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.

How PRD contributes towards the APP:

For this OSINT-based domain analysis application, the PRD outlines the **core functionality**, such as accepting a domain name, collecting public data using tools like WHOIS and Sublist3r, generating visualizations, and exporting the results into a password-protected PDF. It defines **user requirements**, such as ease of input, clarity of reports, and secure access to output, as well as **technical requirements** like integration with data visualization libraries and PDF generation tools.

The PRD helps ensure all stakeholders—including developers, designers, and product managers—are aligned on the **scope, priorities, and constraints** of the project. It also serves as a **baseline for testing and validation**, ensuring that the final product meets both functional expectations and security standards.

Why is PRD essential:

A **Product Requirements Document (PRD)** is vital for this app because it clearly defines the application's **purpose, features, and technical scope**, ensuring all stakeholders are aligned throughout the development lifecycle. This OSINT-based application is designed for tasks such as **verifying domain ownership** using tools like WHOIS, **investigating cybercrime** by collecting and analyzing data on suspicious domains and subdomains, and **gathering intelligence from open sources** to support cybersecurity assessments.

The PRD helps outline each of these use cases, specifying how the app should accept domain input, extract public data, generate visual representations (graphs and pie charts), and securely export findings in a password-protected PDF. It ensures that functionality, security measures, and usability standards are well-documented and followed, making the PRD a **critical blueprint** for building an effective, reliable, and secure application.

KEY ELEMENTS IN A PRD INCLUDE:

- **Product purpose and objectives**
- **Target audience or users**
- **Features and functionalities**
- **User flows or use cases**
- **Assumptions and constraints**
- **Acceptance criteria**

The PRD serves as a **communication bridge** between business needs and technical implementation, guiding the team throughout the development lifecycle.

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.

- **Description:** This feature allows users to input a domain name (e.g., example.com) and retrieve essential details. It performs a WHOIS lookup to get registration information (registrant, registrar, creation/expiration dates, name servers) and fetches DNS records (A, AAAA, MX, NS, TXT, SPF) to identify associated IP addresses, mail servers, and other configurations. It also includes subdomain enumeration and identifies associated IP addresses.

- **How it Works (Step-by-Step):**
  - The user accesses the application's input section.
  - The user enters a target domain name (e.g., example.com) into the provided field.
  - The user clicks "Gather Information" or "Start Scan."
  - The application's backend automatically queries various public OSINT sources, performing:
    - **WHOIS Lookup:** Retrieving domain registration details.
    - **DNS Records:** Fetching A, MX, NS, TXT records.
    - **Subdomain Enumeration:** Discovering associated subdomains.
    - **Associated IP Addresses:** Identifying IPs linked to the domain/subdomains.
    - **Website Technology Identification:** Detecting web technologies (e.g., CMS, server).
  - A loading indicator shows data is being collected.
  - Upon completion, results are prepared for display.

FEATURE 2: SEARCH FOR EMAIL LEAKS

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

- **Description:** Users can enter an email address into the application. The system will then query public data breach databases (e.g., similar to HaveIBeenPwned) to determine if that email address, or any associated credentials, has been exposed in past security incidents. The results will indicate if the email was found in a breach and provide details about the breach if available.

- **How it Works (Step-by-Step):**
  - The user navigates to the "Email Leak Search" section of the app.
  - An input field prompts the user to "Enter Email Address."
  - The user types the desired email address (e.g., user@example.com).
  - The user clicks a "Check for Leaks" button.
  - The application sends a query to a public data breach API (e.g., HaveIBeenPwned).
  - The results are displayed, indicating if the email was found in any breaches, and if so, listing the breach names and dates.
  - A message will confirm if no breaches were found for the entered email address.

FEATURE 3: EXPORT RESULTS AS REPORT

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

- **Description:** After any scan or lookup is completed, the application generates an interactive report displaying all collected data. Users will have the option to export this report. A key functionality is the ability to convert the report into a password-protected PDF document, ensuring confidentiality. Other export formats like JSON, CSV, or plain text could also be made available.

- **How it Works (Step-by-Step):**
  - After any scan or lookup is completed and its report is displayed on the screen, an "Export as PDF" button becomes available.
  - The user clicks the "Export as PDF" button.
  - A modal dialog or inline form appears, prompting the user to "Enter a password for the PDF report." It will also include a "Confirm Password" field.
  - The user enters and confirms their desired password.
  - The user clicks a "Generate Secure PDF" button within the modal.

- The application's backend (or a client-side library if feasible and secure) takes the content of the displayed report.
- It converts this content into a PDF document.
- Crucially, it then applies the user-provided password encryption to the PDF, ensuring that the document cannot be opened without the correct password.
- A download link for the password-protected PDF file is then provided to the user.

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.

```
---------------------------------------------------------------------
|                        OSINT Web App                              |
|-------------------------------------------------------------------|
|  < Back to Search                                                 |
|-------------------------------------------------------------------|
|                                                                   |
|  **OSINT Report for example.com** |
|                                                                   |
|  ... (Report content visible behind modal) ...                    |
|                                                                   |
|  [ Export as PDF ]                                                |
|                                                                   |
|  ---------------------------------------------                    |
|  |           **Secure PDF Export** |                    |
|  |                                           |                    |
|  |  Generating PDF... Please wait.           |                    |
|  |                                           |                    |
|  |  (This may take a few moments)            |                    |
|  |                                           |                    |
|  ---------------------------------------------                    |
|                                                                   |
---------------------------------------------------------------------
```

Step 4: PDF Ready for Download

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

```
---------------------------------------------------------------------
|                        OSINT Web App                              |
|-------------------------------------------------------------------|
|  < Back to Search                                                 |
|-------------------------------------------------------------------|
|                                                                   |
|  **OSINT Report for example.com** |
|                                                                   |
|  ... (Report content visible behind modal) ...                    |
|                                                                   |
|  [ Export as PDF ]                                                |
|                                                                   |
|  ---------------------------------------------                    |
|  |           **Secure PDF Export** |                     |
|  |                                           |                    |
|  |  PDF generated successfully!              |                    |
|  |                                           |                    |
|  |  [ Download Report (example.com.pdf) ]    |                    |
|  |                                           |                    |
|  |  Remember your password to open the file. |                    |
|  |                                           |                    |
|  |  [ Close ]                                |                    |
|  ---------------------------------------------                    |
|                                                                   |
---------------------------------------------------------------------
```

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 AND TIMELINE

Phase 1: requirements gathering, documentation, developing Scoring engine (2 weeks)

Phase 2: local environment setup, GitHub environment setup , front-end, Dashboard UI designing (2 weeks)

Phase 3: back-end database integration, database testing, API integration (3 weeks)

Phase 4: UAT, testing, launch (4 weeks)