DISA STIG Compliance: Application Security and Development

ConfApp - 1.0

ENTERPRISE SECURITY

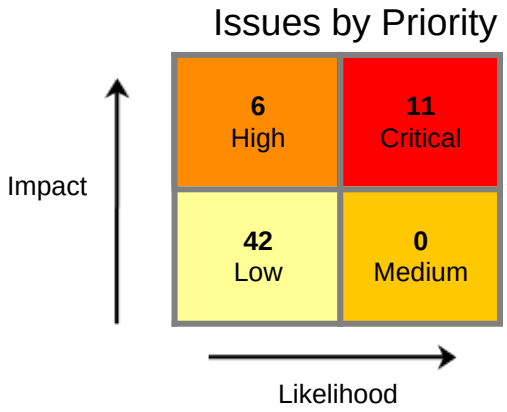
Table of Contents

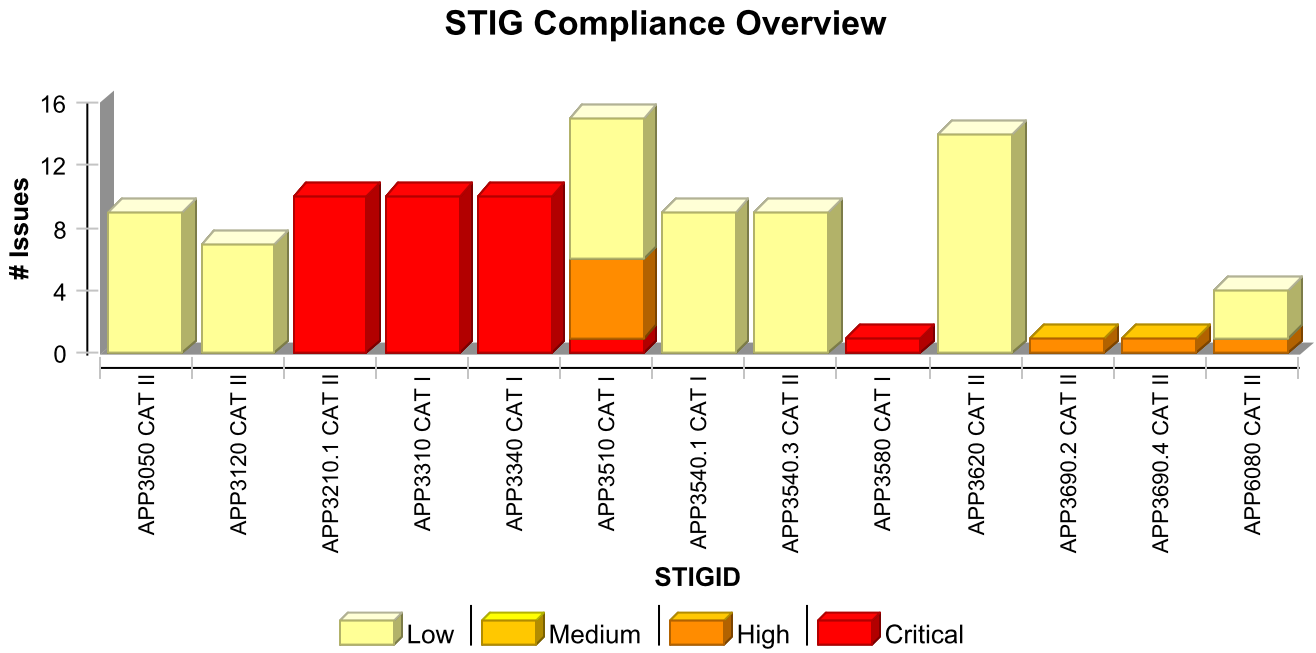
Executive Summary

The following is a summary of the design and development portions of Defence Information Systems Agency (DISA) Application Security and Development Security Technical Implementation Guide (STIG) v3.4. HP Fortify tests for 45 application security related STIGIDs from section 3 of the STIG and reports whether each STIGID is *In Place* or *Not In Place* to indicate whether STIGID related tasks are satisfied or not. This report identifies the specific issues in the application(s) which violate the requirements of DISA STIG 3.4. The information contained in this report is targeted at Application Development Program Managers, Application Designers, Release Managers, Security Managers (SMs), Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators.*

