■■ QUANTUMSENTINEL-NEXUS

+ VALIDATE-OMNISHIELD

COMPREHENSIVE SECURITY ASSESSMENT REPORT

Report Information	
Scan ID:	QS-OMNISHIELD-20251006_121322
Framework:	QuantumSentinel-Nexus + VALIDATE-OMNISHIELD
Version:	1.0.0
Generated:	2025-10-06T12:13:47.608211
Assessment Summary	
Total Findings:	19
Risk Score:	5.9/10
Modules Scanned:	2
Critical Issues:	4
High Issues:	4
Medium Issues:	11

Generated on October 06, 2025 at 12:26 PM

EXECUTIVE SUMMARY

This comprehensive security assessment was conducted using the QuantumSentinel-Nexus platform integrated with VALIDATE-OMNISHIELD universal vulnerability validation framework. The assessment identified **19 security findings** across **2 security modules**, with a calculated risk score of **5.9/10**.

Severity Level	Count	Percentage	Priority
Critical	4	21.1%	Immediate Action Required
High	4	21.1%	Address within 24-48 hours
Medium	11	57.9%	Address within 1 week
Low	0	0.0%	Address within 1 month

Assessment Coverage:
• QuantumSentinel Findings: 19
• OMNISHIELD Validations: 0
• CVE Mappings: 0

DETAILED SECURITY FINDINGS

Critical Severity Findings

Critical-001: Zero-Day: Go Compiler Backend

Finding ID:	QS-ZERO_DAY_RESEARCH-0009
Source Module:	zero_day_research
Severity:	Critical
Confidence:	0.7
Timestamp:	2025-10-06T12:13:47.608112
Description:	Remote Code Execution (RCE)

Critical-002: Zero-Day: PyTorch Model Deserialization

Finding ID:	QS-ZERO_DAY_RESEARCH-0012
Source Module:	zero_day_research
Severity:	Critical
Confidence:	0.7
Timestamp:	2025-10-06T12:13:47.608136
Description:	Remote Code Execution via Pickle

Critical-003: Zero-Day: Go Compiler Backend

Finding ID:	QS-ZERO_DAY_RESEARCH-0014
Source Module:	zero_day_research
Severity:	Critical
Confidence:	0.7
Timestamp:	2025-10-06T12:13:47.608141
Description:	Remote Code Execution (RCE)

Critical-004: Zero-Day: PyTorch Model Deserialization

Finding ID:	QS-ZERO_DAY_RESEARCH-0017
Source Module:	zero_day_research
Severity:	Critical
Confidence:	0.7
Timestamp:	2025-10-06T12:13:47.608151
Description:	Remote Code Execution via Pickle

High Severity Findings

High-001: Zero-Day: Bazel Build System

Finding ID:	QS-ZERO_DAY_RESEARCH-0010
Source Module:	zero_day_research
Severity:	High
Confidence:	0.7
Timestamp:	2025-10-06T12:13:47.608115
Description:	BUILD File Execution

High-002: Zero-Day: Angular Sanitizer

Finding ID:	QS-ZERO_DAY_RESEARCH-0011
Source Module:	zero_day_research
Severity:	High
Confidence:	0.7
Timestamp:	2025-10-06T12:13:47.608133
Description:	XSS Bypass

High-003: Zero-Day: Bazel Build System

Finding ID:	QS-ZERO_DAY_RESEARCH-0015
Source Module:	zero_day_research
Severity:	High
Confidence:	0.7
Timestamp:	2025-10-06T12:13:47.608145
Description:	BUILD File Execution

High-004: Zero-Day: Angular Sanitizer

Finding ID:	QS-ZERO_DAY_RESEARCH-0016
Source Module:	zero_day_research
Severity:	High
Confidence:	0.7
Timestamp:	2025-10-06T12:13:47.608148
Description:	XSS Bypass

Medium Severity Findings

Medium-001: APK Analysis Required: b4583a15-063f-41b3-9507-d12cb27ae203_H4D.apk

Finding ID:	QS-MOBILE_SECURITY-0000
Source Module:	mobile_security
Severity:	Medium
Confidence:	0.7
Timestamp:	2025-10-06T12:13:47.608075
Description:	Android APK file detected requiring security analysis

Medium-002: APK Analysis Required: f46b9e0e-46ef-4ee3-bd01-582ee9acf4c7_H4D.apk

Finding ID:	QS-MOBILE_SECURITY-0001
Source Module:	mobile_security
Severity:	Medium
Confidence:	0.7
Timestamp:	2025-10-06T12:13:47.608085
Description:	Android APK file detected requiring security analysis

Medium-003: APK Analysis Required: b966da7c-79bb-49d3-91bf-e51c0a2e8100_H4C.apk

Finding ID:	QS-MOBILE_SECURITY-0002
Source Module:	mobile_security
Severity:	Medium
Confidence:	0.7
Timestamp:	2025-10-06T12:13:47.608089
Description:	Android APK file detected requiring security analysis

