IBM AppScan - Web Application Vulnerability Testing

What is AppScan

IBM Rational Appscan is a web application security testing tool. Currently OIT has 2 machines with Appscan Standard Edition available.

How it works

AppScan begins its work by recording (exploring) the "good" cases of the web application and generates test cases based on defined policies. AppScan is capable of scanning both the web server and its deployed web applications.

OIT AppScan Test Process

The following diagram shows OIT AppScan Test Process:

Scan Result

Requesting an AppScan Test

If you would like your application scanned, please visit the official request form page via ServiceNow. Once approved, a security engineer will schedule a meeting to go over the application. Prior to this meeting please provide the following via the request form:

1. The URL of the application
2. The test user account to be used. A single user is preferable as using multiple users requires multiple tests which exponentially delays scan from completely as each user is added.
3. Any portions of the application that should not be tested (because they post to external systems, for example)

During the meeting, be prepared to:
1. Point out any areas that might not be obvious. This might include hard to distinguish links, image links, multi-step operations, etc.
2. Setup a dedicated time to run the test. During this period no development can be done.
3. Setup a road map for testing in terms of how soon the scan needs to be completed.

Before the test:

1. **Make sure nobody will be using the web server during the test.** It will be unusable and it will stop the test.
2. **Make sure appscan can reach your application.** This includes modifying any IP restrictions and/or firewall rules. The IP address running the scan is 128.200.141.85 or 128.195.161.52.
3. Turn on "debugging" mode for your app to prevent thousands of emails from being sent.