Project Name:	ConfApp
Project Version:	1.0
SCA:	Results Present
WebInspect:	Results Not Present
SecurityScope:	Results Not Present
Other:	Results Not Present

Vulnerability Severity	# of Issues**
CAT I	45
CAT II	55





** The detailed sections following the Executive Summary contain specifics. Key terminology is defined in Appendix A.*
*** The issue counts for Vulnerability Severity and the STIG Compliance Overview table include overcounting of actual issues, as compared to the actual issue count displayed in the Issue by Priority grid, since an issue typcially can belong to more than one STIGID.*

DISA STIG Compliance

The Application Security and Development Security Technical Implementation Guide (STIG) provides security guidance for use throughout the application development lifecycle. This STIG provides the guidance needed to promote the development, integration, and updating of secure applications. Subjects covered in this document are: development, design, testing, conversions and upgrades for existing applications, maintenance, software configuration management, education, and training. Defense Information Systems Agency (DISA) encourages sites to use these guidelines as early as possible in the application development process. Some vulnerabilities may require significant application changes to correct. The earlier the STIG requirements are integrated into the development lifecycle, the less disruptive the remediation process will be.*

Project Description

SCA

Date of Last Analysis:	Nov 6, 2012 10:13 AM	**Engine Version:**	5.14.0.0034
Host Name:	MDE0-E-4-000203	**Certification:**	VALID
Number of Files:	103	**Lines of Code:**	5,162

Accessibility	Internal Network Access Required
Authentication System	None
Business Risk	High
Business Unit	North America
Data Classification	Confidential Data
Development Languages	Java
Development Phase	Active Development
Development Strategy	Internally Developed
Interfaces	Programmatic API
Known Compliance Obligations	FISMA
Project Classification	Corporate
Project Type	Application
Target Deployment Platform	Platform Neutral

**References:*
http://www.hpenterprisesecurity.com
http://iase.disa.mil/stigs/app_security

Issue Breakdown by STIG 3.4

Each requirement or recommendation identified by the DISA STIG is represented by a STIG identifier (STIGID) which corresponds to a checklist item and a severity code [APP*ID*: CAT *SEV*]. DISA STIG identifies several severities with respect to vulnerabilities:

- CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.
- CAT II: provide information that have a high potential of giving access to an intruder.
- CAT III: provide information that potentially could lead to compromise.

The following table summarizes the number of issues identified accross the different STIGIDs and broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

STIGID	Priority				Total Issues*	Status
	Critical	High	Medium	Low		
APP2060.4 CAT II	0	0	0	0	0	In Place
APP3050 CAT II	0	0	0	9	9	Not In Place
APP3120 CAT II	0	0	0	7	7	Not In Place
APP3150.1 CAT II	0	0	0	0	0	In Place
APP3150.2 CAT II	0	0	0	0	0	In Place
APP3210.1 CAT II	10	0	0	0	10	Not In Place
APP3230.2 CAT II	0	0	0	0	0	In Place
APP3250.1 CAT I	0	0	0	0	0	In Place
APP3250.2 CAT I	0	0	0	0	0	In Place
APP3250.3 CAT II	0	0	0	0	0	In Place
APP3250.4 CAT II	0	0	0	0	0	In Place
APP3305 CAT I	0	0	0	0	0	In Place
APP3310 CAT I	10	0	0	0	10	Not In Place
APP3320.5 CAT II	0	0	0	0	0	In Place
APP3330 CAT I	0	0	0	0	0	In Place
APP3340 CAT I	10	0	0	0	10	Not In Place
APP3350 CAT I	0	0	0	0	0	In Place
APP3405 CAT I	0	0	0	0	0	In Place
APP3415 CAT II	0	0	0	0	0	In Place
APP3460 CAT I	0	0	0	0	0	In Place
APP3470.1 CAT II	0	0	0	0	0	In Place
APP3470.4 CAT II	0	0	0	0	0	In Place
APP3480.1 CAT II	0	0	0	0	0	In Place
APP3480.2 CAT II	0	0	0	0	0	In Place
APP3500 CAT II	0	0	0	0	0	In Place
APP3510 CAT I	1	5	0	9	15	Not In Place
APP3540.1 CAT I	0	0	0	9	9	Not In Place
APP3540.3 CAT II	0	0	0	9	9	Not In Place
APP3550 CAT I	0	0	0	0	0	In Place
APP3560 CAT I	0	0	0	0	0	In Place

