



OpenHack

Project Security Report

Devil's Advocate

Organization: meridian-cloud

Total scans analyzed: 17

Unique findings: 64 active, 0 remediated, 0 dismissed (64 total)

Generated: October 19, 2026 (UTC)

Generated by: ananay@openhack.com

Latest scan: July 28, 2026 (UTC)

CONFIDENTIAL

Executive Risk Summary

Overall Risk: HIGH

This report aggregates security findings from 17 scans of the Devil's Advocate project. A total of 64 unique vulnerabilities were identified across all scans.

Severity Breakdown

Critical	High	Medium	Low
22	26	14	2

Remediation Trail

New	Persisting	Confirmed Fixed
10	0	0

Vulnerability Findings

64 unique findings aggregated from 17 scans, sorted by severity.

[CRITICAL] [SQL Injection] SQL Injection in src/app/api/products/route.ts

src/app/api/products/route.ts:29
CWE-89 | CVSS 9.8 | New

[CRITICAL] [Authentication Bypass] Authentication Bypass in src/app/api/internal/diagnostics/route.ts

src/app/api/internal/diagnostics/route.ts:4
CWE-287 | CVSS 9.8 | New | 3 scans

[CRITICAL] [Authentication Bypass] Authentication Bypass in src/lib/auth.ts

src/lib/auth.ts:30
CWE-287 | CVSS 9.8 | New | 2 scans

[CRITICAL] [RCE] RCE in src/lib/auth.ts

src/lib/auth.ts:144
CWE-502 | CVSS 9.8 | New | 2 scans

[CRITICAL] [Command Injection] Command Injection in src/app/api/internal/diagnostics/route.ts

src/app/api/internal/diagnostics/route.ts:17
CWE-78 | CVSS 10.0 | New | 7 scans

[CRITICAL] [Command Injection] Command Injection in src/app/api/internal/diagnostics/route.ts

src/app/api/internal/diagnostics/route.ts:6
CWE-78 | CVSS 10.0 | New

[CRITICAL] [SQL Injection] SQL Injection in src/app/api/auth/login/route.ts

src/app/api/auth/login/route.ts:24
CWE-89 | CVSS 9.8 | New | 4 scans

[CRITICAL] [Open Redirect] Open Redirect in src/app/api/redirect/route.ts

src/app/api/redirect/route.ts:3
CWE-601 | CVSS 8.1 | New

[CRITICAL] [SSRF] SSRF in src/app/api/users/import-avatar/route.ts

src/app/api/users/import-avatar/route.ts:6
CWE-918 | CVSS 7.5 | New

[CRITICAL] [Path Traversal] Path Traversal in src/app/api/internal/files/route.ts

src/app/api/internal/files/route.ts:8
CWE-22 | CVSS 9.1 | New | 2 scans

[CRITICAL] [Authentication Bypass] Authentication Bypass in src/lib/auth.ts

src/lib/auth.ts:36
CWE-287 | CVSS 9.8 | New

[CRITICAL] [Data Exposure] Data Exposure in src/app/api/internal/users/route.ts

src/app/api/internal/users/route.ts:4
CWE-200 | CVSS 9.1 | New | 2 scans

[CRITICAL] [Authentication Bypass] Authentication Bypass in src/app/api/internal/stats/route.ts

src/app/api/internal/stats/route.ts:4
CWE-287 | CVSS 8.6 | New

[CRITICAL] [RCE] RCE in src/app/api/internal/diagnostics/route.ts

src/app/api/internal/diagnostics/route.ts:16
CVSS 10.0 | New

[CRITICAL] [SQL Injection] SQL Injection in src/app/api/products/route.ts

src/app/api/products/route.ts:14
CWE-89 | CVSS 9.8 | New

[CRITICAL] [Command Injection] Command Injection in src/lib/server-utils.ts

src/lib/server-utils.ts:4
CWE-78 | CVSS 10.0 | New

[CRITICAL] [Command Injection] Command Injection in src/lib/server-utils.ts

src/lib/server-utils.ts:9
CWE-78 | CVSS 10.0 | New

[CRITICAL] [SSRF] SSRF in src/app/api/internal/webhooks/route.ts

src/app/api/internal/webhooks/route.ts:25
CWE-918 | CVSS 9.1 | New

[CRITICAL] [Path Traversal] Path Traversal in src/app/api/internal/files/route.ts

src/app/api/internal/files/route.ts:5
CWE-22 | CVSS 9.1 | New

[CRITICAL] [Authentication Bypass] Authentication Bypass in src/lib/auth.ts

src/lib/auth.ts:29
CWE-287 | CVSS 9.8 | New

[CRITICAL] [Authentication Bypass] Authentication Bypass in src/lib/auth.ts

src/lib/auth.ts:59
CWE-287 | CVSS 9.8 | New

[CRITICAL] [Hardcoded Secret] Hardcoded Secret in docker-compose.yml

docker-compose.yml:32
CWE-798 | CVSS 9.8 | New

[HIGH] [Insecure Cryptography] Insecure Cryptography in src/lib/auth.ts

src/lib/auth.ts:6
CVSS 9.1 | New | 6 scans

[HIGH] [Security Misconfiguration] Security Misconfiguration in src/app/api/auth/forgot-password/route.ts

