Tech_Test1

example.com

Created At: April 25, 2025 at 10:53
Updated At: April 25, 2025 at 10:53

Report Metadata

Version:	1.0
Generated By:	PDF Report Generator
Generated At:	2025-04-25 10:53:44

Executive Summary

This is heading 1

This is heading 2

This is heading 3

This is heading 4

This is heading 5

This is heading 6

Overview:

This report provides a comprehensive security assessment of the target domain and identifies potential vulnerabilities and risks.

Scope:

Primary target: example.com and all subdomains

Subdomains

- api.example.com
- dev.example.com
- staging.example.com
- admin.example.com

Exposed Assets

- Web Application
- API Gateway
- Database Server
- Load Balancer

Leaked Credentials

- API Keys (GitHub)
- Customer Data (Pastebin)

Vulnerabilities

ID	Description	Severity	CVSS
CVE-2023-1234	Critical SQL Injection vulnerability in login form	High	9.8
CVE-2023-5678	Cross-Site Scripting (XSS) in comment section	Medium	6.5
CVE-2023-9012	Information disclosure in error messages	Low	3.2

Network Intelligence

Domains

- example.com
- example-staging.com
- example-dev.com

IP Ranges

- 192.168.1.0/24
- 10.0.0.0/16

Open Ports

IP Address	Port	Service
192.168.1.10	80	HTTP
192.168.1.10	443	HTTPS
192.168.1.20	22	SSH

Data Leaks and Breaches

Identified Data Leaks

Source	Date	Type	Severity
GitHub	2023-01-15	API Keys	High
Pastebin	2023-02-20	Customer Data	Critical

Compromised Employee Accounts

Email	Breaches	Last Breach
john.doe@example.com	3	2022-11-10
jane.smith@example.com	1	2023-01-05

Risk Assessment

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

High Risks

Exposed Admin Interface

Description: The admin interface is accessible from the internet without proper authentication

Recommended Mitigation: Implement IP restrictions and strong authentication

---

Outdated Software

Description: Several critical services are running outdated versions with known vulnerabilities

Recommended Mitigation: Implement a regular patching schedule

---

Medium Risks

Weak Password Policy

Description: Current password policy does not enforce sufficient complexity

Recommended Mitigation: Update password policy to require longer passwords with special characters

---

Insecure Cookies

Description: Session cookies are not using secure and httpOnly flags

Recommended Mitigation: Configure all cookies with secure and httpOnly flags

---

Low Risks

Missing Security Headers

Description: Several recommended security headers are not implemented

Recommended Mitigation: Add Content-Security-Policy and other security headers