Organizational Security Management Platform

Auther: Phanukorn Khumsalut
Adviser: Noparut Vanitchanant, Ph.D.
Company: TCC Technology Co., Ltd.

Abstract

This report is a part of a cooperative education project focusing on the development of an Organizational Security Management Platform. The objective of this project is to integrate various security products used by the team, along with open-source solutions and data from other teams, in the organization into a unified platform to enhance data correlation and analysis. The primary goal is to consolidate information on security products and solutions for improved organizational security management.

In developing of the platform, the following tasks are performed: 1. identifying subdomain discovery tools 2. performing subdomain scans and data collection 3. organizing data in Google Sheets 4. creating a PostgreSQL database. 5. identifying vulnerability assessment tools 6. conducting scans on target systems and storing the results in the database.

The project resulted in the discovery of hundreds of significant subdomains using tools such as theHarvester and Amass, which provided comprehensive and efficient results without brute force techniques. Additionally, Bighuge BLS OSINT Tool, an OSINT tool, proved the capability of the extensive subdomain data collection. Vulnerability assessments using OpenVAS and Nessus demonstrated the ability to detect various vulnerabilities, while OWASP ZAP excelled in identifying security flaws, further enhancing system security assurance.

Introduction

This project focuses on developing an Organizational Security Management Platform that integrates various security tools and open-source solutions to streamline data correlation and analysis. The platform aims to consolidate information from multiple security products, facilitating efficient subdomain discovery, vulnerability scanning, and risk assessment. By leveraging automated scanning tools and a centralized database, the system enhances the accuracy and efficiency of security monitoring, ultimately improving organizational cybersecurity in alignment with the NIST Cybersecurity Framework (CSF)

