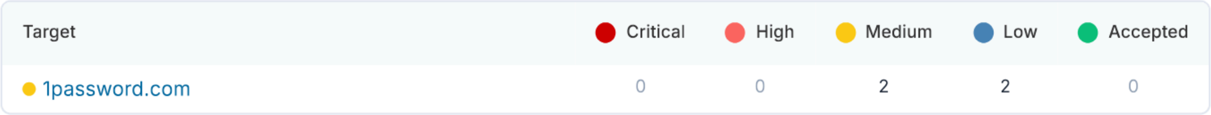
Assignment_1_Module_3

Topic: Vulnerability Assessment Report
Scan Date: June 4, 2025
Tool Used: HostedScan OWASP Vulnerability Scanner
Target: https://1password.com

A vulnerability scan was conducted on the domain `1password.com` using HostedScan's OWASP security scanner. The assessment aimed to detect potential vulnerabilities by scanning for open TCP ports and other security exposures. The scan identified 4 vulnerabilities in total, categorized into 2 Medium and 2 Low severity issues. No Critical or High risk vulnerabilities were found.

Targets Summary

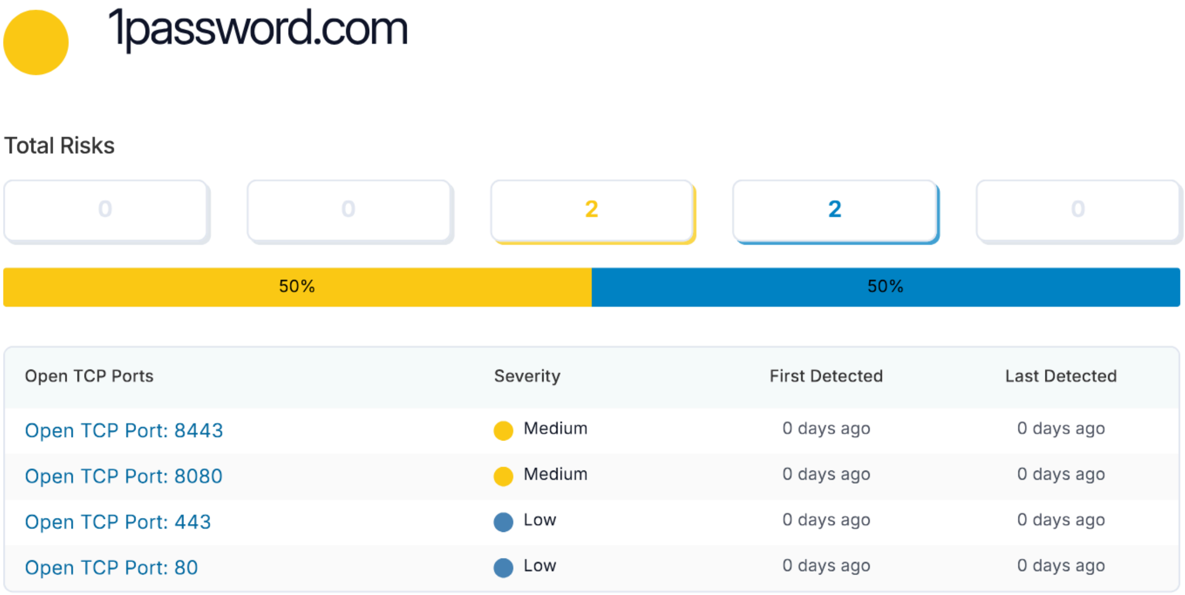
The number of potential vulnerabilities found for each target by severity.



Target	● Critical	● High	● Medium	● Low	● Accepted
● 1password.com	0	0	2	2	0

Target Breakdowns

Details for the potential vulnerabilities found for each target by scan type.



