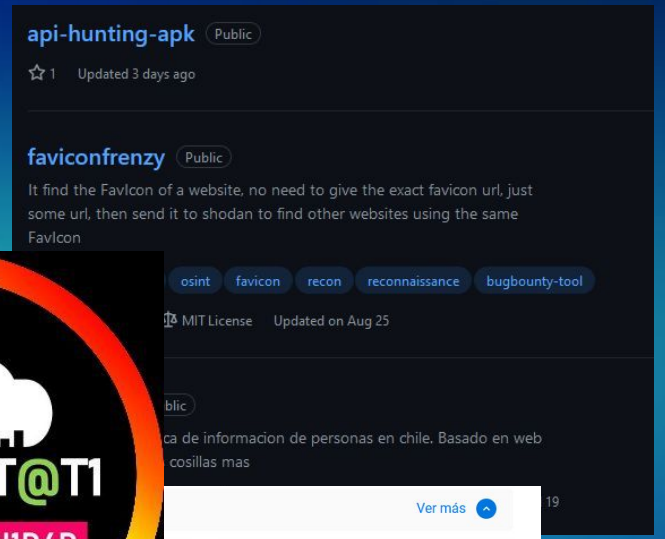
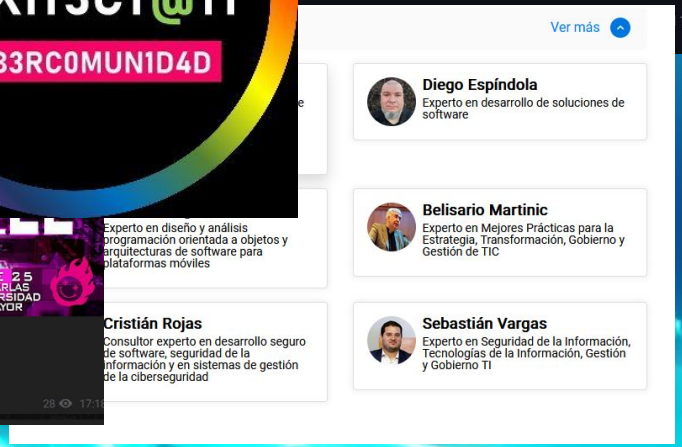
Cazando Apis en Aplicaciones Android

Diego Espíndola

- Linkedin Link
- GitHub Link
- Diplomado UC Link
- Telegram Link
- Comunidades





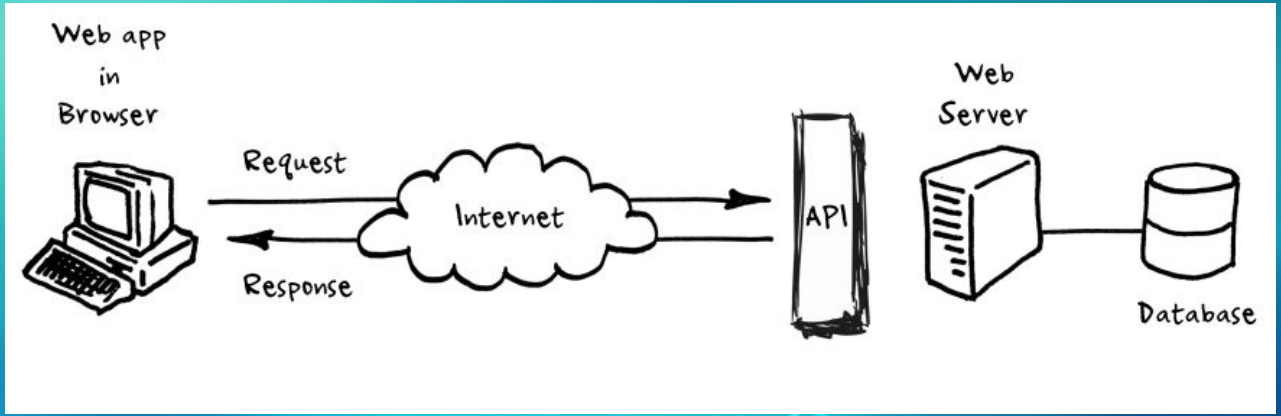
SOCHISI®

SOCIEDAD CHILENA
DE SEGURIDAD
DE LA INFORMACIÓN

Agenda

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

¿APIs, Que es eso?

