qr-val-api-test-case-detail

✅ PASS

Status	Alert Name	Plugin ID
PASS	Directory Browsing	0
PASS	Vulnerable JS Library (Powered by Retire.js)	10003
PASS	In Page Banner Information Leak	10009
PASS	Cookie No HttpOnly Flag	10010
PASS	Cookie Without Secure Flag	10011
PASS	Re-examine Cache-control Directives	10015
PASS	Cross-Domain JavaScript Source File Inclusion	10017
PASS	Content-Type Header Missing	10019
PASS	Anti-clickjacking Header	10020
PASS	X-Content-Type-Options Header Missing	10021
PASS	Info Disclosure - Sensitive Info in URL	10024
PASS	Info Disclosure - Sensitive Info in Referrer	10025
PASS	HTTP Parameter Override	10026
PASS	Info Disclosure - Suspicious Comments	10027
PASS	Open Redirect	10028
PASS	Cookie Poisoning	10029
PASS	User Controllable Charset	10030
PASS	User Controllable HTML Attribute (XSS)	10031
PASS	Viewstate	10032
PASS	Directory Browsing	10033
PASS	Heartbleed OpenSSL Vulnerability (Indicative)	10034
PASS	Strict-Transport-Security Header	10035
PASS	HTTP Server Response Header	10036
PASS	Server Leaks Info via X-Powered-By	10037
PASS	Content Security Policy (CSP) Not Set	10038
PASS	X-Backend-Server Info Leak	10039
PASS	Mixed Content on Secure Pages	10040
PASS	HTTP to HTTPS Form Post Transition	10041
PASS	HTTPS to HTTP Form Post Transition	10042
PASS	User Controllable JavaScript Event (XSS)	10043
PASS	Big Redirect Detected	10044
PASS	Source Code Disclosure - /WEB-INF	10045
PASS	Content Cacheability	10049
PASS	Retrieved from Cache	10050
PASS	X-ChromeLogger-Data Header Info Leak	10052
PASS	Cookie without SameSite Attribute	10054
PASS	CSP	10055
PASS	X-Debug-Token Info Leak	10056
PASS	Username Hash Found	10057
PASS	GET for POST	10058
PASS	X-AspNet-Version Response Header	10061
PASS	PII Disclosure	10062
PASS	Permissions Policy Header Not Set	10063

PASS	Timestamp Disclosure	10096
PASS	Hash Disclosure	10097
PASS	Cross-Domain Misconfiguration	10098
PASS	Source Code Disclosure	10099
PASS	User Agent Fuzzer	10104
PASS	Weak Authentication Method	10105
PASS	Reverse Tabnabbing	10108
PASS	Modern Web Application	10109
PASS	Dangerous JS Functions	10110
PASS	Authentication Request Identified	10111
PASS	Session Management Response Identified	10112
PASS	Verification Request Identified	10113
PASS	Script from Malicious Domain (polyfill)	10115
PASS	Absence of Anti-CSRF Tokens	10202
PASS	Private IP Disclosure	2
PASS	Heartbleed OpenSSL Vulnerability	20015
PASS	Source Code Disclosure - CVE-2012-1823	20017
PASS	Remote Code Execution - CVE-2012-1823	20018
PASS	External Redirect	20019
PASS	Session ID in URL Rewrite	3
PASS	Buffer Overflow	30001
PASS	Format String Error	30002
PASS	CRLF Injection	40003
PASS	Parameter Tampering	40008
PASS	Server Side Include	40009
PASS	XSS (Reflected)	40012
PASS	XSS (Persistent)	40014
PASS	XSS (Persistent) - Prime	40016
PASS	XSS (Persistent) - Spider	40017
PASS	SQL Injection	40018
PASS	SQL Injection - MySQL	40019
PASS	SQL Injection - Hypersonic SQL	40020
PASS	SQL Injection - Oracle	40021
PASS	SQL Injection - PostgreSQL	40022
PASS	SQL Injection - SQLite	40024
PASS	XSS (DOM Based)	40026
PASS	SQL Injection - MsSQL	40027
PASS	ELMAH Info Leak	40028
PASS	Trace.axd Info Leak	40029
PASS	.htaccess Info Leak	40032
PASS	.env Info Leak	40034
PASS	Hidden File Finder	40035
PASS	Spring Actuator Info Leak	40042
PASS	Log4Shell	40043
PASS	Spring4Shell	40045
PASS	Script Active Scan Rules	50000
PASS	Script Passive Scan Rules	50001
PASS	Path Traversal	6

