PRODUCT REQUIREMENTS DOCUMENT (PRD)

Product name: DomainDive

Document version: 1.0

Last Updated: June 20 2025

Owner: Cycops business solutions

Executive Summary

This document outlines the Product Requirements Document (PRD) for an innovative web/app designed as an automated Open Source Intelligence (OSINT) tool. Its core purpose is to provide individuals and organizations with a secure, comprehensive overview of their public digital footprint by taking a given domain, automatically collecting publicly available data (including WHOIS, DNS records, and subdomains), and presenting it in visually engaging graphs and charts. The compiled information, encompassing both raw data and visualizations, is then securely delivered as a password-protected PDF report. The PRD serves as the essential blueprint guiding the development, ensuring this application precisely meets its objectives of delivering accurate, actionable, and secure domain intelligence.

USERS

- **Cybersecurity Analysts** – to assess the security posture of a domain, identify subdomains, and detect potential vulnerabilities or threats.

- **Penetration Testers / Ethical Hackers** – to gather domain-related intelligence during the reconnaissance phase of security testing.

- **Incident Response Teams** – to investigate domains involved in cyber incidents or suspected malicious activity.

- **Law Enforcement & Cybercrime Units** – to track domain ownership and related infrastructure during digital forensics and cybercrime investigations.

- **IT Administrators / Network Security Teams** – to monitor and audit their own domain infrastructure for unauthorized or forgotten subdomains.

- **Researchers / OSINT Investigators** – to gather intelligence on domains of interest from publicly available sources.

- **Private Investigators / Journalists** – who may use OSINT data as part of investigative reporting or background checks.

GOALS

- **Simplify Domain Ownership Lookup**
  Enable users to easily retrieve domain ownership and registration details using WHOIS data, including registrar information, creation/expiry dates, and contact records.

- **Enable Breach Data Search**
  Integrate functionality to allow users to check if email addresses associated with the domain have appeared in known data breaches, using open breach databases or APIs like *Have I Been Pwned*.

- **Provide Exportable Reports**
  Allow users to export all collected intelligence, visualizations, and summaries into a structured, password-protected PDF file for offline access, sharing, and record-keeping.

MAIN FEATURES OF THE APP

FEATURE 1: DOMAIN/WHOIS LOOKUP

- **Purpose:** To gather comprehensive publicly available information about a specific domain name.

FEATURE 2: SEARCH FOR EMAIL LEAKS

- **Purpose:** To check if a given email address has been compromised in known data breaches.

FEATURE 3: EXPORT RESULTS AS REPORT

- **Purpose:** To allow users to securely save and share the gathered OSINT information in a structured document format.

STEP-BY-STEP DISPLAY

Step 1: Report Displayed & Export Button Available

After the domain information gathering is complete, the report is visible, and the "Export as PDF" button is active.

```
-----------------------------------------------------------------------
|                         OSINT Web App                               |
|---------------------------------------------------------------------|
|  < Back to Search                                                   |
|---------------------------------------------------------------------|
|                                                                     |
|  **OSINT Report for example.com** |
|                                                                     |
|  **Overview** |
|  Target Domain: example.com                                         |
|  Scan Date: 2025-07-01 11:30 AM                                     |
|                                                                     |
|  **WHOIS Information** [v]                                          |
|  - Registrant: Example Inc.                                         |
|  - Registrar: DomainRegistrar.com                                   |
|  - Creation Date: 1995-08-14                                        |
|  ...                                                                |
|                                                                     |
|  **DNS Records** [v]                                                |
|  - A: 93.184.216.34                                                 |
|  - MX: mail.example.com (Priority 10)                               |
|  ...                                                                |
|                                                                     |
```

```
|  **Website Technologies** [v]                                        |
|  - Web Server: Nginx                                                 |
|  - Analytics: Google Analytics                                       |
|  ...                                                                 |
|                                                                      |
|  [ Export as PDF ]                                                   |
|                                                                      |
------------------------------------------------------------------------
```

