

## 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.

