

Health Assessment / Vulnerability Scanning IBM AppScan

Comprehensive Vulnerability Assessment

This offering is designed to accommodate medium to large applications. Encore tests the application using a combination of AppScan and manual security testing methods. The resulting data is cleansed, evaluated for risk and the client is given an actionable remediation report. This offering is comparable to an application level security test.

Encore will spend up to at least 1 working week testing the application on the Comprehensive Vulnerability Assessment.

Scan Preparation

- Encore meets with client for initial analysis and requirements gathering
- Information about test criteria gathered and approved by stakeholders. This includes identifying the Application and agreeing on test window
- Project management and administration

Scanning & Verification

- Encore performs automated Assessment
- Encore filters false positives from results
- Encore will conduct a Risk Analysis to ensure the issues are rated appropriately

Manual Testing

- Encore conducts manual tests to enhance the findings identified. This will include exploitation of identified findings and producing examples to enhance reports.
- This will include running of additional tools which will include the following:
 - Customer authentication & password policy checks
 - Escalation of privilege
 - Token analysis

Reporting

- Encore produces hard copy results report for client.
- Encore conducts results review meeting with customer using AppScan and Connect Session to highlight issues
- Encore releases the AppScan file for client's potential future use