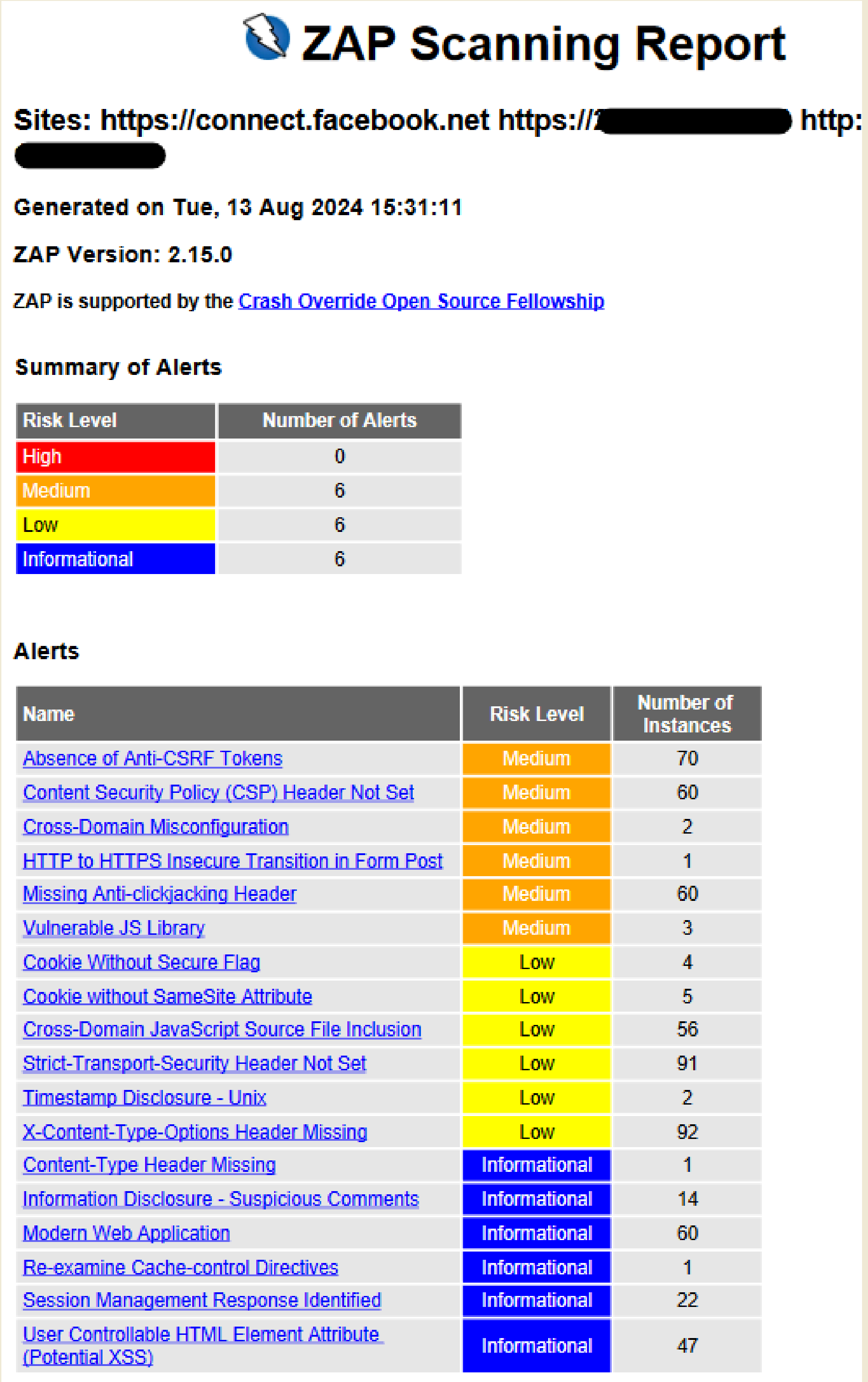
Methodology

1. Task Assignment and Tool Selection
2. Subdomain Scanning and Data Collection
3. Data Organization in Google Sheets
4. Database Creation in PostgreSQL
5. Vulnerability Assessment Tool Selection
6. Target Scanning and Data Insertion
7. Data Preparation and CSV Management
8. Database Design and Implementation

Technology

Result

The development and integration of various security tools in the organizational security management platform demonstrated significant advancements in subdomain discovery and vulnerability scanning. Tools such as Bighuge BLS OSINT Tool, Amass, and theHarvester showed varied performance in subdomain discovery, with Bighuge BLS providing the most comprehensive results. For vulnerability scanning, OWASP ZAP excelled in detecting vulnerabilities but required substantial RAM, while Nessus offered ease of use with fewer detected vulnerabilities. OpenVAS, despite installation challenges, provided a robust solution for vulnerability detection. The integration of these tools into a unified platform enhanced the organization's ability to efficiently manage cyberattack risks and make informed decisions. This approach also improved data accuracy and streamlined vulnerability management, reinforcing the organization's cybersecurity posture.



ZAP Scanning Report

Sites: https://connect.facebook.net https://[redacted] http:[redacted]

Generated on Tue, 13 Aug 2024 15:31:11

ZAP Version: 2.15.0

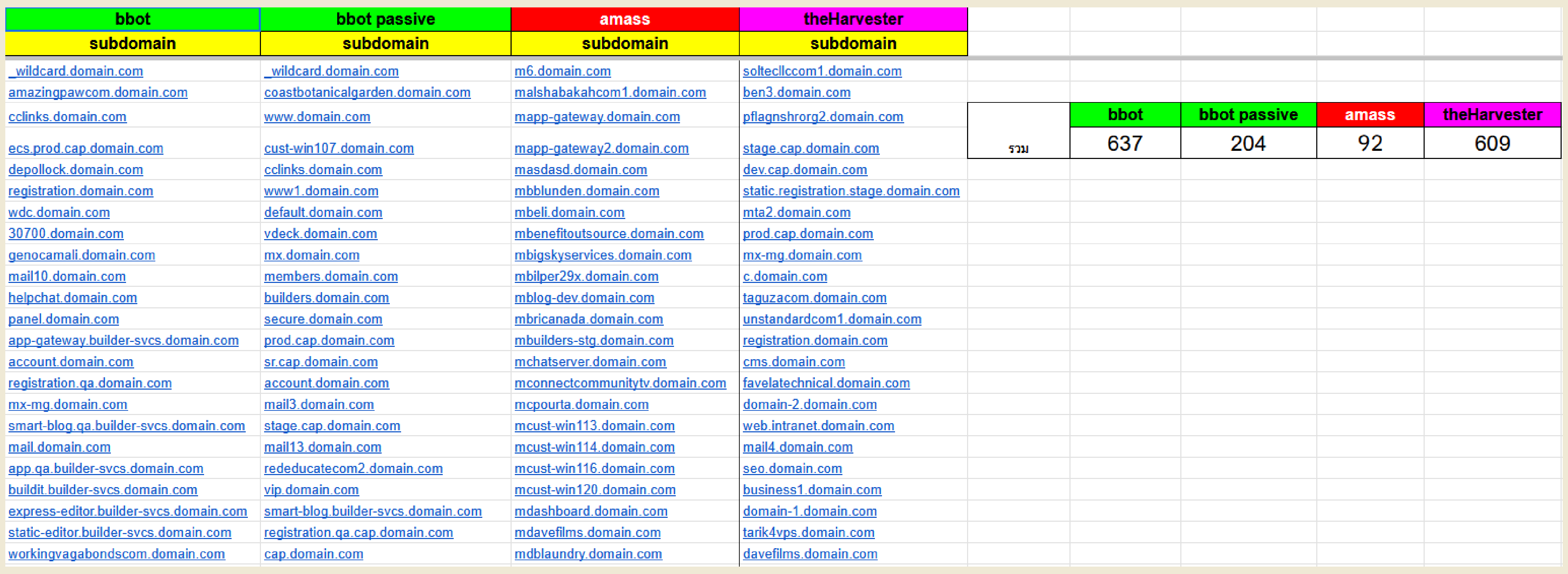
ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	6
Low	6
Informational	6

