

## Health Assessment / Vulnerability Scanning IBM AppScan

### Basic Vulnerability Assessment

This is the entry level AppScan offering and is designed to cater to small applications. Encore tests the application using AppScan, cleanses the resulting data, and then produces an actionable remediation report.

Encore will spend at least 3 days testing the application on the Basic Vulnerability Assessment.

#### Scan Preparation

- Encore will meet 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.

#### Reporting

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

# 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

## Health Assessment / Vulnerability Scanning

# Advanced Application Penetration Test

This is the premium offering of the Encore AppScan vulnerability assessment. It is designed to accommodate the largest and most complex applications. Encore tests the application using a combination of AppScan and manual methods, and also spends a considerable amount of time attempting to exploit all vulnerabilities in line with PCI Requirements. The resulting data is cleansed and the client is given an actionable remediation report.

Encore will spend at least 2 working weeks testing the application on the Advanced Application Penetration Test.

### 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.
- Additional 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.
  - Brute force attacks.
  - Escalation of privilege.
  - Token analysis.
- Manual tests to verify against PCI guidelines for applications specifically;
  - Section 6.5 (secure code guidelines).
  - Section 6.6 (known web attacks).
  - Section 8 (Password control and best practice).

### 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.

### Follow up

- Encore will re-test the application for free within 30 days of original scan date. This will include a rescan of application and verification of manual findings.



	Basic Vulnerability Assessment	Comprehensive Vulnerability Assessment	Advanced Application Pen Test
Run automated scan using AppScan	YES	YES	YES
Validate issues / filter false positives from results	YES	YES	YES
Conduct additional manual testing and verification	NO	YES	YES
Conduct exploitation testing including:	NO	YES	YES
<input type="checkbox"/> Customer authentication & password policy checks	NO	YES	YES
<input type="checkbox"/> Brute force attacks	NO	YES	YES
<input type="checkbox"/> Escalation of privilege	NO	YES	YES
<input type="checkbox"/> Token analysis	NO	YES	YES
<input type="checkbox"/> Manual tests against secure coding guidelines in accordance to PCI Section 6.5	NO	NO	YES
<input type="checkbox"/> Manual tests against known Web attacks in accordance to PCI Section 6.6	NO	NO	YES
<input type="checkbox"/> Password Control in accordance to PCI Section 8	NO	NO	YES
Conduct custom risk analysis of findings	YES	YES	YES
Prioritize findings for remediation	YES	YES	YES
Deliver detailed results report	YES	YES	YES
Provide saved AppScan file to client (if desired)	YES	YES	YES
Review final results report with client	YES	YES	YES
Re-test verification (within 30 days)	NO	NO	YES
Application re-scan (within 30 days)	NO	NO	YES

Basic Vulnerability Assessment	Comprehensive Vulnerability Assessment	Advanced Application Pen Test
3 Days	1 Week	2 Weeks

