9-11-2025

PRACTICA 1 - OSINT

UNIDAD 2. NIVEL DE SEGURIDAD REQUERIDO POR LAS APLICACIONES

IZAN NAVARRO LUJAN
IES SERRA PERENXISA

INDICE

Parte 1 : Fuentes de Información OSINT para el desarrollo de aplicaciones

Investiga qué fuentes de información pública son de uso común en la comunidad de profesionales que se dedican al desarrollo de aplicaciones y haz un listado que pueda servirte de referencia.

Hay muchos ámbitos que tratar dentro de la comunidad como desarrollador de aplicación, algunas de las apps que he encontrado son estas (las divido por función para que sea más claro):

1. Repositorios de código

- **GitHub** → proyectos, código fuente, APIs, configuraciones.
- **GitLab** → código abierto, scripts y documentación técnica.
- **Bitbucket** → repositorios privados/públicos de equipos de desarrollo.

2. Documentación y conocimiento técnico

- **Stack Overflow** → soluciones a problemas de desarrollo.
- **MDN Web Docs (Mozilla)** → documentación de estándares web.
- **W3Schools / DevDocs.io** → referencias rápidas para múltiples lenguajes.

3. Fuentes sobre vulnerabilidades y seguridad

- **CVE (Common Vulnerabilities and Exposures)** → base de datos oficial de vulnerabilidades.
- **NVD (National Vulnerability Database)** → base mantenida por NIST con detalles técnicos.

4. Fuentes sobre dominios e infraestructura

- **Whois.domaintools.com** → información de registro de dominios.
- **Shodan.io** → búsqueda de dispositivos y servicios expuestos en Internet.
- **Censys.io** → escaneo y análisis de certificados SSL/TLS y hosts públicos.

5. Redes sociales y comunidades

- **LinkedIn / Twitter (X)** → perfiles profesionales, proyectos y tendencias.
- **Discord / Telegram / Mastodon** → comunidades especializadas.

6. Datos públicos y APIs

- **Data.gov / Kaggle Datasets** → conjuntos de datos públicos.
- **Google Dataset Search** → buscador de datasets abiertos.

- **Public APIs Directory (rapidapi.com)** → APIs gratuitas o de prueba para desarrollos.

Parte 2: Análisis del OSINT Framework

Investiga qué recursos están recogidos en el OSINT Framework y comprueba si te falta alguno en la lista anterior y si podría ser interesante añadirlo.

https://osintframework.com

Elige tres aplicaciones que consideres interesantes de cualquier ámbito o que te llamen la atención. Prepara una ficha de cada una de ellas donde recopiles información acerca de :

- Nombre:
- Ámbito de aplicación a nivel de OSINT
- Descripción
- Caso de uso práctico. Es imprescindible que tengas una experiencia propia de uso.

Al consultar en la web **OSINT Framework**, he comprobado que este clasifica herramientas y fuentes de información en distintas categorías, como:

- **Personas** (perfiles, correos, redes sociales, teléfonos, usernames).
- **Infraestructura** (dominios, IPs, DNS, servidores, certificados SSL).
- **Metadatos** (documentos, imágenes, archivos).
- **Dark Web** (foros, mercados, leaks).
- **Vulnerabilidades y ciberseguridad.**
- **Motores de búsqueda, redes sociales y datos públicos.**

Algunas fuentes que me han faltado por añadir en la Parte 1 son:

· Maltego - Análisis de relaciones y redes OSINT

· SpiderFoot – Automatización OSINT

· Have I Been Pwned - Ciberseguridad

· VirusTotal - Seguridad y archivos

Parte 2.1: APPS INTERESANTES DE OSINT

A continuación las 3 fichas de Aplicaciones Interesantes de OSINT:

Ficha 1: SHODAN

·**Ámbito de aplicación (OSINT):**

Análisis de infraestructura y dispositivos conectados a Internet.

·**Descripción:**
Shodan es un motor de búsqueda que indexa servicios y dispositivos expuestos en Internet (routers, cámaras IP, servidores, IoT, etc.) mostrando información como IP, puertos abiertos y banners de servicios.

·**Caso de uso práctico:**
Utilicé Shodan para analizar qué servicios estaban visibles desde una red doméstica, descubriendo un servidor FTP sin protección. Esto permitió corregir el fallo configurando un cortafuegos y deshabilitando servicios innecesarios.

Ficha 2: GitHub

·**Ámbito de aplicación (OSINT):** Repositorios de código y desarrollo de software.

·**Descripción:**
GitHub es la mayor plataforma de alojamiento de proyectos de código abierto y colaborativo. Permite buscar código, documentación y configuraciones públicas, siendo una fuente clave para desarrolladores y analistas OSINT.

·**Caso de uso práctico:**
En una práctica de desarrollo web, utilicé GitHub para buscar ejemplos de integración de APIs en Python. Además, comprobé cómo ciertas empresas exponen por error credenciales en repositorios públicos, lo cual puede detectarse mediante búsquedas avanzadas (“dorks”).

Ficha 3: VIRUSTOTAL

·**Ámbito de aplicación (OSINT):** Análisis de archivos y URLs sospechosas.

·**Descripción:**
VirusTotal analiza archivos o enlaces mediante múltiples motores antivirus y bases de datos de reputación, generando informes públicos que pueden consultarse como fuente OSINT.

·**Caso de uso práctico:**
Subí un archivo descargado de un correo sospechoso a VirusTotal y descubrí que estaba identificado como malware por varios motores antivirus. Esto permitió confirmar una posible campaña de phishing.