STIGID	Priority				Total Issues*	Status
	Critical	High	Medium	Low		
APP3570 CAT I	0	0	0	0	0	In Place
APP3580 CAT I	1	0	0	0	1	Not In Place
APP3585 CAT II	0	0	0	0	0	In Place
APP3590.1 CAT I	0	0	0	0	0	In Place
APP3590.2 CAT II	0	0	0	0	0	In Place
APP3600 CAT II	0	0	0	0	0	In Place
APP3610 CAT I	0	0	0	0	0	In Place
APP3620 CAT II	0	0	0	14	14	Not In Place
APP3630.1 CAT II	0	0	0	0	0	In Place
APP3680.4 CAT II	0	0	0	0	0	In Place
APP3680.5 CAT II	0	0	0	0	0	In Place
APP3690.2 CAT II	0	1	0	0	1	Not In Place
APP3690.4 CAT II	0	1	0	0	1	Not In Place
APP3810 CAT I	0	0	0	0	0	In Place
APP6080 CAT II	0	1	0	3	4	Not In Place

** Reported issues in the above table may violate more than one STIG 3.4 requirement. As such, the same issue may appear in more than one row. The total number of unique vulnerabilities are reported in the executive summary table.*

STIG 3.4 Issue Details

Below is an enumeration of all issues found in the project. The issues are organized by STIG 3.4, Fortify Priority Order, and vulnerability category. If the detailed view was chosen for the report the issues are then further broken down by the package, namespace, or location in which they occur. The priority of an issue can be Critical, High, Medium, or Low. Issues reported at the same line number with the same category originate from different taint sources.

Critical-priority issues have high impact and high likelihood. Critical-priority issues are easy to detect and exploit and result in large asset damage. These issues represent the highest security risk to the application. As such, they should be remediated immediately.

High-priority issues have high impact and low likelihood. High-priority issues are often difficult to detect and exploit, but can result in large asset damage. These issues represent a high security risk to the application. High-priority issues should be remediated in the next scheduled patch release.

Medium-priority issues have low impact and high likelihood. Medium-priority issues are easy to detect and exploit, but typically result in small asset damage. These issues represent a moderate security risk to the application. Medium-priority issues should be remediated in the next scheduled product update.

Low-priority issues have low impact and low likelihood. Low-priority issues can be difficult to detect and exploit and typically result in small asset damage. These issues represent a minor security risk to the application. Low-priority issues should be remediated as time allows.

APP2060.4 CAT II

STIGID APP2060.4: CAT II states: "The Designer will not use unsafe functions documented in the project coding standards."

No Issues

APP3050 CAT II

STIGID APP3050: CAT II states: "The Designer will ensure the application does not contain source code that is never invoked during operation, except for software components and libraries from approved third-party products, which may include un-invoked code."

