Overview

Vulnerability Scan

2.2 Target Risk Data
2.3 Risk Breakdowns

This report contains the discovered potential risks for each target that was scanned as part of this scan. This report details the discovered potential risks from these scans. Risks have been classified based on their level of threat and degree of potential harm they may pose.

Details are shown about each risk found by the scan.

Open TCP Port: 443 data

Description

Fully Qualified Domain Name (FQDN)

Dabbaghi-walid

1 Executive Summary

An Executive Summary is a high level summary of this report.

2. Total Risks Summary

Total Risks found by severity.

The total number of risks found for each target, by severity.

Below is the total number of risks found by severity. High risks are the most severe and should be considered first. An accepted risk is one which has been manually reviewed and classified as acceptable at this time, such as a false positive or an intentional part of the system's architecture.

Total Risks:

Target	High	Medium	Low	Accepted
Risk	High	Medium	Low	Accepted
site name	data	data	data	
Open TCP Ports				
High, TCP Port: 22 data	Medium	Low	Accepted	
nom de site	Medium	Low	Accepted	
Open TCP Port: 443 data	data	data	data	
Target	data	data	data	
nom de site				

3. Risks Breakdown

A Summary list of all detected risks.

Open TCP Ports(Title):

Open TCP Port: 22 data

Open TCP Port: 443 data

3.2 Risks Breakdown

A target represents target is a single URL, IP address, or fully qualified domain name (FQDN) that was scanned.

Threat Level

The threat level represents the estimated potential severity of a particular risk. Threat level is divided into 5 categories: Critical, High, Medium, Low and Accepted.

1.2 Report Coverage

This report includes findings for 1 target that were scanned. Each target is a single URL, IP address, or fully qualified domain name (FQDN).

Threat Level

The threat level represents the estimated potential severity of a particular risk. Threat level is divided into 5 categories: Critical, High, Medium, Low and Accepted.

4. Glossary

A glossary.

Vulnerable Target

data

Vulnerability Categories

CVSS Score

data

The CVSS 3.0 score is a global standard for evaluating vulnerabilities with a 0 to 10 scale. CVSS maps to threat levels: 0.1 - 4.9 = Low, 5 - 8.5 = Medium, 8.6 - 10 = High

Open TCP Ports

A fully qualified domain name is a complete domain name for a specific website or service on the Internet. This includes not only the website or service name, but also the top-level domain name. For example, www.example.com is an FQDN. Port 80 to serve websites over http and port 443 to serve websites over https. For a list of commonly used ports see https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.

An unexpected open port could give unintended access to applications, data, and private networks. Open ports can also be dangerous when expected services are out of date and exploited through security vulnerabilities.