1password.com

Total Risks

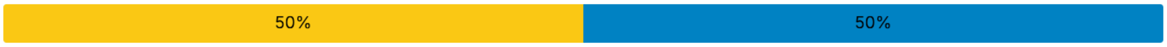
0	0	2	2	0

Open TCP Ports	Severity	First Detected	Last Detected
Open TCP Port: 8443	● Medium	0 days ago	0 days ago
Open TCP Port: 8080	● Medium	0 days ago	0 days ago
Open TCP Port: 443	● Low	0 days ago	0 days ago
Open TCP Port: 80	● Low	0 days ago	0 days ago

Total Vulnerabilities

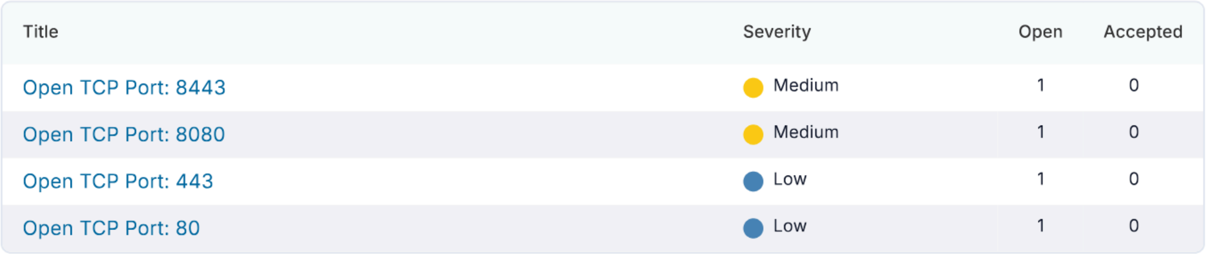
Total number of vulnerabilities found by severity.

Critical	High	Medium	Low	Accepted
0	0	2	2	0



Vulnerabilities Breakdown

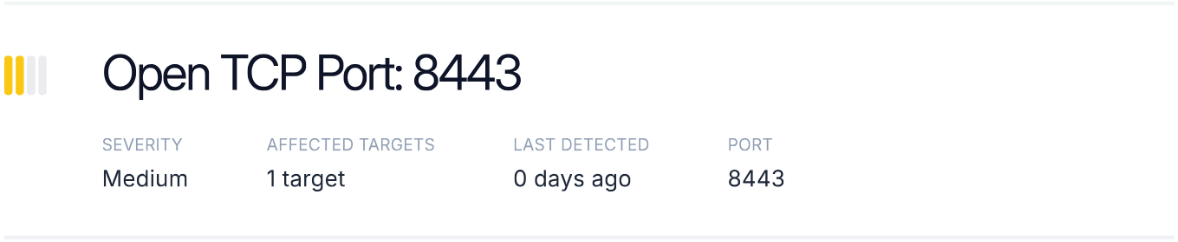
Summary list of all detected vulnerabilities.



Title	Severity	Open	Accepted
Open TCP Port: 8443	● Medium	1	0
Open TCP Port: 8080	● Medium	1	0
Open TCP Port: 443	● Low	1	0
Open TCP Port: 80	● Low	1	0

Vulnerability Details

Detailed information about each potential vulnerability found by the scan.

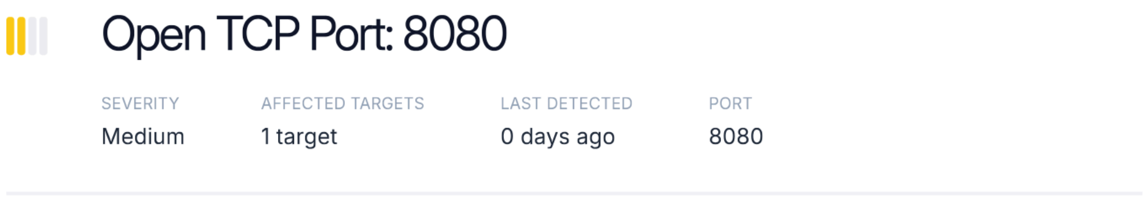


Open TCP Port: 8443

SEVERITY	AFFECTED TARGETS	LAST DETECTED	PORT
Medium	1 target	0 days ago	8443

Description

An open port may be an expected configuration. For example, web servers use 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.