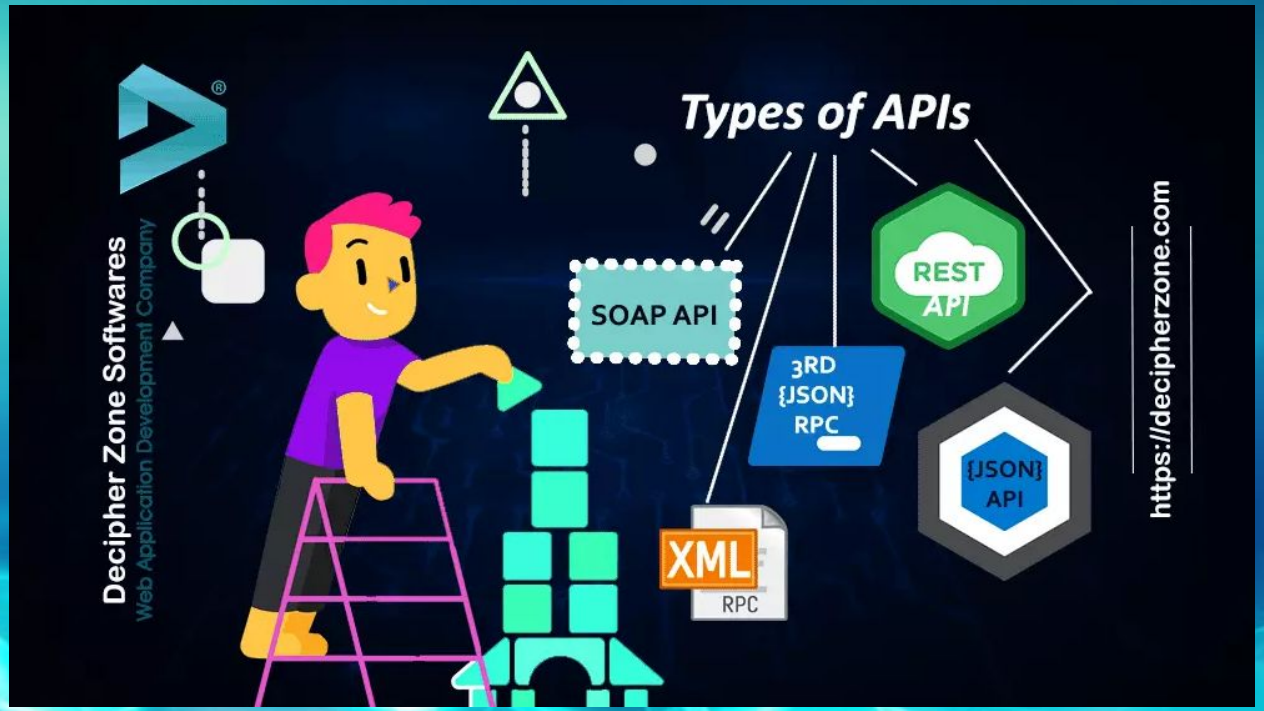


https://kozub.com.ar/que-es-exactamente-una-api/

¿APIs, Que es eso?

https://geekflare.com/es/api-monitoring-tools/

¿APIs, Que es eso?

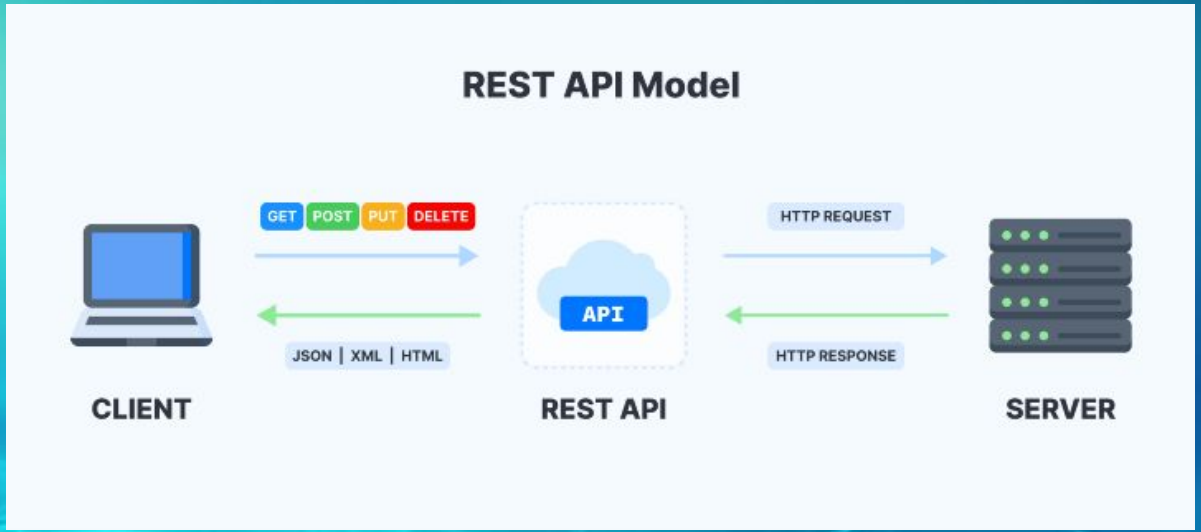


https://www.decipherzone.com/blog-detail/Types-of-APIs

¿APIs, Que es eso?