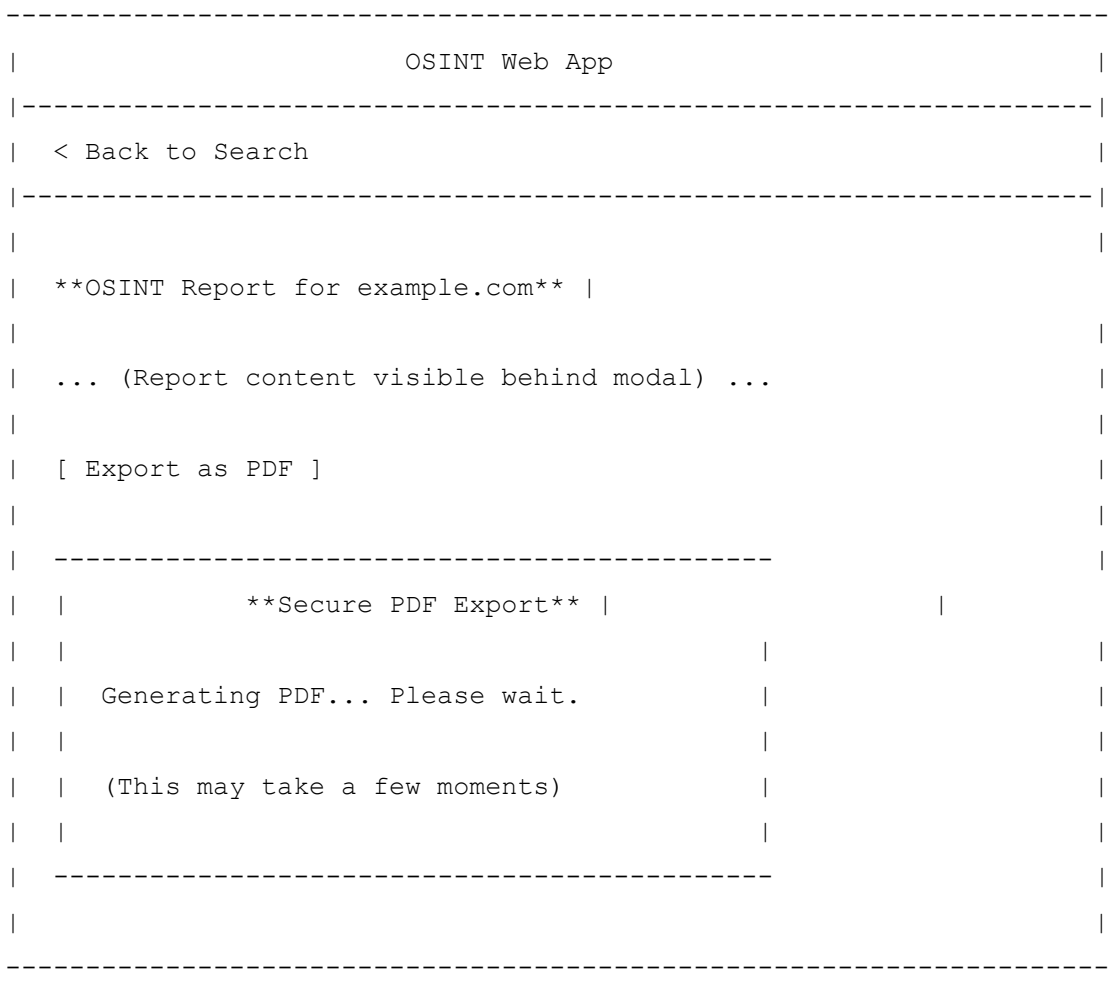
Step 2: User Clicks "Export as PDF" - Password Prompt Appears

A modal window or overlay appears, asking for the password.

```
------------------------------------------------------------------------
|                        OSINT Web App                                 |
|----------------------------------------------------------------------|
|  < Back to Search                                                    |
|----------------------------------------------------------------------|
|                                                                      |
|  **OSINT Report for example.com** |
|                                                                      |
|  ... (Report content visible behind modal) ...                       |
|                                                                      |
|  [ Export as PDF ]                                                   |
|                                                                      |
|  ---------------------------------------------                       |
|  |           **Secure PDF Export** |                    |
|  |                                              |                    |
|  |  Please enter a password for your PDF:       |                    |
|  |  Password: [_____________________]           |                    |
|  |  Confirm:  [_____________________]           |                    |
|  |                                              |                    |
|  |  [ Cancel ] [ Generate Secure PDF ]          |                    |
|  ---------------------------------------------                       |
|                                                                      |
------------------------------------------------------------------------
```