PASS	Remote File Inclusion	7
PASS	Insecure JSF ViewState	90001
PASS	Java Serialization Object	90002
PASS	Sub Resource Integrity Missing	90003
PASS	Charset Mismatch	90011
PASS	XSLT Injection	90017
PASS	Server Side Code Injection	90019
PASS	Remote OS Command Injection	90020
PASS	XPath Injection	90021
PASS	XML External Entity Attack	90023
PASS	Generic Padding Oracle	90024
PASS	SOAP Action Spoofing	90026
PASS	SOAP XML Injection	90029
PASS	WSDL File Detection	90030
PASS	Loosely Scoped Cookie	90033
PASS	Cloud Metadata Potentially Exposed	90034
PASS	Server Side Template Injection	90035
PASS	SSTI (Blind)	90036

⚠ WARN

Status	Alert Name	Plugin ID	Sample URLs
WARN-NEW	Unexpected Content-Type was returned	100001	Multiple `404` URLs including `/latest/meta-data/`, `/metadata/instance`, etc.
WARN-NEW	Info Disclosure - Debug Error Messages	10023	`/pay_api/api/v1/payments/webhook` (500 error)
WARN-NEW	Spectre Vulnerability - Site Isolation	90004	`/ServiceStatus`, `/api-docs`
WARN-NEW	Application Error Disclosure	90022	`/pay_api/api/v1/payments/webhook` (500 error)

❌ FAIL

Status	Count
FAIL	0

Result

docker run -v "D:/Zap":/zap/wrk/:rw zaproxy/zap-stable zap-api-scan.py -t http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/pay_api/api-docs -f openapi -r qr-pay-scan-report.html -z "-config scanner.attackStrength=HIGH -config scanner.levelOfAlertThreshold=LOW"

2025-04-13 07:45:51,920 Number of Imported URLs: 14

Total of 28 URLs

PASS: Directory Browsing [0]

PASS: Vulnerable JS Library (Powered by Retire.js) [10003]

PASS: In Page Banner Information Leak [10009]

PASS: Cookie No HttpOnly Flag [10010]

PASS: Cookie Without Secure Flag [10011]

PASS: Re-examine Cache-control Directives [10015]

PASS: Cross-Domain JavaScript Source File Inclusion [10017]

PASS: Content-Type Header Missing [10019]

PASS: Anti-clickjacking Header [10020]

PASS: X-Content-Type-Options Header Missing [10021]

PASS: Information Disclosure - Sensitive Information in URL [10024]

PASS: Information Disclosure - Sensitive Information in HTTP Referrer Header [10025]

PASS: HTTP Parameter Override [10026]

PASS: Information Disclosure - Suspicious Comments [10027]

PASS: Open Redirect [10028]

PASS: Cookie Poisoning [10029]

PASS: User Controllable Charset [10030]

PASS: User Controllable HTML Element Attribute (Potential XSS) [10031]

PASS: Viewstate [10032]

PASS: Directory Browsing [10033]

PASS: Heartbleed OpenSSL Vulnerability (Indicative) [10034]

PASS: Strict-Transport-Security Header [10035]

PASS: HTTP Server Response Header [10036]

PASS: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) [10037]

PASS: Content Security Policy (CSP) Header Not Set [10038]

PASS: X-Backend-Server Header Information Leak [10039]

PASS: Secure Pages Include Mixed Content [10040]

PASS: HTTP to HTTPS Insecure Transition in Form Post [10041]

PASS: HTTPS to HTTP Insecure Transition in Form Post [10042]

PASS: User Controllable JavaScript Event (XSS) [10043]

PASS: Big Redirect Detected (Potential Sensitive Information Leak) [10044]

PASS: Source Code Disclosure - /WEB-INF Folder [10045]

PASS: Content Cacheability [10049]

PASS: Retrieved from Cache [10050]

PASS: X-ChromeLogger-Data (XCOLD) Header Information Leak [10052]

PASS: Cookie without SameSite Attribute [10054]

PASS: CSP [10055]

PASS: X-Debug-Token Information Leak [10056]

PASS: Username Hash Found [10057]

PASS: GET for POST [10058]

PASS: X-AspNet-Version Response Header [10061]

PASS: PII Disclosure [10062]