Dead Code: Expression is Always true — Low

Package: bah.conference.appliation.database.quick

Location	Analysis Info	Analyzer
TouchImageView.java:73	**Sink:** IfStatement **Enclosing Method:** TouchImageView()	SCA

Dead Code: Unused Method — Low

Package: bah.conference.appliation.database

Location	Analysis Info	Analyzer
Local.java:56	**Sink:** Function: excStatements **Enclosing Method:** excStatements()	SCA

Poor Style: Value Never Read — Low

Package: bah.conference.appliation.MenuItems

Location	Analysis Info	Analyzer
Speakers.java:115	**Sink:** VariableAccess: height **Enclosing Method:** onClick()	SCA
Speakers.java:116	**Sink:** VariableAccess: width **Enclosing Method:** onClick()	SCA

Package: bah.conference.appliation.dataStructures

Location	Analysis Info	Analyzer
ScheduleItem2.java:117	**Sink:** VariableAccess: m **Enclosing Method:** formatTime()	SCA
ScheduleItem2.java:152	**Sink:** VariableAccess: m **Enclosing Method:** formatYearMonthDay()	SCA
ScheduleItem2.java:159	**Sink:** VariableAccess: h **Enclosing Method:** formatYearMonthDay()	SCA

Poor Style: Value Never Read	Low

Package: bah.conference.appliation.dialogs

Location	Analysis Info	Analyzer
ComboDialog.java:102	**Sink:** VariableAccess: worked **Enclosing Method:** onClick()	SCA
NoteDetails.java:46	**Sink:** VariableAccess: worked **Enclosing Method:** hide()	SCA

APP3120 CAT II

STIGID APP3120: CAT II states: "The Designer will ensure the application is not subject to error handling vulnerabilities."

Poor Error Handling: Empty Catch Block	Low

Package: bah.conference.appliation.web

Location	Analysis Info	Analyzer
Network.java:49	**Sink:** CatchBlock **Enclosing Method:** grabFeed()	SCA
Network.java:50	**Sink:** CatchBlock **Enclosing Method:** grabFeed()	SCA
Network.java:83	**Sink:** CatchBlock **Enclosing Method:** getSchedule2()	SCA
Network.java:84	**Sink:** CatchBlock **Enclosing Method:** getSchedule2()	SCA
Network.java:159	**Sink:** CatchBlock **Enclosing Method:** getExhibitors()	SCA
Network.java:160	**Sink:** CatchBlock **Enclosing Method:** getExhibitors()	SCA

Poor Error Handling: Overly Broad Catch	Low

Package: bah.conference.appliation.dialogs

Location	Analysis Info	Analyzer
BioDetails.java:66	**Sink:** CatchBlock **Enclosing Method:** getResId()	SCA

APP3150.1 CAT II

STIGID APP3150.1: CAT II states: "The Designer will ensure the application uses FIPS 140-2 validated cryptographic modules if the application implements encryption, key exchange, digital signature, and hash functionality."

No Issues

APP3150.2 CAT II

STIGID APP3150.2: CAT II states: "The Designer will ensure the application uses a FIPS 140-2 validated random number generator to support cryptographic functions."

No Issues

APP3210.1 CAT II

STIGID APP3210.1: CAT II states: "The Designer will ensure NIST-certified cryptography is used to protect stored sensitive information if required by the information owner."

Privacy Violation		Critical
Package: bah.conference.appliation		
Location	**Analysis Info**	**Analyzer**
MainActivity.java:102	**Sink:** java.io.Writer.write() **Enclosing Method:** outputToFile() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getBo oths() **In** src/bah/conference/appliation/ database/Local.java:499	SCA
MainActivity.java:107		SCA

Privacy Violation		Critical
Package: bah.conference.appliation		
Location	**Analysis Info**	**Analyzer**
	Sink: android.util.Log.wtf() **Enclosing Method:** outputToFile() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getBo oths() **In** src/bah/conference/appliation/ database/Local.java:499	
MainActivity.java:108	**Sink:** java.io.PrintStream.println() **Enclosing Method:** outputToFile() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getBo oths() **In** src/bah/conference/appliation/ database/Local.java:499	SCA
MainActivity.java:117	**Sink:** android.app.Activity.startActivity() **Enclosing Method:** outputToFile() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getBo oths() **In** src/bah/conference/appliation/ database/Local.java:499	SCA
Package: bah.conference.appliation.MenuItems		
Location	**Analysis Info**	**Analyzer**
Favorites.java:76	**Sink:** android.app.Activity.startActivity() **Enclosing Method:** onClick() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getFa voriteTimeSlots() **In** src/bah/conference/ appliation/database/Local.java:337	SCA
Notes.java:75	**Sink:** android.app.Activity.startActivity() **Enclosing Method:** onClick() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getSc hedule2TimeSlots() **In** src/bah/conference/ appliation/database/Local.java:403	SCA

