

Customer Case Study: Online Retailer Enhances Web Application Security**Industry:** Online Retail**Engagement Type:** Web App Scanning**Delivery Format:** Remote**Engagement Duration:** 1 week

Client Overview

Online Retailer, a leader in high-performance ecommerce company, engaged our team to strengthen their web application security program. With a growing number of customer-facing and internal apps across development and production environments, Online Retailer needed better visibility into application-layer vulnerabilities.

This engagement focused on deploying a Web App Scanning (WAS) tool as part of their broader vulnerability management platform, aligning tool capabilities with their existing infrastructure, operational responsibilities, and security goals.

Engagement Objectives

- Deploy Tenable Web App Scanning within Online Retailer's existing Vulnerability Management ecosystem
- Scan up to 10 web applications to provide a baseline of vulnerability posture
- Tune and optimize 3 selected applications for in-depth, high-fidelity scanning
- Enable internal stakeholders to manage, schedule, and interpret scan results
- Configure appropriate authentication, access roles, and operational governance

Strategic Priorities

- **Operational Scanning Capability:** Online Retailer wanted to immediately operationalize Tenable WAS with the ability to run credentialed and unauthenticated scans across multiple environments.
- **Authenticated Access Coverage:** Some applications required Selenium-based login flows to access protected content. Online Retailer emphasized securing authenticated areas as part of the scan scope.



Address:
1000 Brickell Av, Suite 1015
Miami, FL 33131



Phone:
+1 (786) 397-0480



Mail:
info@mpivpartners.com

- **Internal Ownership Enablement:** The team prioritized training and RBAC setup to empower InfoSec, DevOps, and QA stakeholders with self-service scan management and visibility.
 - **Scan Optimization:** Reducing false positives and ensuring complete scan coverage for multi-layered web applications was critical for Online Retailer 's lean security team.
 - **Platform Integration and Continuity:** Ensuring that all scanning tools were properly deployed, secured, and documented for continuity and future auditability.
-

Approach

Our consultants delivered the deployment in alignment with a four-phase service model:

Phase 1: Preparation and Planning

- Conducted a pre-engagement call to verify prerequisites such as user access, scanner connectivity, and firewall exceptions.
- Gathered initial scan targets and prioritized up to 10 business-critical applications across environments (Dev, QA, Prod).
- Reviewed login types, identifying apps requiring Selenium scripts versus form or cookie-based authentication.
- Validated that two on-prem scanners were pre-deployed and operational.

Phase 2: Initialization and Scanning

- Validated connectivity to Vulnerability Management Tool and integration of WAS scanners.
- Configured Role-Based Access Control (RBAC) including Admin, Scan Operator, and Basic roles to reflect Online Retailer's security hierarchy.
- Executed Quick Scans on five key applications using optimized templates to evaluate:
 - Component vulnerabilities
 - HTTP security headers
 - SSL/TLS configurations
 - OWASP Top 10 risks
- Selected three applications for in-depth scanning and configured Overview Scans using detailed sitemap analysis.

Phase 3: Tuning and Optimization

- Performed scan tuning and configuration on three applications using Selenium and form-based login



Address:
1000 Brickell Av, Suite 1015
Miami, FL 33131



Phone:
+1 (786) 397-0480



Mail:
info@mpivpartners.com

- Optimized crawler behavior, login session tracking, and scan scope to improve efficiency and reduce noise.
- Reviewed authentication regexes, session verification, and scan exclusion settings with Online Retailer engineers.
- Provided recommendations for scheduling and scan frequency based on deployment cadences (e.g., weekly for test, monthly for production).

Phase 4: Documentation and Knowledge Transfer

- Delivered a final engagement document with:
 - Full list of scanned URLs and scan types (quick vs. in-depth)
 - Authentication configuration by app
 - Recommendations for RBAC, scheduling, and maintenance
 - Guidance on leveraging Tenable dashboards and exports (PDF, CSV, JSON, etc.)
- Aligned scan reporting with Online Retailer's operational workflows, including future integrations into CI/CD and change windows.

Results & Impact

- **Operational Scanning Achieved:** The organization now actively scans key applications with both unauthenticated and credentialed profiles.
- **Security Coverage Improved:** Apps protected by login flows are now included in the vulnerability management lifecycle.
- **RBAC Successfully Implemented:** Admins, operators, and basic users have defined access levels to perform their duties without overprovisioning.
- **Scan Quality Enhanced:** After tuning, scan noise was reduced and critical plugin families were prioritized.
- **Documentation Delivered:** Online Retailer has a blueprint for expanding WAS coverage and maintaining the platform internally.

Customer Feedback

"The engagement was professional, well-paced, and packed with actionable insights. We now have a clear path forward for managing application risk at scale."

— **Cybersecurity Team Lead**, Online Retailer

**Address:**

1000 Brickell Av, Suite 1015
Miami, FL 33131

**Phone:**

+1 (786) 397-0480

**Mail:**

info@mpivpartners.com