qr-fbk-api-test-case-detail

✅ Passed Scans

Status	Alert Name	Alert ID
PASS	Directory Browsing	0, 10033
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 (URL/Referrer)	10024/25
PASS	HTTP Parameter Override	10026
PASS	Suspicious Comments	10027
PASS	Open Redirect	10028
PASS	Cookie Poisoning	10029
PASS	User Controllable Charset / HTML Attribute	10030/31
PASS	Viewstate	10032
PASS	Heartbleed (Indicative)	10034
PASS	HTTP Headers (HSTS, X-Powered-By, etc.)	10035–37
PASS	CSP Not Set	10038
PASS	Mixed Content / HTTPS to HTTP Forms	10040–42
PASS	XSS (Reflected, Persistent, DOM, etc.)	40012–17, 40026
PASS	SQL Injection (All Types)	40018–24, 40027
PASS	Path Traversal, RFI, OS Cmd Injection, SSTI, XXE, etc.	6, 7, 90019–24, etc.
PASS	Various Header/Info Leaks	10052, 10054, 10056, 10061, etc.
PASS	Others (SOAP/XML/Env/.htaccess Info Leak, Log4Shell, etc.)	many

⚠️ WARN

Status	Alert Name	Alert ID	URL
WARN	**Unexpected Content-Type Returned**	100001	`/5821453902438382176`, `/latest/meta-data/`, `/opc/v1/instance/`
WARN	**Information Disclosure - Debug Error Messages**	10023	`/api/v1/feedbacks/id`, `/feedbacks/date?date=date`
WARN	**Buffer Overflow**	30001	`/feedbacks/General`, `/api/v1/feedbacks`

WARN	**Insufficient Site Isolation (Spectre Mitigation)**	90004	`/api-docs`, `/feedbacks/General`, `/feedbacks`
WARN	**Application Error Disclosure**	90022	`/feedbacks/id`, `/feedbacks/date?date=date`

❌ Failures

Status	Count
FAIL	0

Summary

Result Type	Count
PASS	134
WARN	3
FAIL	0
INFO	0
IGNORE	0

Result

docker run -v "D:/Zap":/zap/wrk/:rw zaproxy/zap-stable zap-api-scan.py -t http://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/fbk_api/api-docs -f openapi -r qr-fbk-scan-report.html -z "-config scanner.attackStrength=HIGH -config scanner.levelOfAlertThreshold=LOW"

2025-04-13 09:36:32,004 Number of Imported URLs: 9

Total of 23 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: 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://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/5821453902438382176 (404)

http://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/latest/meta-data/ (404)

http://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/computeMetadata/v1/ (404)

http://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/opc/v1/instance/ (404)

http://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/metadata/instance (404)

WARN-NEW: Information Disclosure - Debug Error Messages [10023] x 4

http://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/fbk_api/api/v1/feedbacks/id (500)

http://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/fbk_api/api/v1/feedbacks/id (500)

http://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/fbk_api/api/v1/feedbacks/id (500)

http://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/fbk_api/api/v1/feedbacks/date?date=date (500)

WARN-NEW: Buffer Overflow [30001] x 2

http://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/fbk_api/api/v1/feedbacks/General (500)

http://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/fbk_api/api/v1/feedbacks (500)

WARN-NEW: Insufficient Site Isolation Against Spectre Vulnerability [90004] x 4

http://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/fbk_api/api-docs (200)

http://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/fbk_api/api/v1/feedbacks/General (201)

http://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/fbk_api/api/v1/feedbacks (201)

http://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/fbk_api/api/v1/feedbacks (200)

WARN-NEW: Application Error Disclosure [90022] x 4

http://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/fbk_api/api/v1/feedbacks/id (500)

http://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/fbk_api/api/v1/feedbacks/id (500)

http://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/fbk_api/api/v1/feedbacks/id (500)

http://ac40c779f7a9f4cbd9a92993c9706e35-762169467.ap-southeast-1.elb.amazonaws.com:8080/fbk_api/api/v1/feedbacks/date?date=date (500)

FAIL-NEW: 0 FAIL-INPROG: 0 WARN-NEW: 5 WARN-INPROG: 0 INFO: 0 IGNORE: 0 PASS: 108