Privacy Violation		Critical
Package: bah.conference.appliation.database.quick		
Location	**Analysis Info**	**Analyzer**
TouchImageView.java:360	**Sink:** android.widget.Toast.setText() **Enclosing Method:** doWork() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getEx hibitor() **In** src/bah/conference/appliation/ database/Local.java:555	SCA
Package: bah.conference.appliation.dialogs		
Location	**Analysis Info**	**Analyzer**
BioDetails.java:38	**Sink:** android.widget.TextView.setText() **Enclosing Method:** initialize() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getBi oItem() **In** src/bah/conference/appliation/ database/Local.java:447	SCA
NoteDetails.java:34	**Sink:** android.widget.TextView.setText() **Enclosing Method:** initialize() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getSc hedule2Item() **In** src/bah/conference/ appliation/database/Local.java:349	SCA
ScheduleItemDetails.java:27	**Sink:** android.widget.TextView.setText() **Enclosing Method:** initialize() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getSc hedule2Item() **In** src/bah/conference/ appliation/database/Local.java:349	SCA

APP3230.2 CAT II

STIGID APP3230.2: CAT II states: "The Designer will ensure the application properly clears or overwrites all memory blocks used to classified data."

No Issues

APP3250.1 CAT I

STIGID APP3250.1: CAT I states: "The Designer will ensure unclassified, sensitive data transmitted through a commercial or wireless network is protected using NIST-certified cryptography."

No Issues

APP3250.2 CAT I

STIGID APP3250.2: CAT I states: "The Designer will ensure classified data, transmitted through a network that is cleared to a lower level than the data being transmitted, is separately protected using NSA approved cryptography."

No Issues

APP3250.3 CAT II

STIGID APP3250.3: CAT II states: "The Designer will ensure information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, is protected minimally with NIST-certified cryptography."

No Issues

APP3250.4 CAT II

STIGID APP3250.4: CAT II states: "The Designer will ensure SAMI information in transit through a network at the same classification level is protected with NSA-approved cryptography."

No Issues

APP3305 CAT I

STIGID APP3305: CAT I states: "The Designer will ensure the application using PKI validates certificates for expiration, confirms origin is from a DoD-authorized CA, and verify certificate has not been revoked by CRL or OCSP, and CRL cache (if used) is updated at least daily."

No Issues

APP3310 CAT I

STIGID APP3310: CAT I states: "The Designer will ensure the application does not display account passwords as clear text."

Privacy Violation		Critical
Package: bah.conference.appliation		
Location	**Analysis Info**	**Analyzer**
MainActivity.java:102	**Sink:** java.io.Writer.write() **Enclosing Method:** outputToFile() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getBo oths() **In** src/bah/conference/appliation/ database/Local.java:499	SCA
MainActivity.java:107	**Sink:** android.util.Log.wtf() **Enclosing Method:** outputToFile() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getBo oths() **In** src/bah/conference/appliation/ database/Local.java:499	SCA
MainActivity.java:108	**Sink:** java.io.PrintStream.println() **Enclosing Method:** outputToFile() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getBo oths() **In** src/bah/conference/appliation/ database/Local.java:499	SCA
MainActivity.java:117		SCA

Privacy Violation

Critical

Package: bah.conference.appliation

Location	Analysis Info	Analyzer
	Sink: android.app.Activity.startActivity() **Enclosing Method:** outputToFile() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getBo oths() **In** src/bah/conference/appliation/ database/Local.java:499	

