

Project Title: Web Application Security Assessment Report

Questions Received

- What is the hardware platform(s) that the Custom Data Access application is hosted on?
x86 -- MDH would discuss specific information about the hardware platform directly with the vendor.
- What is the database platform that the Custom Data Access application uses?
The application uses the PostgreSQL platform.
- What programming language is the Custom Data Access application written in?
The application is written in Java.
- What (if any) application server is used by the application?
The application resides on an Apache Tomcat server.
- Are there any other system software components used by the application?
No
- How many tiers does the application have?
The application consists of a client, server, and database.
 - Are there firewalls between the tiers?
Yes -- Firewalls exist between each layer.
 - Are the tiers on separate network segments
Yes
- Is there a DMZ? What components of the application reside in the DMZ?
MDH would discuss specific information about the DMZ(s) directly with the vendor.
- Will the testing be performed against the production environment, or a test environment?
Testing would be performed against a replicated test environment.

- Will we be able to test during the normal business day, or will we need to test after hours?

Testing should be performed during normal business hours (e.g., 8 AM-5 PM).

- Is the testing only from an external perspective? If yes, how many web-applications or URLs are in scope?

Yes -- this external perspective includes both non-authenticated and authenticated external users; see below for more information. The testing would be done on one application (1 root URL).

- Also, please provide number of active IP addresses that are in scope for network layer testing?

Only 1 IP address is in scope.

- Will this be only unauthenticated testing? Or, will there be authenticated testing?

Both -- MDH is asking the vendor to access data as an unauthenticated, unauthorized entity anonymously accessing the application, and then as a fully authenticated and authorized user.

- If authenticated testing is in scope, will the testing be done on a replicated test environment or in production environment?

Testing would be performed against a replicated test environment.

- If MDH is looking for authenticated testing, how many applications will be tested? Are they web-input form apps, web-services, flash components?

Custom Data Access is considered 1 application, which includes some web input forms. MDH would discuss specific information about web services directly with the vendor.

- If authenticated testing is in-scope, please provide number of web-input forms, web service methods, user profiles (admin, user)?

Authenticated testing would include no more than 5 web input forms and include 1 or 2 defined user roles. MDH would discuss specific information about web services directly with the vendor.