QBurst | A High AI-Q™ Company

Trust vs. Zero Trust: Advanced Application Security Hardening for Government Intranet Systems

Transitioning a sensitive on-premises GlassFish infrastructure from implicit network trust to a resilient, defense-in-depth security model using OWASP assessment methodologies.

Overview

We simulated an internal adversary leveraging the OWASP Testing Methodology to evaluate a sensitive, unpatched on-premises infrastructure deployment.

- Discovered a critical kill chain combining implicit node trust with an active End-of-Life (EOL) GlassFish vulnerability (CVE-2017-1000028) to execute unauthenticated Local File Inclusion (LFI).
- Mapped, classified, and provided remediation blueprints for 22 distinct security vulnerabilities spanning host configuration, credential storage, and transport layer ciphers.

Client Profile

Based in South Africa, the client is a prominent government sector organization managing critical internal infrastructure and handling highly sensitive data. To protect their assets, they operate entirely within an isolated intranet environment, shielded from public internet exposure by enterprise-grade firewalls and strict access controls.

Challenges: The Pitfalls of Implicit Network Trust

Relying entirely on perimeter walls created deep security vulnerabilities across the internal application layer:

- **Implicit Structural Trust:** Internal firewall rules were configured to automatically grant unrestricted, cross-enclave communication based purely on a device's logical IP subnet assignment.

- **Application-Layer Modernization Deferral:** Because the systems lacked external public internet routing, critical patch management cycles and active vulnerability scanning had been systematically deferred, keeping highly vulnerable, EOL enterprise service versions active.
- **Absence of Host Defense-in-Depth:** The local operating environments lacked strict permission limits, file system constraints, or behavioral logging, assuming that an attacker could never compromise an internal workstation.

Solution: Threat Simulation and Vulnerability Mapping

QBurst's specialized cybersecurity division initiated a comprehensive, controlled white-hat pentesting engagement. Mimicking a malicious insider or a lateral-moving malware strain, we attached a standard endpoint directly to a trusted network node to systematically audit the hidden application layer.

- **Exploiting the Implicit Path (Phase 1):** The initial network mapping confirmed that our testing workstation bypassed boundary firewalls, gaining a clear line of sight to the administrative interfaces of the on-premises GlassFish node. Manual enumeration verified the server was running a legacy version susceptible to CVE-2017-1000028 (an unauthenticated path traversal flaw).
- **Executing Proof-of-Concept Verification:** To validate the threat, our engineers constructed a heavily encoded path traversal payload, appending it directly to the active login URL parameter. The application instantly bypassed the authentication wall, resolving the local file inclusion and displaying the host operating system's restricted win.ini file directly in our testing browser.
- **Deep-Dive Structural Risk Analysis (Phase 2):** Following the successful LFI breach, we performed an exhaustive on-premise configuration audit across the underlying system architecture, discovering severe configuration drift and widespread structural gaps.

Intranet Vulnerability Registry

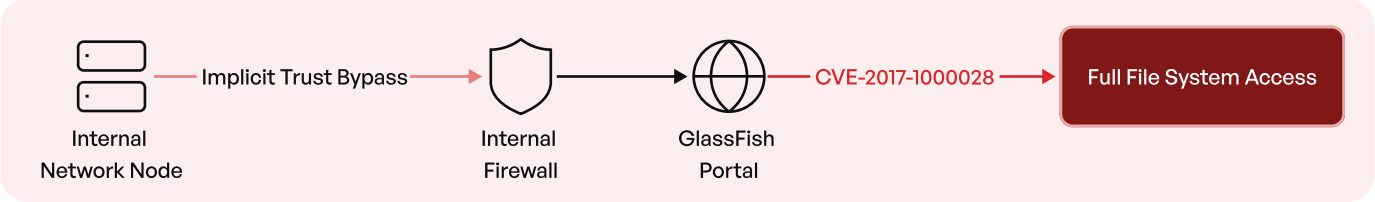
OWASP Category	Finding Count	Severity	Architectural Risk & Impact
A01:2021 – Broken Access Control	3	Critical	Enables unauthenticated path traversal to access arbitrary system files, unauthorized directory access, and administrative panel exposure.
A06:2021 – Vulnerable and Outdated Components	1	High	Leaves system exposed to publicly documented exploits and unsupported End-of-Life (EOL) middleware/OS dependencies.
A02:2021 – Cryptographic Failures	2	Medium	Exposes unencrypted service credentials in configuration files and exposes network traffic via outdated SSL/TLS cipher suites.
A04:2021 – Insecure Design	2	Medium	Absence of rate-limiting controls and resource consumption bounds leaves host susceptible to brute-force attacks and internal Denial of Service (DoS).
A05:2021 – Security Misconfiguration	10	Medium	Facilitates system fingerprinting, arbitrary code execution via default deployments, lingering legacy artifacts, unencrypted admin traffic, and missing HTTP security headers.
A07:2021 – Identification and Authentication Failures	2	Medium	Increases susceptibility to automated password guessing, session hijacking, and unauthorized administrative takeover due to weak policies and excessive timeouts.

A09:2021 – Security Logging and Monitoring Failures	2	Info	Prevents real-time detection of active exploits and impairs forensic audit capabilities during security incidents.

This engagement was explicitly structured as an analytical risk-mapping assessment to generate mitigation blueprints. Final validation and retesting of engineering patches were excluded from the project scope.

Key Features and Technical Highlights

- **OWASP-Driven Threat Modeling:** Standardized testing principles used to map internal lateral attack paths accurately.
- **LFI Payload Execution Verification:** Live cryptographic and encoded character manipulation to prove data leakage vulnerabilities without causing system downtime.
- **Multi-Layer Configuration Auditing:** Broad evaluation spanning web deployment configurations (web.xml), access policies, and server engines.
- **Cryptographic Cipher Verification:** Security scanning to locate and eliminate weak SSL/TLS cipher suites vulnerable to traffic sniffing.
- **Systemic DoS Mitigation Identification:** Diagnostics to flag high resource consumption caused by hidden, unmanaged default background services.



Initial Attack Vector

Impact

- **Dismantled a Critical Attack Path:** Pinpointed a severe lateral kill chain, preventing compromised internal nodes or automated ransomware strains from seizing control of the host operating system.
- **Insulated Classified Core Assets:** Uncovering plaintext database connection strings and configuration passwords allowed the client to rotate credentials, blocking future database pivoting.
- **Delivered a 22-Point Risk Blueprint:** Provided a highly detailed risk registry that mapped out hidden technical debt, enabling targeted remediation strategies.
- **Restored Operational Capacity:** Identifying high hardware utilization driven by auto-deploy defaults helped the client eliminate performance lag and avoid internal, accidental Denial of Service (DoS) states.
- **Accelerated Compliance Readiness:** Our technical insights provided the client's internal engineering teams with the exact blueprints needed to align their on-premises stack with rigid government security standards before formal state audits.