PASS: Permissions Policy Header Not Set [10063]

PASS: Timestamp Disclosure [10096]

PASS: Hash Disclosure [10097]

PASS: Cross-Domain Misconfiguration [10098]

PASS: Source Code Disclosure [10099]

PASS: User Agent Fuzzer [10104]

PASS: Weak Authentication Method [10105]

PASS: Reverse Tabnabbing [10108]

PASS: Modern Web Application [10109]

PASS: Dangerous JS Functions [10110]

PASS: Authentication Request Identified [10111]

PASS: Session Management Response Identified [10112]

PASS: Verification Request Identified [10113]

PASS: Script Served From Malicious Domain (polyfill) [10115]

PASS: Absence of Anti-CSRF Tokens [10202]

PASS: Private IP Disclosure [2]

PASS: Heartbleed OpenSSL Vulnerability [20015]

PASS: Source Code Disclosure - CVE-2012-1823 [20017]

PASS: Remote Code Execution - CVE-2012-1823 [20018]

PASS: External Redirect [20019]

PASS: Session ID in URL Rewrite [3]

PASS: Buffer Overflow [30001]

PASS: Format String Error [30002]

PASS: CRLF Injection [40003]

PASS: Parameter Tampering [40008]

PASS: Server Side Include [40009]

PASS: Cross Site Scripting (Reflected) [40012]

PASS: Cross Site Scripting (Persistent) [40014]

PASS: Cross Site Scripting (Persistent) - Prime [40016]

PASS: Cross Site Scripting (Persistent) - Spider [40017]

PASS: SQL Injection [40018]

PASS: SQL Injection - MySQL [40019]

PASS: SQL Injection - Hypersonic SQL [40020]

PASS: SQL Injection - Oracle [40021]

PASS: SQL Injection - PostgreSQL [40022]

PASS: SQL Injection - SQLite [40024]

PASS: Cross Site Scripting (DOM Based) [40026]

PASS: SQL Injection - MsSQL [40027]

PASS: ELMAH Information Leak [40028]

PASS: Trace.axd Information Leak [40029]

PASS: .htaccess Information Leak [40032]

PASS: .env Information Leak [40034]

PASS: Hidden File Finder [40035]

PASS: Spring Actuator Information Leak [40042]

PASS: Log4Shell [40043]

PASS: Spring4Shell [40045]

PASS: Script Active Scan Rules [50000]

PASS: Script Passive Scan Rules [50001]

PASS: Path Traversal [6]

PASS: Remote File Inclusion [7]

PASS: Insecure JSF ViewState [90001]

PASS: Java Serialization Object [90002]

PASS: Sub Resource Integrity Attribute Missing [90003]

PASS: Charset Mismatch [90011]

PASS: XSLT Injection [90017]

PASS: Server Side Code Injection [90019]

PASS: Remote OS Command Injection [90020]

PASS: XPath Injection [90021]

PASS: XML External Entity Attack [90023]

PASS: Generic Padding Oracle [90024]

PASS: SOAP Action Spoofing [90026]

PASS: SOAP XML Injection [90029]

PASS: WSDL File Detection [90030]

PASS: Loosely Scoped Cookie [90033]

PASS: Cloud Metadata Potentially Exposed [90034]

PASS: Server Side Template Injection [90035]

PASS: Server Side Template Injection (Blind) [90036]

WARN-NEW: Unexpected Content-Type was returned [100001] x 6

http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/5820472884515476146 (404)

http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/latest/meta-data/ (404)

http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/computeMetadata/v1/ (404)

http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/opc/v1/instance/ (404)

http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/metadata/instance (404)

WARN-NEW: Information Disclosure - Debug Error Messages [10023] x 1

http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/pay_api/api/v1/payments/webhook (500)

WARN-NEW: Insufficient Site Isolation Against Spectre Vulnerability [90004] x 2

http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/pay_api/api/v1/payments/ServiceStatus (200)

http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/pay_api/api-docs (200)

WARN-NEW: Application Error Disclosure [90022] x 1

http://a9ee8979c10c84febbd2d45bd6075bca-1416825320.ap-southeast-1.elb.amazonaws.com:8080/pay_api/api/v1/payments/webhook (500)

FAIL-NEW: 0 FAIL-INPROG: 0 WARN-NEW: 4 WARN-INPROG: 0 INFO: 0 IGNORE: 0 PASS: 109