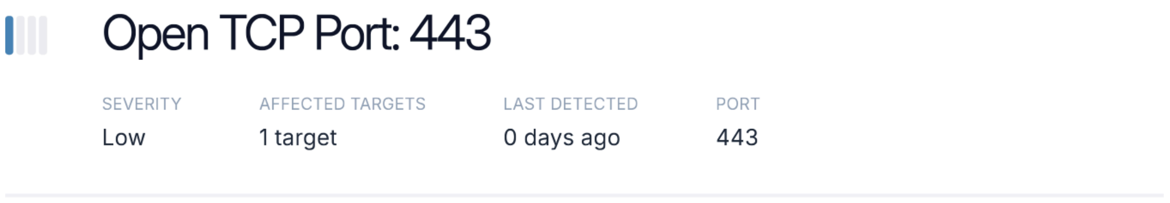


Open TCP Port: 8080

SEVERITY	AFFECTED TARGETS	LAST DETECTED	PORT
Medium	1 target	0 days ago	8080

Description

An open port may be an expected configuration. For example, web servers use 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.



Open TCP Port: 443

SEVERITY	AFFECTED TARGETS	LAST DETECTED	PORT
Low	1 target	0 days ago	443

Description

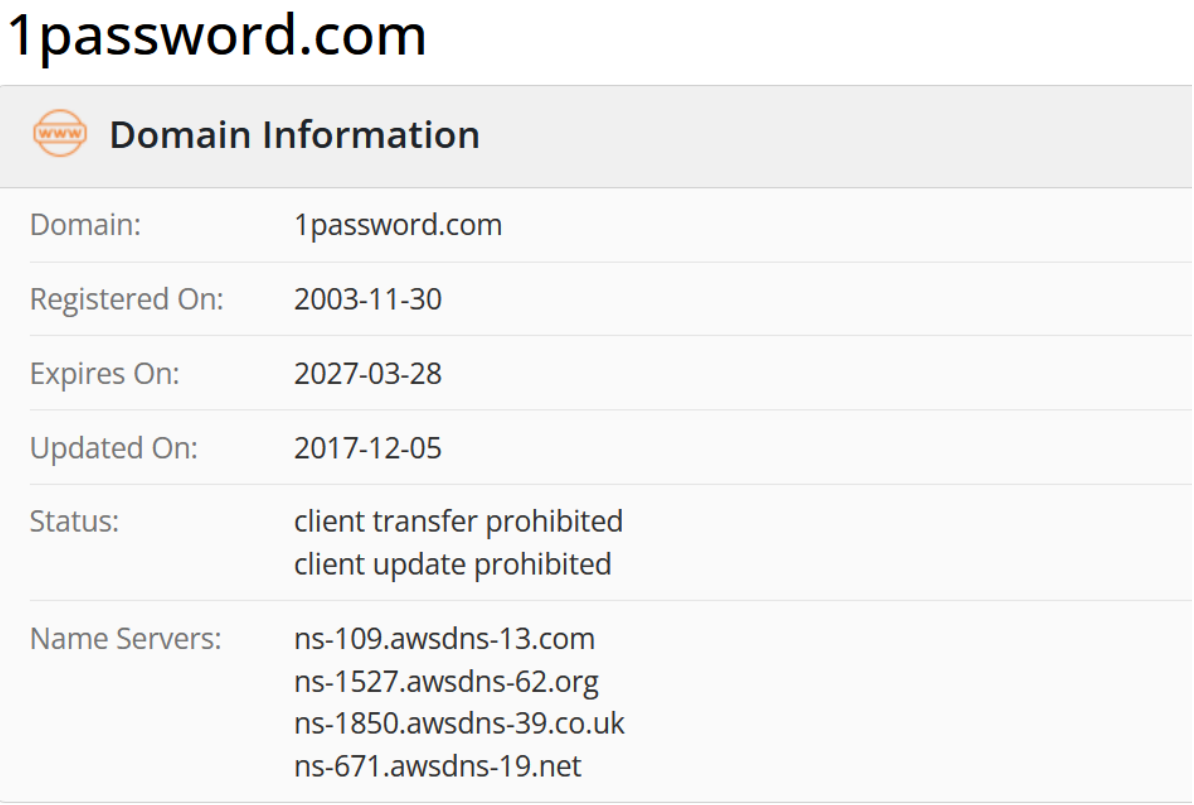
An open port may be an expected configuration. For example, web servers use port 80 to serve websites over http and port 443 to serve websites over https. For a list of commonly used ports see https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers. An unexpected open port could give unintended 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.

