BASIC SCAN INFORMATION

Information

File

EECS4481-PROJECT-T5.GIT

SHA256 Hash

1A000FC454E344C245178D351874D7F772DB43105B2A147943FA9D813646D237

Total Files Scanned

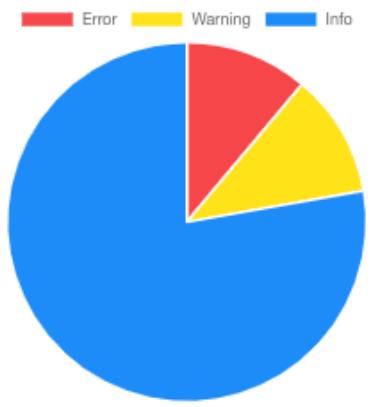
13

Types of Issues 18

Total No of Issues 20

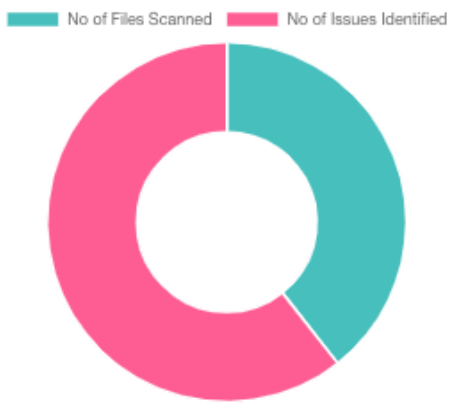
DISTRIBUTION OF SEVERITY BY ISSUE TYPES

Severity



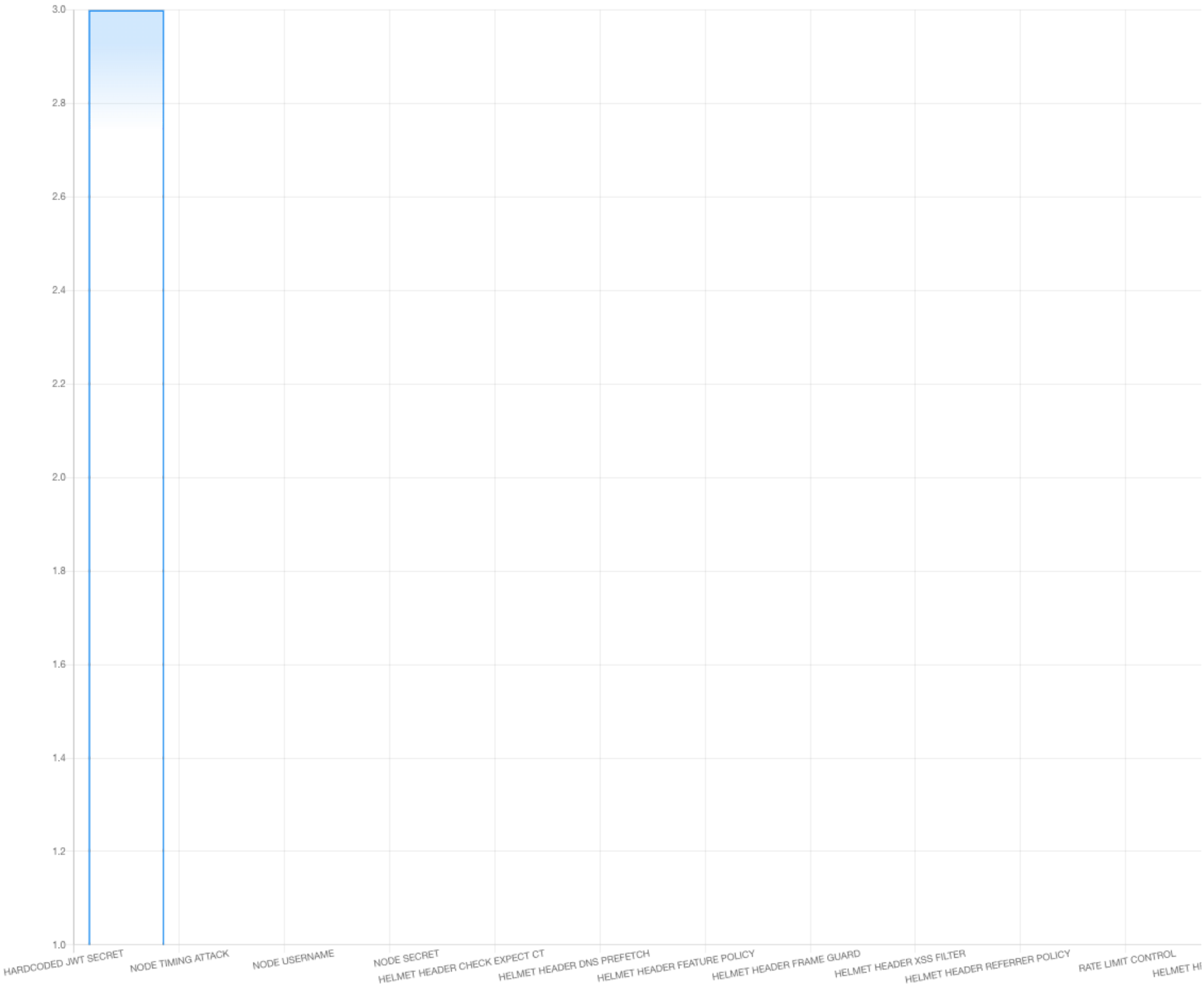
NO OF FILES SCANNED VS ISSUES IDENTIFIED