Alerts

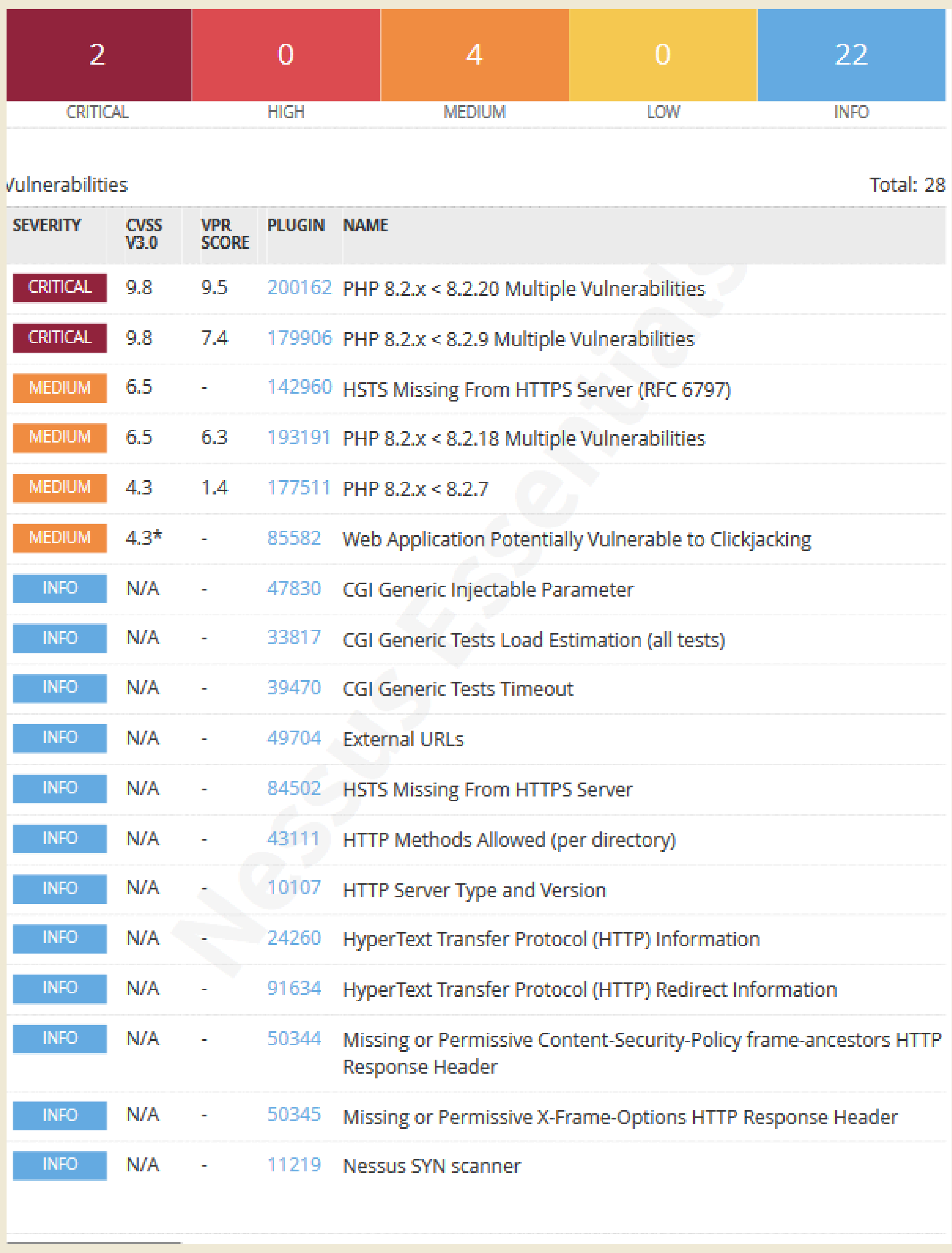
Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	70
Content Security Policy (CSP) Header Not Set	Medium	60
Cross-Domain Misconfiguration	Medium	2
HTTP to HTTPS Insecure Transition in Form Post	Medium	1
Missing Anti-clickjacking Header	Medium	60
Vulnerable JS Library	Medium	3
Cookie Without Secure Flag	Low	4
Cookie without SameSite Attribute	Low	5
Cross-Domain JavaScript Source File Inclusion	Low	56
Strict-Transport-Security Header Not Set	Low	91
Timestamp Disclosure - Unix	Low	2
X-Content-Type-Options Header Missing	Low	92
Content-Type Header Missing	Informational	1
Information Disclosure - Suspicious Comments	Informational	14
Modern Web Application	Informational	60
Re-examine Cache-control Directives	Informational	1
Session Management Response Identified	Informational	22
User Controllable HTML Element Attribute (Potential XSS)	Informational	47



