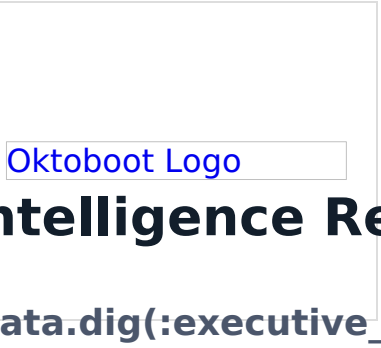
# Tech_Test

## Report Metadata

| | |
|---|---|
| **Generated By:** | PDF Report Generator |

## Executive Summary




# Threat Intelligence Report

## <%= @report_data.dig(:executive_summary, :targets_scope) || "Unspecified Domain" %>

**Created At:** <%= @report_data[:created_at]&.to_s || "N/A" %>
**Updated At:** <%= @report_data[:updated_at]&.to_s || "N/A" %>

## Report Metadata

| | |
|---|---|
| **Version:** | <%= @report_data.dig(:report_metadata, :report_version) \|\| "N/A" %> |
| **Generated By:** | <%= @report_data.dig(:report_metadata, :generated_by) \|\| "N/A" %> |
| **Generated At:** | <%= @report_data.dig(:report_metadata, :generated_at) \|\| "N/A" %> |

## Executive Summary

**Overview:** <%= overview %>

**Scope:** <%= targets %>

Subdomains

**<%= subdomains %>**

Exposed Assets

**<%= assets %>**

Leaked Credentials

**<%= leaks %>**

# Methodology

## <%= category %>

Status: <%= task[:status] %>

<%= task[:description] %>

# Domain & DNS Intelligence

## Domains

**Total Domains Identified:** <%= dns_info[:domains] || 0 %>

## DNS Records

### NS Records

| Name | IP |
| --- | --- |
| <%= rec[:name] %> | <%= rec[:ip] %> |

<%= dns_summary[:ns_note] %>

### MX Records

| Name | IP |
| --- | --- |
| <%= rec[:name] %> | <%= rec[:ip] %> |

<%= dns_summary[:mx_note] %>

## WHOIS Records

| Domain | Registrar | Created | Updated | Expires |
| --- | --- | --- | --- | --- |
| <%= w[:domain_name] \|\| "N/A" %> | <%= w[:registrar] \|\| "N/A" %> | <%= w[:creation_date] \|\| "N/A" %> | <%= w[:updated_date] \|\| "N/A" %> | <%= w[:expiration_date] \|\| "N/A" %> |

<%= dns_info[:whois_note] %>

# Network Infrastructure

## AS Number Overview

**Total ASNs Identified:** <%= network[:asn_count] %>

## Shared Hosting Exposure

| Domain | Shared With |
| --- | --- |
| <%= host[:domain] %> | <% host[:shared_with].each do \|shared\| %> <%= shared %> <% end %> <% if host[:shared_with_truncated] %> *(truncated)* <% end %> |

<%= shared_summary[:note] %>

# Subdomain Enumeration

This section highlights a sample of the subdomains identified during the reconnaissance process. The full list — along with associated technologies, open ports, and vulnerabilities — is available in the Oktoboot dashboard for deeper investigation and remediation.

**Total Unique Subdomains Found:** <%= subdomains[:total_found] %>

| Root Domain | Subdomain |
| --- | --- |
| <%= index.zero? ? root : "" %> | <%= sd %> |

<%= subdomains[:note] %>

## Certificate HTTPS Enumeration

This section summarizes digital certificates discovered during reconnaissance. Certificates may reveal subdomains or exposure timelines. Review carefully — and check Oktoboot Dashboard for full details.

| Common Name | Valid From | Valid To |
| --- | --- | --- |
| <%= cert[:common_name].presence \|\| "N/A" %> | <%= cert[:valid_from].presence \|\| "N/A" %> | <%= cert[:valid_to].presence \|\| "N/A" %> <% if is_expired %> (expired)<% end %> |

Only the first 5 certificates are shown. View the Oktoboot dashboard for the full list.

# Exposed Assets Overview

These exposed assets may pose risk due to open ports, outdated services, or certificate leaks. Risk levels and recommendations are based on observed configurations and known vulnerabilities.