Detections



OVERVIEW OF IDENTIFIED ISSUES

Issues



SUMMARY OF FINDINGS

Findings Summary

ISSUE	DESCRIPTION	SEVERITY	STANDARDS
HARDCODED JWT SECRET	Hardcoded JWT secret was found. Store it properly in an environment variable.	ERROR	CWE-798: Use of Hard-coded Credentials
NODE TIMING ATTACK	String comparisons using '===', '!==', '!=' and '==' is vulnerable to timing attacks. More info: https://snyk.io/blog/node-js-timing-attack-ccc-ctf/	WARNING	CWE-208: Observable Timing Discrepancy
NODE USERNAME	A hardcoded username in plain text is identified. Store it properly in an environment variable.	WARNING	CWE-798: Use of Hard-coded Credentials
NODE SECRET	A hardcoded secret is identified. Store it properly in an environment variable.	ERROR	CWE-798: Use of Hard-coded Credentials
HELMET HEADER CHECK EXPECT CT	Helmet Expect CT header is not configured for this application.	INFO	CWE-693: Protection Mechanism Failure
HELMET HEADER DNS PREFETCH	Helmet DNS Prefetch header is not configured for this application.	INFO	CWE-693: Protection Mechanism Failure
HELMET HEADER FEATURE POLICY	Helmet Feature Policy header is not configured for this application.	INFO	CWE-693: Protection Mechanism Failure
HELMET HEADER FRAME GUARD	Helmet X Frame Options header is not configured for this application.	INFO	CWE-693: Protection Mechanism Failure
HELMET HEADER XSS FILTER	Helmet XSS Protection header is not configured for this application.	INFO	CWE-693: Protection Mechanism Failure
HELMET HEADER REFERRER POLICY	Helmet Referrer Policy header is not configured for this application.	INFO	CWE-693: Protection Mechanism Failure
RATE LIMIT CONTROL	This application does not have API rate limiting controls.	INFO	CWE-770: Allocation of Resources Without Limits or Throttling
HELMET HEADER IENOOPEN	Helmet IE No Open header is not configured for this application.	INFO	CWE-693: Protection Mechanism Failure

ISSUE	DESCRIPTION	SEVERITY	STANDARDS
HELMET HEADER NOSNIFF	Helmet No Sniff header is not configured for this application.	INFO	CWE-693: Protection Mechanism Failure
HELMET HEADER X POWERED BY	Helmet X Powered By header is not configured for this application.	INFO	CWE-693: Protection Mechanism Failure
HELMET HEADER CHECK CSP	Helmet Content Security Policy header is not configured for this application.	INFO	CWE-693: Protection Mechanism Failure
HELMET HEADER HSTS	Helmet HSTS header is not configured for this application.	INFO	CWE-693: Protection Mechanism Failure
ANTI CSRF CONTROL	This application does not have anti CSRF protection which prevents cross site request forgery attacks.	INFO	CWE-352: Cross-Site Request Forgery (CSRF)
HELMET HEADER CHECK CROSSDOMAIN	Helmet X Permitted Cross Domain Policies header is not configured for this application.	INFO	CWE-693: Protection Mechanism Failure

ALL IDENTIFIED NODE.JS ISSUES

JavaScript Issues

- HARDCODED JWT SECRET - **3**
- NODE TIMING ATTACK - **1**
- NODE USERNAME - **1**
- NODE SECRET - **1**
- HELMET HEADER CHECK EXPECT CT - **1**
- HELMET HEADER DNS PREFETCH - **1**
- HELMET HEADER FEATURE POLICY - **1**
- HELMET HEADER FRAME GUARD - **1**
- HELMET HEADER XSS FILTER - **1**
- HELMET HEADER REFERRER POLICY - **1**
- RATE LIMIT CONTROL - **1**
- HELMET HEADER IENOOPEN - **1**
- HELMET HEADER NOSNIFF - **1**
- HELMET HEADER X POWERED BY - **1**
- HELMET HEADER CHECK CSP - **1**
- HELMET HEADER HSTS - **1**
- ANTI CSRF CONTROL - **1**
- HELMET HEADER CHECK CROSSDOMAIN - **1**

ALL IDENTIFIED TEMPLATE ISSUES

Template Issues

ISSUES MARKED AS NOT APPLICABLE

Not Applicable

ISSUES MARKED AS FALSE POSITIVE

False Positive

FILES IN THE ARCHIVE

Files

Search in files

Search in files

FILE

client-app/package-lock.json

client-app/package.json

client-app/tsconfig.json

client-app/public/index.html

client-app/public/manifest.json

client-app/src/config/default.js

client-app/src/utils/helpers.js

client-app/src/utils/cookie.js

server-app/setup-db.sh

server-app/server.js

server-app/package-lock.json

server-app/package.json

server-app/.nvmrc