Medium-004: APK Analysis Required: 96ed20ca-dc19-4280-8a0f-89e06246f885_H4C.apk

Finding ID:	QS-MOBILE_SECURITY-0003
Source Module:	mobile_security
Severity:	Medium
Confidence:	0.7
Timestamp:	2025-10-06T12:13:47.608093
Description:	Android APK file detected requiring security analysis

Medium-005: APK Analysis Required: 40bbe685-5086-4df5-bd9d-7698009dfa9e_H4C.apk

Finding ID:	QS-MOBILE_SECURITY-0004
Source Module:	mobile_security
Severity:	Medium
Confidence:	0.7
Timestamp:	2025-10-06T12:13:47.608096

Description:	Android APK file detected requiring security analysis

Medium-006: APK Analysis Required: 94261026-8418-44e0-8775-34f8d1d5020b_H4D.apk

Finding ID:	QS-MOBILE_SECURITY-0005
Source Module:	mobile_security
Severity:	Medium
Confidence:	0.7
Timestamp:	2025-10-06T12:13:47.608099
Description:	Android APK file detected requiring security analysis

Medium-007: APK Analysis Required: 0f3d8734-5f16-49d1-a5fe-30d430aaa849_H4C.apk

Finding ID:	QS-MOBILE_SECURITY-0006
Source Module:	mobile_security
Severity:	Medium
Confidence:	0.7
Timestamp:	2025-10-06T12:13:47.608102
Description:	Android APK file detected requiring security analysis

Medium-008: APK Analysis Required: eeba765f-7537-4345-8435-1374681db983_H4D.apk

Finding ID:	QS-MOBILE_SECURITY-0007
Source Module:	mobile_security
Severity:	Medium
Confidence:	0.7
Timestamp:	2025-10-06T12:13:47.608105
Description:	Android APK file detected requiring security analysis

Medium-009: APK Analysis Required: c11162c8-b376-4dd3-a3ba-be13869115b6_H4D.apk

Finding ID:	QS-MOBILE_SECURITY-0008
Source Module:	mobile_security
Severity:	Medium
Confidence:	0.7
Timestamp:	2025-10-06T12:13:47.608108
Description:	Android APK file detected requiring security analysis

Medium-010: Zero-Day: TensorFlow Runtime

Finding ID:	QS-ZERO_DAY_RESEARCH-0013
Source Module:	zero_day_research

Severity:	Medium
Confidence:	0.7
Timestamp:	2025-10-06T12:13:47.608138
Description:	Model Tampering & Buffer Overflow

Medium-011: Zero-Day: TensorFlow Runtime

Finding ID:	QS-ZERO_DAY_RESEARCH-0018
Source Module:	zero_day_research
Severity:	Medium
Confidence:	0.7
Timestamp:	2025-10-06T12:13:47.608154
Description:	Model Tampering & Buffer Overflow

SECURITY MODULE BREAKDOWN

Security Module	Findings Count	Status
Mobile Security	9	■ Completed
Api Security	0	■ No Findings
Network Security	0	■ No Findings
Bug Bounty	0	■ No Findings
Threat Intelligence	0	■ No Findings
Binary Analysis	0	■ No Findings
Zero Day Research	10	■ Completed

Mobile Security

Analysis of mobile applications (APK files) for security vulnerabilities

Findings: 9

Zero Day Research

Novel vulnerability discovery and validation

Findings: 10

SECURITY RECOMMENDATIONS

Recommendation 1: Address 4 Critical Security Issues Immediately

Priority:	**URGENT**
Category:	Critical Remediation
Description:	Critical vulnerabilities detected requiring immediate attention

Recommended Actions:
- Patch critical vulnerabilities within 24 hours
- Implement emergency mitigations
- Monitor for active exploitation
- Update incident response procedures

Recommendation 2: QuantumSentinel-Nexus Security Improvements

Priority:	**HIGH**
Category:	Quantum Security
Description:	Address 19 findings from specialized security modules

Recommended Actions:
- Review mobile application security controls
- Strengthen API authentication and authorization
- Implement network segmentation controls
- Enhance threat intelligence integration

Recommendation 3: Establish Continuous Security Monitoring

Priority:	**MEDIUM**
Category:	Continuous Monitoring
Description:	Implement ongoing security assessment processes

Recommended Actions:
- Schedule regular comprehensive scans
- Integrate security tools into CI/CD pipelines
- Establish security metrics and KPIs
- Create automated alert mechanisms

Recommendation 4: Strengthen Security Governance

Priority:	**MEDIUM**
Category:	Security Governance
Description:	Improve organizational security posture

Recommended Actions:
- Develop comprehensive security policies
- Conduct regular security training
- Implement security code review processes
- Establish incident response procedures