The scan results from HostedScan revealed minor but notable exposures in the form of open TCP ports on `1password.com`. While no critical threats were identified, medium-severity issues suggest that further review of active services and network configurations is recommended to minimize any potential risks.

Others Tools Like Whois.com, Shudan.com , crt.com :

In this time, I’m using Whois.com :

Domain Information:

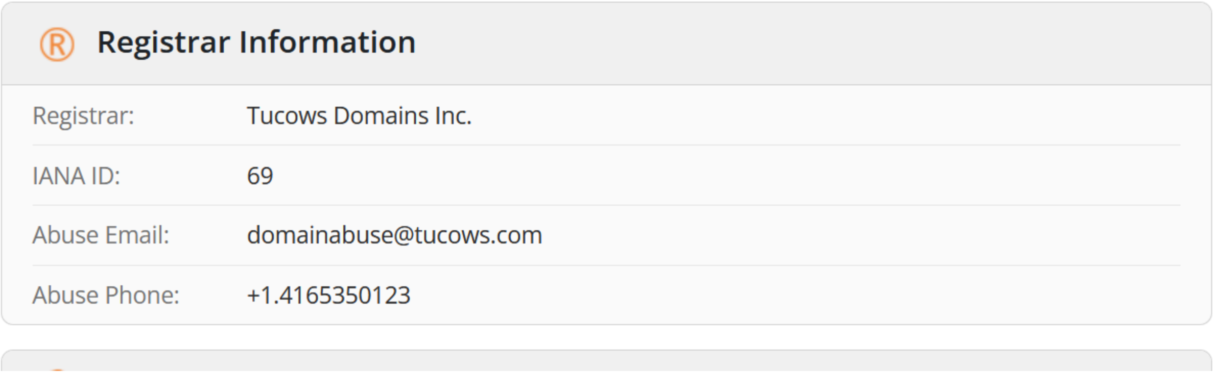


1password.com

Domain Information

Domain:	1password.com
Registered On:	2003-11-30
Expires On:	2027-03-28
Updated On:	2017-12-05
Status:	client transfer prohibited client update prohibited
Name Servers:	ns-109.awsdns-13.com ns-1527.awsdns-62.org ns-1850.awsdns-39.co.uk ns-671.awsdns-19.net

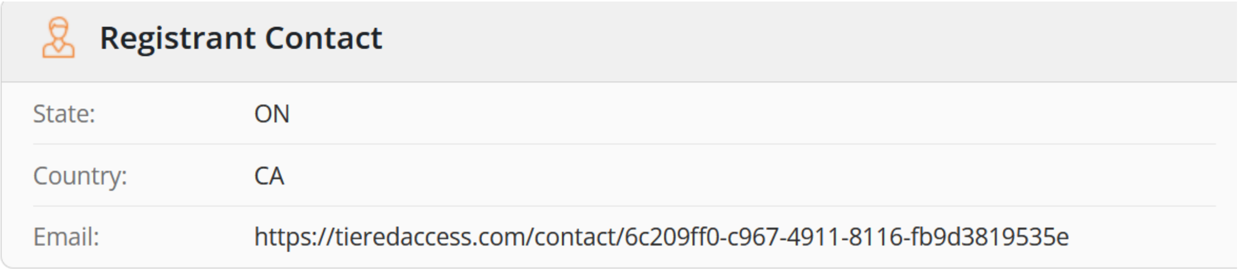
Registrar Information:



Registrar Information

Registrar:	Tucows Domains Inc.
IANA ID:	69
Abuse Email:	domainabuse@tucows.com
Abuse Phone:	+1.4165350123

Registrant Contact:



Registrant Contact

State:	ON
Country:	CA
Email:	https://tieredaccess.com/contact/6c209ff0-c967-4911-8116-fb9d3819535e

The vulnerability assessment on 1password.com was performed using two tools — HostedScan and Whois.com — to gather a comprehensive view of the domain's security posture. Both tools provided consistent insight into the system's exposure points and potential vulnerabilities.