- M9: Reverse Engineering
- M10: Extraneous Functionality

Proyectos OWASP relacionados

- OWASP Top 10 Mobile
- OWASP MASVS

Security Verification Requirements

#	MSTG-ID	Description	L1	L2
3.1	MSTG-CRYPTO-1	The app does not rely on symmetric cryptography with hardcoded keys as a sole method of encryption.	x	x
3.2	MSTG-CRYPTO-2	The app uses proven implementations of cryptographic primitives.	x	x
3.3	MSTG-CRYPTO-3	The app uses cryptographic primitives that are appropriate for the particular use-case, configured with parameters that adhere to industry best practices.	x	x
3.4	MSTG-CRYPTO-4	The app does not use cryptographic protocols or algorithms that are widely considered deprecated for security purposes.	x	x
3.5	MSTG-CRYPTO-5	The app doesn't re-use the same cryptographic key for multiple purposes.	x	x
3.6	MSTG-CRYPTO-6	All random values are generated using a sufficiently secure random number generator.	x	x

Proyectos OWASP relacionados

- [OWASP Top 10 Mobile](#)
- [OWASP MASVS](#)
- [OWASP TOP 10 API](#)

OWASP API SECURITY TOP 10

A1:2019	Broken Object Level Authorization
A2:2019	Broken Authentication
A3:2019	Excessive Data Exposure
A4:2019	Lack of Resources & Rate Limiting
A5:2019	Broken Function Level Authorization
A6:2019	Mass Assignment
A7:2019	Security Misconfiguration
A8:2019	Injection
A9:2019	Improper Assets Management
A10:2019	Insufficient Logging & Monitoring

Proyectos OWASP relacionados

- OWASP Top 10 Mobile
- OWASP MASVS
- OWASP TOP 10 API
- OWASP Application Security Verification Standard

V13 API y Servicios Web	61
<i>Objetivo de Control</i>	<i>61</i>
<i>V13.1 Seguridad Genérica de Servicios Web.....</i>	<i>61</i>
<i>V13.2 Servicio Web RESTful</i>	<i>61</i>
<i>V13.3 Servicio Web SOAP.....</i>	<i>62</i>
<i>V13.4 GraphQL.....</i>	<i>62</i>
<i>Referencias</i>	<i>62</i>

Proyectos OWASP relacionados

- [OWASP Top 10 Mobile](#)
- [OWASP MASVS](#)
- [OWASP TOP 10 API](#)
- [OWASP Application Security](#)
- [REST Security Cheat Sheet](#)

REST Security Cheat Sheet

Introduction

REST (or **RE**presentational **S**tate **T**ransfer) is an architectural style first described in [Roy Fielding's](#) Ph.D. dissertation on [Architectural Styles and the Design of Network-based Software Architectures](#).

It evolved as Fielding wrote the HTTP/1.1 and URI specs and has been proven to be well-suited for developing distributed hypermedia applications. While REST is more widely applicable, it is most commonly used within the context of communicating with services via HTTP.



That's all Folks!