## <%= asset[:ip] %>

**Domain:** <%= asset[:domain].presence || "N/A" %> | **ISP:** <%= asset[:isp].presence || "N/A" %> | **Risk:** "> <%= asset[:risk_level] %>

### Open Ports

| Port | Module | Version | SSL |
| --- | --- | --- | --- |
| <%= port[:port] %> | <%= port[:module] %> | <%= port[:version].presence || "N/A" %> | <% if port[:ssl].present? %> <% port[:ssl].each do \|ssl\| %> **<%= ssl[:common_name] %>** <%= ssl[:issuer] %> \| <%= ssl[:versions] %> <% end %> <% else %> N/A <% end %> |

### Top Vulnerabilities

#### <%= vuln[:title] %>

<%= vuln[:description] %>

*Only the first 5 vulnerabilities are shown. See dashboard for more.*

### Recommended Mitigation

<%= asset[:recommendation] %>

<%= @report_data.dig(:findings, :exposed_assets, :note) %>

# Data Leaks & Credential Exposure

These exposed credentials were found across malware logs, public breaches, and combo lists. They may be linked to user accounts or internal access points. Please investigate and rotate impacted credentials immediately. Full dump available in the Oktoboot dashboard.

## Logstealer Leaks

| URL | Email | Password | Year |
| --- | --- | --- | --- |
| <%= entry[2] %> | <%= entry[0] %> | <%= entry[1] %> | <%= entry[3] %> |

<%= leaks[:logstealer_leaks][:note] %>

## Public Breach Leaks

| Leak Source | Email | Password | Year |
| --- | --- | --- | --- |
| <%= entry[2] %> | <%= entry[0] %> | <%= entry[1] %> | <%= entry[3] %> |

<%= leaks[:public_leaks][:note] %>

## Combo List Leaks

| Domain | Email | Password | Year |
| --- | --- | --- | --- |
| <%= entry[2] %> | <%= entry[0] %> | <%= entry[1] %> | <%= entry[3] %> |

<%= leaks[:combo_leaks][:note] %>

# Employee Enumeration

This section lists publicly accessible employees discovered during reconnaissance. Full role breakdowns and exposure context are available in the Oktoboot dashboard.

**Total Identified:** <%= employees[:total_found] %>

**<%= emp[:fullname] %>**

<%= emp[:poste].presence || "N/A" %>

<%= employees[:note] %>

# Metadata & Public Files

This section lists publicly accessible files and detected metadata exposures. View complete data in your Oktoboot dashboard.

## Discovered Files

| File Name | URL |
| --- | --- |
| <%= file[:name].presence \|\| "N/A" %> | <% if file[:url].present? %> <%= file[:url] %> <% else %> N/A <% end %> |

# Risk Assessment

The following risks were identified during the reconnaissance phase. They are categorized by severity and may require immediate remediation or strategic consideration.

## High Risks

- <%= risk %>

## Medium Risks

- <%= risk %>

## Informational

- <%= risk %>

# Recommendations

Prioritized guidance based on reconnaissance findings. Grouped by severity for operational clarity.

### <%= severity %> Recommendations

<%= rec[:recommendation] %>

## Overview:

## Scope:

## Subdomains

## Exposed Assets

## Leaked Credentials

## Vulnerabilities

| ID | Description | Severity | CVSS |
|---|---|---|---|

| ID | Description | Severity | CVSS |
|---|---|---|---|
| | | High | |
| CVE-2023-5678 | Cross-Site Scripting (XSS) in comment section | Medium | 6.5 |
| | | Low | |

## Network Intelligence

### Domains

### IP Ranges

### Open Ports

| IP Address | Port | Service |
|---|---|---|
| | | |
| 192.168.1.10 | 443 | HTTPS |
| | | |

# Data Leaks and Breaches

## Identified Data Leaks

| Source | Date | Type | Severity |
|---|---|---|---|
| | | | High |
| Pastebin | 2023-02-20 | Customer Data | Critical |

## Compromised Employee Accounts

| Email | Breaches | Last Breach |
|---|---|---|
| | | |
| jane.smith@example.com | 1 | 2023-01-05 |

# Risk Assessment

Risk Distribution: High (2) | Medium (2) | Low (1)

## High Risks

### Exposed Admin Interface

---

### Outdated Software

---

## Medium Risks

### Weak Password Policy

---

### Insecure Cookies

---

## Low Risks

## Missing Security Headers