src/app/api/auth/forgot-password/route.ts:46
CWE-693 | CVSS 9.1 | New | 2 scans

[HIGH] [Path Traversal] Path Traversal in src/app/api/internal/files/route.ts

src/app/api/internal/files/route.ts:17
CWE-22 | CVSS 7.5 | New | 3 scans

[HIGH] [XSS] XSS in src/components/ReviewSection.tsx

src/components/ReviewSection.tsx:176
CWE-79 | CVSS 7.1 | New | 6 scans

[HIGH] [SSRF] SSRF in src/app/api/internal/webhooks/test/route.ts

src/app/api/internal/webhooks/test/route.ts:25
CWE-918 | CVSS 8.6 | New

[HIGH] [Mass Assignment] Mass Assignment in src/app/api/auth/register/route.ts

src/app/api/auth/register/route.ts:38
CVSS 8.1 | New | 5 scans

[HIGH] [Information Disclosure] Information Disclosure in src/app/api/auth/forgot-password/route.ts

src/app/api/auth/forgot-password/route.ts:43
CWE-200 | CVSS 9.1 | New

[HIGH] [IDOR] IDOR in src/app/api/users/[id]/route.ts

src/app/api/users/[id]/route.ts:8
CWE-862 | CVSS 9.1 | New | 6 scans

[HIGH] [Authorization Bypass] Authorization Bypass in src/app/api/orders/[id]/route.ts

src/app/api/orders/[id]/route.ts:10
CWE-862 | CVSS 8.6 | New

[HIGH] [CSRF] CSRF in src/app/api/users/change-password/route.ts

src/app/api/users/change-password/route.ts:6
CWE-352 | CVSS 5.3 | New

[HIGH] [Storage Misconfiguration] Storage Misconfiguration in src/app/api/upload/route.ts

src/app/api/upload/route.ts:28
CVSS 7.2 | New

[HIGH] [SSRF] SSRF in src/lib/server-utils.ts

src/lib/server-utils.ts:13
CWE-918 | CVSS 8.6 | New | 2 scans

[HIGH] [Storage Misconfiguration] Storage Misconfiguration in src/app/api/upload/route.ts

src/app/api/upload/route.ts:34
CVSS 7.1 | New

[HIGH] [Mass Assignment] Mass Assignment in src/app/api/users/[id]/route.ts

src/app/api/users/[id]/route.ts:54
CVSS 9.8 | New

[HIGH] [SSRF] SSRF in src/app/api/users/import-avatar/route.ts

src/app/api/users/import-avatar/route.ts:27
CWE-918 | CVSS 8.6 | New | 2 scans

[HIGH] [Data Exposure] Data Exposure in src/app/api/internal/users/route.ts

src/app/api/internal/users/route.ts:5
CWE-200 | CVSS 9.8 | New | 2 scans

[HIGH] [Business Logic Flow] Business Logic Flow in src/app/api/orders/route.ts

src/app/api/orders/route.ts:76
CVSS 7.5 | New

[HIGH] [Authorization Bypass] Authorization Bypass in src/app/api/orders/[id]/route.ts

src/app/api/orders/[id]/route.ts:64
CWE-862 | CVSS 8.1 | New

[HIGH] [SSRF] SSRF in src/app/api/redirect/route.ts

src/app/api/redirect/route.ts:11
CWE-918 | CVSS 7.1 | New

[HIGH] [Data Exposure] Data Exposure in src/app/api/internal/users/route.ts

src/app/api/internal/users/route.ts:17
CWE-200 | CVSS 7.5 | New

[HIGH] [Security Misconfiguration] Security Misconfiguration in src/app/api/upload/route.ts

src/app/api/upload/route.ts:44
CWE-693 | CVSS 7.1 | New

[HIGH] [Authorization Bypass] Authorization Bypass in src/app/api/products/[id]/route.ts

src/app/api/products/[id]/route.ts:49
CWE-862 | CVSS 8.2 | New

[HIGH] [Data Exposure] Data Exposure in src/app/api/internal/stats/route.ts

src/app/api/internal/stats/route.ts:5
CWE-200 | CVSS 7.5 | New

[HIGH] [XXE] XXE in src/lib/server-utils.ts

src/lib/server-utils.ts:23
CWE-611 | CVSS 8.6 | New

[HIGH] [Authorization Bypass] Authorization Bypass in src/app/api/products/[id]/route.ts

src/app/api/products/[id]/route.ts:48
CWE-862 | CVSS 9.1 | New

[HIGH] [CSRF] CSRF in src/app/api/users/[id]/route.ts

src/app/api/users/[id]/route.ts:15
CWE-352 | CVSS 9.8 | New

[MEDIUM] [Open Redirect] Open Redirect in src/app/api/redirect/route.ts

src/app/api/redirect/route.ts:12
CWE-601 | CVSS 6.1 | New | 5 scans

[MEDIUM] [Information Disclosure] Information Disclosure in src/app/api/internal/files/route.ts