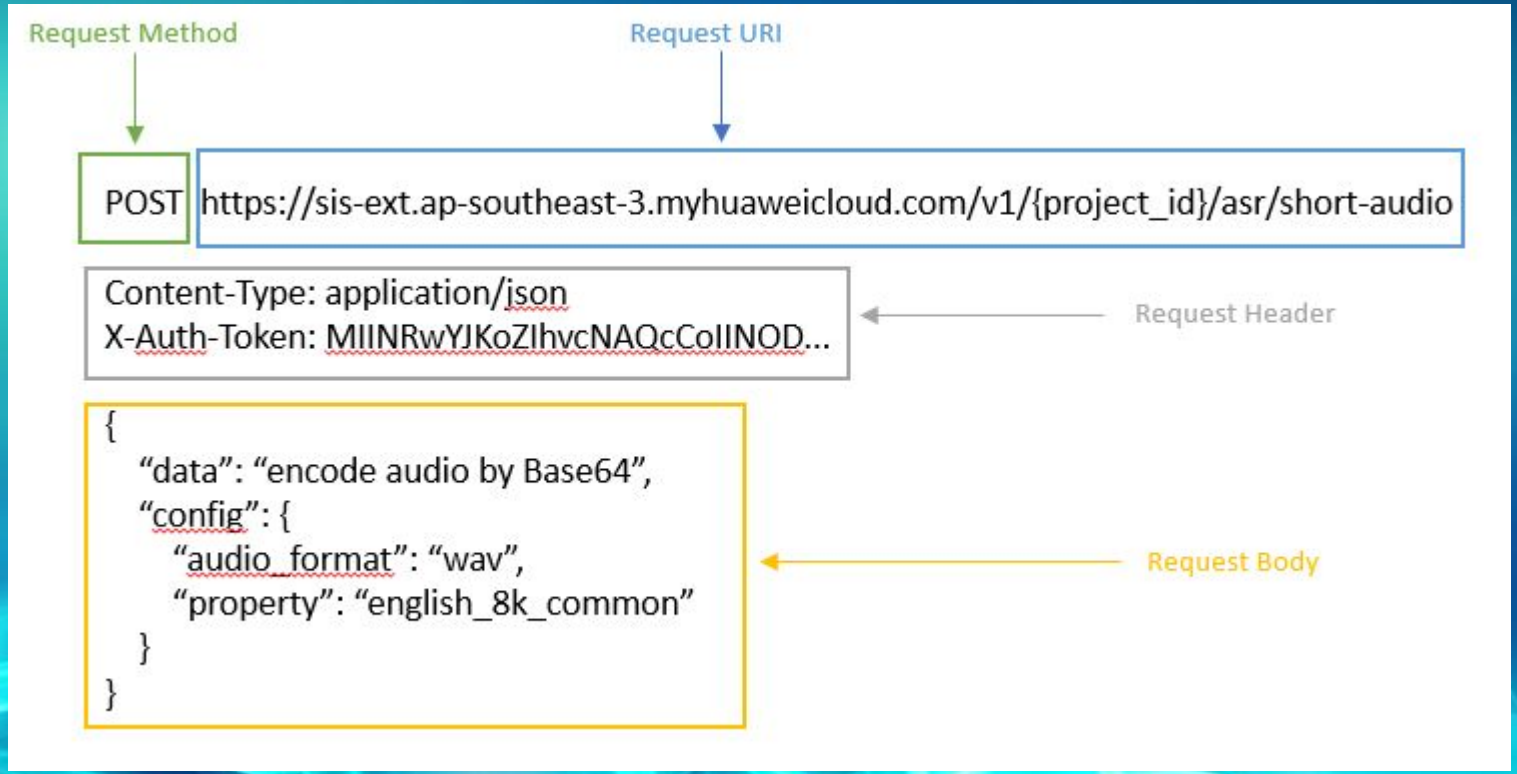
https://medium.com/codestorm/best-practices-for-rest-api-development-8434352f3213

¿APIs, Que es eso?