Package: bah.conference.appliation.MenuItems

Location	Analysis Info	Analyzer
Favorites.java:76	**Sink:** android.app.Activity.startActivity() **Enclosing Method:** onClick() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getFa voriteTimeSlots() **In** src/bah/conference/ appliation/database/Local.java:337	SCA
Notes.java:75	**Sink:** android.app.Activity.startActivity() **Enclosing Method:** onClick() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getSc hedule2TimeSlots() **In** src/bah/conference/ appliation/database/Local.java:403	SCA

Package: bah.conference.appliation.database.quick

Location	Analysis Info	Analyzer
TouchImageView.java:360	**Sink:** android.widget.Toast.setText() **Enclosing Method:** doWork() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getEx hibitor() **In** src/bah/conference/appliation/ database/Local.java:555	SCA

Package: bah.conference.appliation.dialogs

Location	Analysis Info	Analyzer
BioDetails.java:38		SCA

Privacy Violation		Critical
Package: bah.conference.appliation.dialogs		
Location	**Analysis Info**	**Analyzer**
	Sink: android.widget.TextView.setText() **Enclosing Method:** initialize() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getBi oItem() **In** src/bah/conference/appliation/ database/Local.java:447	
NoteDetails.java:34	**Sink:** android.widget.TextView.setText() **Enclosing Method:** initialize() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getSc hedule2Item() **In** src/bah/conference/ appliation/database/Local.java:349	SCA
ScheduleItemDetails.java:27	**Sink:** android.widget.TextView.setText() **Enclosing Method:** initialize() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getSc hedule2Item() **In** src/bah/conference/ appliation/database/Local.java:349	SCA

APP3320.5 CAT II

STIGID APP3320.5: CAT II states: "The Designer will ensure the application has the capability to limit reuse of account passwords within the last 10 password changes."

No Issues

APP3330 CAT I

STIGID APP3330: CAT I states: "The Designer will ensure the application transmits account passwords in an approved encrypted format."

No Issues

APP3340 CAT I

STIGID APP3340: CAT I states: "The Designer will ensure the application stores account passwords in an approved encrypted format."

Privacy Violation		Critical
Package: bah.conference.appliation		
Location	**Analysis Info**	**Analyzer**
MainActivity.java:102	**Sink:** java.io.Writer.write() **Enclosing Method:** outputToFile() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getBo oths() **In** src/bah/conference/appliation/ database/Local.java:499	SCA
MainActivity.java:107	**Sink:** android.util.Log.wtf() **Enclosing Method:** outputToFile() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getBo oths() **In** src/bah/conference/appliation/ database/Local.java:499	SCA
MainActivity.java:108	**Sink:** java.io.PrintStream.println() **Enclosing Method:** outputToFile() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getBo oths() **In** src/bah/conference/appliation/ database/Local.java:499	SCA
MainActivity.java:117	**Sink:** android.app.Activity.startActivity() **Enclosing Method:** outputToFile() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getBo oths() **In** src/bah/conference/appliation/ database/Local.java:499	SCA

Privacy Violation — Critical

Package: bah.conference.appliation.MenuItems

Location	Analysis Info	Analyzer
Favorites.java:76	**Sink:** android.app.Activity.startActivity() **Enclosing Method:** onClick() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getFa voriteTimeSlots() **In** src/bah/conference/ appliation/database/Local.java:337	SCA
Notes.java:75	**Sink:** android.app.Activity.startActivity() **Enclosing Method:** onClick() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getSc hedule2TimeSlots() **In** src/bah/conference/ appliation/database/Local.java:403	SCA

Package: bah.conference.appliation.database.quick

Location	Analysis Info	Analyzer
TouchImageView.java:360	**Sink:** android.widget.Toast.setText() **Enclosing Method:** doWork() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getEx hibitor() **In** src/bah/conference/appliation/ database/Local.java:555	SCA