src/app/api/internal/files/route.ts:11
CWE-200 | CVSS 5.3 | New

[MEDIUM] [Security Misconfiguration] Security Misconfiguration in src/app/api/redirect/route.ts

src/app/api/redirect/route.ts:14
CWE-693 | CVSS 5.3 | New

[MEDIUM] [Security Misconfiguration] Security Misconfiguration in src/lib/auth.ts

src/lib/auth.ts:48
CWE-693 | CVSS 5.3 | New

[MEDIUM] [Unknown] Unknown in

CVSS 9.8 | New | 2 scans

[MEDIUM] [Business Logic Flaw] Business Logic Flaw in prisma/seed.ts

prisma/seed.ts:171
CWE-327 | CVSS 5.3 | New

[MEDIUM] [Security Misconfiguration] Security Misconfiguration in src/app/api/auth/login/route.ts

src/app/api/auth/login/route.ts:68
CWE-693 | CVSS 6.5 | New

[MEDIUM] [Security Misconfiguration] Security Misconfiguration in src/middleware.ts

src/middleware.ts:8
CWE-693 | CVSS 5.3 | New

[MEDIUM] [Security Misconfiguration] Security Misconfiguration in next.config.js

next.config.js:5
CWE-693 | CVSS 5.3 | New

[MEDIUM] [Information Disclosure] Information Disclosure in src/app/api/internal/files/route.ts

src/app/api/internal/files/route.ts:22
CWE-200 | CVSS 5.3 | New

[MEDIUM] [Business Logic Flaw] Business Logic Flaw in src/app/api/auth/forgot-password/route.ts

src/app/api/auth/forgot-password/route.ts:24
CVSS 5.3 | New

[MEDIUM] [Security Misconfiguration] Security Misconfiguration in next.config.js

next.config.js:4
CWE-693 | CVSS 5.3 | New | 2 scans

[MEDIUM] [Security Misconfiguration] Security Misconfiguration in src/middleware.ts

src/middleware.ts:13
CWE-693 | CVSS 4.3 | New

[MEDIUM] [Information Disclosure] Information Disclosure in src/app/api/contact/route.ts

src/app/api/contact/route.ts:19
CWE-200 | CVSS 3.1 | New

[LOW] [Data Exposure] Data Exposure in src/app/api/auth/forgot-password/route.ts

src/app/api/auth/forgot-password/route.ts:44
CWE-200 | CVSS 9.8 | New

[LOW] [CSRF] CSRF in src/app/api/auth/login/route.ts

src/app/api/auth/login/route.ts:67
CWE-352 | CVSS 6.5 | New | 2 scans

Methodology & Disclaimer

Scan Methodology

Source code was analyzed using AI-based static analysis. Each source file was examined for security vulnerabilities including injection flaws, authentication and authorization issues, cryptographic weaknesses, server-side request forgery, cross-site scripting, path traversal, insecure deserialization, and configuration errors. The analysis pipeline consists of reconnaissance, vulnerability hunting, and validation stages.

Aggregated Report

This report aggregates findings from 17 completed scans. This project-level report provides the most complete picture by combining results from all scans and including the full remediation trail.

Severity Methodology

Severity reflects business and data-sensitivity impact rather than CVSS base score alone. In a PHI-handling context, findings are rated Critical/High/Medium/Low based on exploitability in the deployed environment, data-exposure surface, and the sensitivity of affected health data. CVSS base scores are provided for reference and are not determinative; a finding may carry a severity higher or lower than its CVSS band indicates.

Risk Rating

The overall risk level is computed based on active (unresolved) findings only: 'No Open Findings' if all findings are remediated or dismissed; HIGH if any active finding has Critical severity or 3+ active High-severity findings; MODERATE if any active High-severity findings are present; LOW otherwise. This is an automated heuristic — manual review is recommended.

Regulatory Context

Canadian federal and provincial privacy requirements apply to this application. Health-related data is subject to applicable provincial health-privacy legislation (e.g. PHIPA in Ontario) and privacy obligations under PIPEDA (Personal Information Protection and Electronic Documents Act). This report should be reviewed in conjunction with your organization's compliance framework.

Disclaimer

This report was generated automatically by OpenHack. Findings reflect the state of the codebase at the time of the scans and may not account for vulnerabilities introduced afterward. This report is intended for internal audit and compliance purposes and should be used in conjunction with manual security review.

Report Metadata

Project: Devil's Advocate
Organization: meridian-cloud
Scans analyzed: 17
Unique findings: 64 active, 0 remediated, 0 dismissed (64 total)
Latest scan: 2026-07-28T16:59:45.169Z
Report generated: 2026-10-19T11:28:16.146Z
Engine: OpenHack Enterprise AI SAST