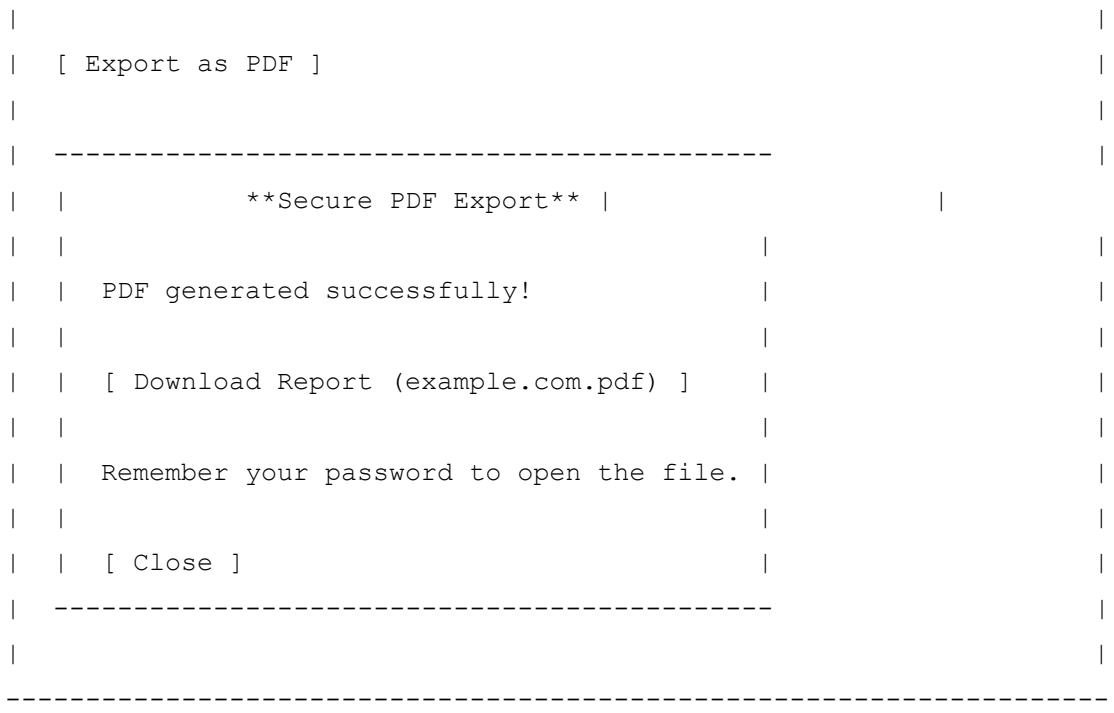
Step 3: Password Entered & PDF Generation Initiated

The user enters the password, and the "Generate Secure PDF" button is clicked. The modal might show a "Generating..." state.



Step 4: PDF Ready for Download

Once the PDF is generated and secured, a download link is provided.



OVERVIEW

This chapter describes the technical tools, third-party APIs, data storage, hosting configuration, and architecture to construct our security web application. The account is simple and easy and is appropriate for developers and stakeholders alike.

Frameworks & Tools for Optional Development

Python : Data handling, APIs, and main backend logic.

Streamlit :A Python frontend framework for making interactive web user interfaces.

HTML/CSS :When Streamlit is required for small-scale interface customization.

Integration of OSINT Tools and APIs

What we're talking about WhatWeb Outlines tech stack, CMS and plugins from site URL/domain Tech stack, CMS, plugins WHOIS GIVES domain's reg info Domain Owner, registrar, reg date, exp date.

HaveIBeenPwned/api :

Does an email/username check for security breaches Email/username Compromise history

IntelligenceX:

Advanced OSINT into dark and archived data Keywords/domain/email Related results

Sublist3r:

Runs out a list of subs Domain Subdomains

Sherlock:

Social media profile search by username Username Social profiles 7

WebBester:

Does malware/phishing site check Domain/URL Safety grade Shodan
API Reports on IoT devices' and open ports' info IP/domain Port, service info, banner VirusTotal API Does in depth analysis of virus/malware in a file/URL File/URL Security report Spiderfoot (optional) Full automation of OSINT process Domain/IP Vulnerabilities Google Dorking (basic) Builds custom Google search queries Custom strings .

INFORMATION STORAGE ARCHITECTURE

User input logs capture domain and email address searches. This information is captured within MongoDB and created in JSON or free-form text formats. Through APIs, both OSINT processed and raw results are returned to users in JSON format. These API outputs are either temporarily cached in SQLite or permanently stored in MongoDB.

EXAMPLE API REQUEST:

HaveIBeenPwned User Types: example@gmail.com

↓

API Call: GET https://haveibeenpwned.com/api/v3/breachedaccount/example@gmail.com

↓

Headers: { "hibp-api-key": "YOUR_API_KEY" }

↓

Response: [{ breach: Adobe, date: 2013, compromised: email, password }, ...]

↓

Displayed in UI formatted

MILESTONES

PHASE	DURATION	AGENDA
Phase 1	2 weeks	requirements gathering, documentation, developing Scoring engine
Phase 2	2 weeks	local environment setup, GitHub environment setup , front-end, Dashboard UI designing
Phase 3	3 weeks	back-end database integration, database testing, API integration
Phase 4	4 weeks	UAT, testing, launch