bbot	bbot passive	amass	theHarvester
subdomain	subdomain	subdomain	subdomain
_wildcard.domain.com	_wildcard.domain.com	m6.domain.com	soltecllccom1.domain.com
amazingpawcom.domain.com	coastbotanicalgarden.domain.com	malshabakahcom1.domain.com	ben3.domain.com
cclinks.domain.com	www.domain.com	mapp-gateway.domain.com	pflagnshrorg2.domain.com
ecs.prod.cap.domain.com	cust-win107.domain.com	mapp-gateway2.domain.com	stage.cap.domain.com
depollock.domain.com	cclinks.domain.com	masdasd.domain.com	dev.cap.domain.com
registration.domain.com	www1.domain.com	mbblunden.domain.com	static.registration.stage.domain.com
wdc.domain.com	default.domain.com	mbeli.domain.com	mta2.domain.com
30700.domain.com	vdeck.domain.com	mbenefitoutsource.domain.com	prod.cap.domain.com
genocamali.domain.com	mx.domain.com	mbigskyservices.domain.com	mx-mg.domain.com
mail10.domain.com	members.domain.com	mbilper29x.domain.com	c.domain.com
helpchat.domain.com	builders.domain.com	mblog-dev.domain.com	taguzacom.domain.com
panel.domain.com	secure.domain.com	mbricanada.domain.com	unstandardcom1.domain.com
app-gateway.builder-svcs.domain.com	prod.cap.domain.com	mbuilders-stg.domain.com	registration.domain.com
account.domain.com	sr.cap.domain.com	mchatserver.domain.com	cms.domain.com
registration.qa.domain.com	account.domain.com	mconnectcommunitytv.domain.com	favelatechnical.domain.com
mx-mg.domain.com	mail3.domain.com	mcpourta.domain.com	domain-2.domain.com
smart-blog.qa.builder-svcs.domain.com	stage.cap.domain.com	mcust-win113.domain.com	web.intranet.domain.com
mail.domain.com	mail13.domain.com	mcust-win114.domain.com	mail4.domain.com
app.qa.builder-svcs.domain.com	rededucatecom2.domain.com	mcust-win116.domain.com	seo.domain.com
buildit.builder-svcs.domain.com	vip.domain.com	mcust-win120.domain.com	business1.domain.com
express-editor.builder-svcs.domain.com	smart-blog.builder-svcs.domain.com	mdashboard.domain.com	domain-1.domain.com
static-editor.builder-svcs.domain.com	registration.qa.cap.domain.com	mdavefilms.domain.com	tarik4vps.domain.com
workingvagabondscom.domain.com	cap.domain.com	mdblaundry.domain.com	davefilms.domain.com