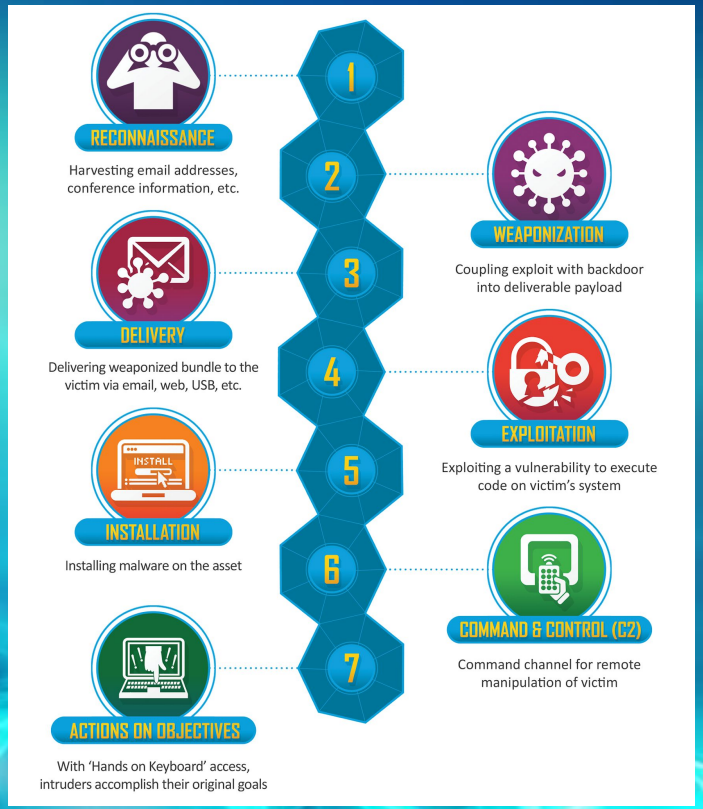
https://medium.com/codestorm/best-practices-for-rest-api-development-8434352f3213

¿APIs, Que es eso?



https://support.huaweicloud.com/intl/en-us/api-sis/sis_03_0057.html

Manos a la masa



https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

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 codigo 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+