	bbot	bbot passive	amass	theHarvester
รวม	637	204	92	609

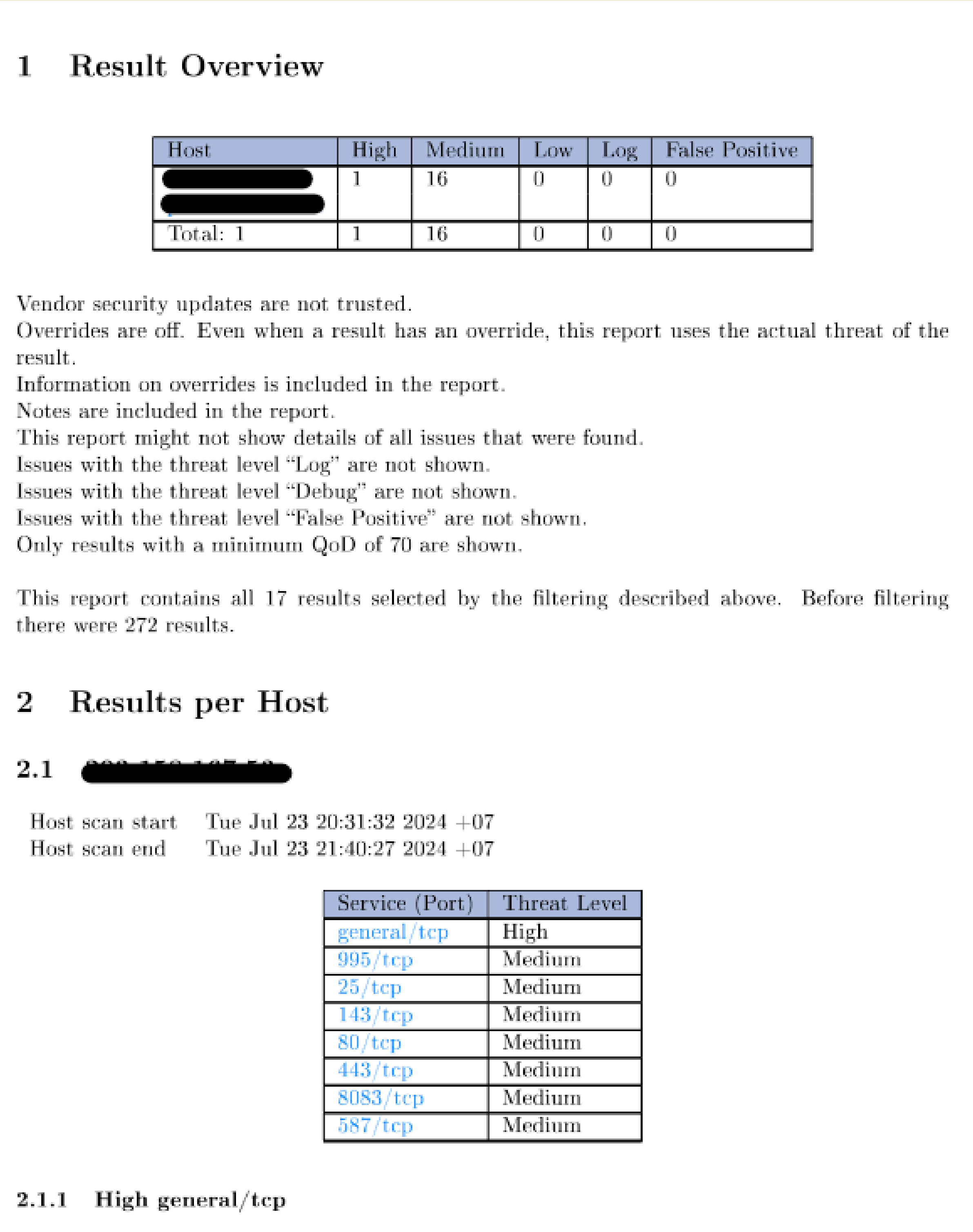
Conclusion



2	0	4	0	22
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 28

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.5	200162	PHP 8.2.x < 8.2.20 Multiple Vulnerabilities
CRITICAL	9.8	7.4	179906	PHP 8.2.x < 8.2.9 Multiple Vulnerabilities
MEDIUM	6.5	-	142960	HSTS Missing From HTTPS Server (RFC 6797)
MEDIUM	6.5	6.3	193191	PHP 8.2.x < 8.2.18 Multiple Vulnerabilities
MEDIUM	4.3	1.4	177511	PHP 8.2.x < 8.2.7
MEDIUM	4.3*	-	85582	Web Application Potentially Vulnerable to Clickjacking
INFO	N/A	-	47830	CGI Generic Injectable Parameter
INFO	N/A	-	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	-	39470	CGI Generic Tests Timeout
INFO	N/A	-	49704	External URLs
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	91634	HyperText Transfer Protocol (HTTP) Redirect Information
INFO	N/A	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	50345	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	-	11219	Nessus SYN scanner



1 Result Overview

Host	High	Medium	Low	Log	False Positive
[redacted]	1	16	0	0	0
Total: 1	1	16	0	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 17 results selected by the filtering described above. Before filtering there were 272 results.

2 Results per Host

2.1 [redacted]

Host scan start Tue Jul 23 20:31:32 2024 +07
Host scan end Tue Jul 23 21:40:27 2024 +07

Service (Port)	Threat Level
general/tcp	High
995/tcp	Medium
25/tcp	Medium
143/tcp	Medium
80/tcp	Medium
443/tcp	Medium
8083/tcp	Medium
587/tcp	Medium

2.1.1 High general/tcp

Co-operative Project, 204496 Department of Computer Science, 2024
Department of Computer Science, Faculty of Science, Chiangmai University