https://developer.android.com/training/articles/security-config

Proyectos OWASP relacionados

- OWASP Top 10 Mobile

Proyectos OWASP rela

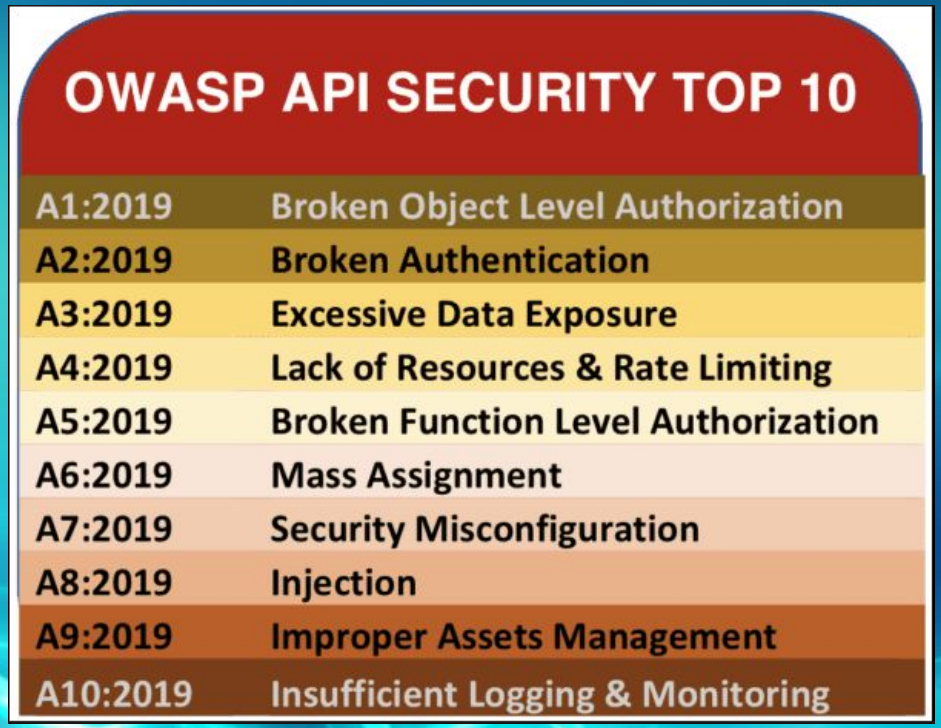
- OWASP Top 10 Mobile
- OWASP MASVS

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

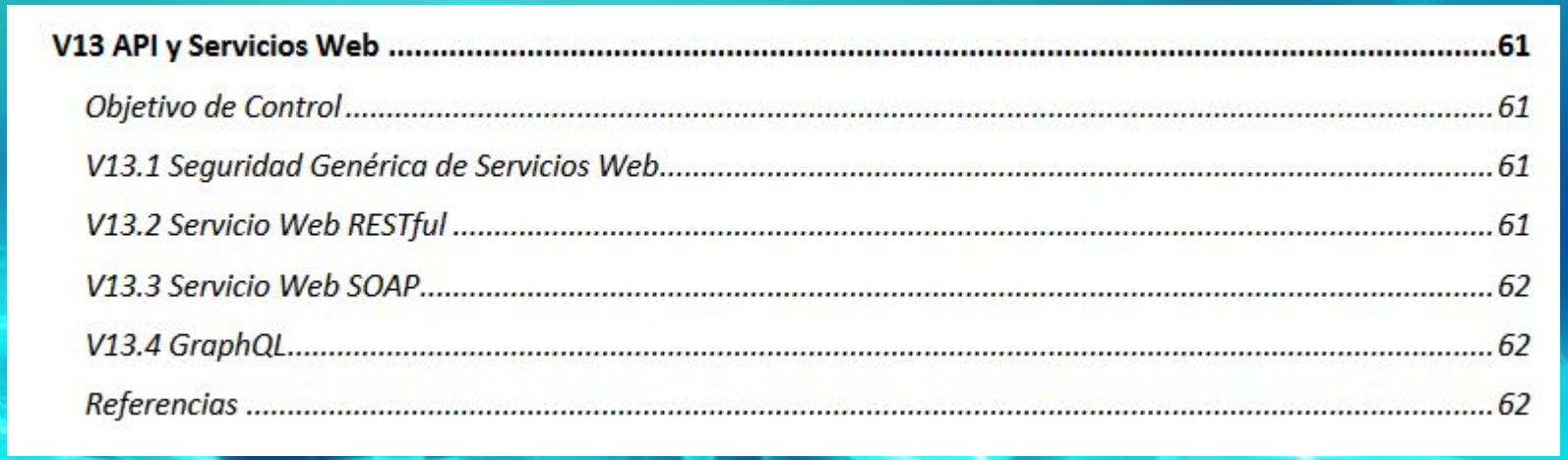
Proyectos OWASP relacionados

- OWASP Top 10 Mobile
- OWASP MASVS
- OWASP TOP 10 API



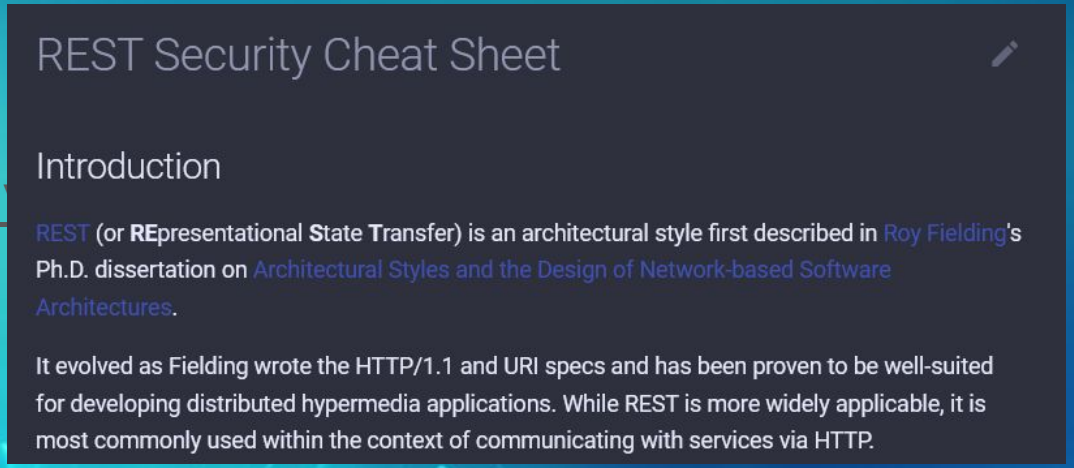
Proyectos OWASP relacionados

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



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!