Package: bah.conference.appliation.dialogs

Location	Analysis Info	Analyzer
BioDetails.java:38	**Sink:** android.widget.TextView.setText() **Enclosing Method:** initialize() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getBi oItem() **In** src/bah/conference/appliation/ database/Local.java:447	SCA
NoteDetails.java:34		SCA

Privacy Violation		Critical
Package: bah.conference.appliation.dialogs		
Location	**Analysis Info**	**Analyzer**
	Sink: android.widget.TextView.setText() **Enclosing Method:** initialize() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getSc hedule2Item() **In** src/bah/conference/ appliation/database/Local.java:349	
ScheduleItemDetails.java:27	**Sink:** android.widget.TextView.setText() **Enclosing Method:** initialize() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getSc hedule2Item() **In** src/bah/conference/ appliation/database/Local.java:349	SCA

APP3350 CAT I

STIGID APP3350: CAT I states: "The Designer will ensure the application does not contain embedded authentication data."

No Issues

APP3405 CAT I

STIGID APP3405: CAT I states: "The Designer will ensure the application supports detection and/or prevention of communication session hijacking."

No Issues

APP3415 CAT II

STIGID APP3415: CAT II states: "The Designer will ensure the application provides a capability to automatically terminate a session and logout after a system defined session idle time limit is exceeded."

No Issues

APP3460 CAT I

STIGID APP3460: CAT I states: "The Designer will ensure the application does not rely solely on a resource name to control access to a resource."

No Issues

APP3470.1 CAT II

STIGID APP3470.1: CAT II states: "The Designer will ensure the application is organized by functionality and roles to support the assignment of specific roles to specific application functions."

No Issues

APP3470.4 CAT II

STIGID APP3470.4: CAT II states: "The IAO will ensure the application account is established and administered in accordance with a role-based access scheme to enforce least privilege and separation of duties."

No Issues

APP3480.1 CAT II

STIGID APP3480.1: CAT II states: "The Designer will ensure access control mechanisms exist to ensure data is accessed and changed only by authorized personnel."

No Issues

APP3480.2 CAT II

STIGID APP3480.2: CAT II states: "The Designer will ensure the access procedures enforce the principles of separation of duties and "least privilege"."

No Issues

APP3500 CAT II

STIGID APP3500: CAT II states: "The Designer will ensure the application executes with no more privileges than necessary for proper operation."

No Issues

APP3510 CAT I

STIGID APP3510: CAT I states: "The Designer will ensure the application validates all input."

Cross-Site Scripting: Persistent — Critical

Package: bah.conference.appliation.database.quick

Location	Analysis Info	Analyzer
TouchImageView.java:360	**Sink:** android.widget.Toast.setText() **Enclosing Method:** doWork() **Source:** android.database.sqlite.SQLiteDatabase .rawQue() **from** bah.conference.appliation.database.Local.getExhibitor() **In** src/bah/conference/appliation/database/Local.java:555	SCA

Access Control: Database — High

Package: bah.conference.appliation.database

Location	Analysis Info	Analyzer
Local.java:292		SCA

Access Control: Database — High

Package: bah.conference.appliation.database

Location	Analysis Info	Analyzer
	Sink: android.database.sqlite.SQLiteDatabase.i nsert () **Enclosing Method:** insertRow() **Source:** java.io.BufferedReader.readLine() **from** bah.conference.appliation.web.Network.getExhib itors() **In** src/bah/conference/appliation/web/ Network.java:155	
Local.java:292	**Sink:** android.database.sqlite.SQLiteDatabase.i nsert () **Enclosing Method:** insertRow() **Source:** java.io.BufferedReader.readLine() **from** bah.conference.appliation.web.Network.grabFeed () **In** src/bah/conference/appliation/web/ Network.java:45	SCA
Local.java:292	**Sink:** android.database.sqlite.SQLiteDatabase.i nsert () **Enclosing Method:** insertRow() **Source:** java.io.BufferedReader.readLine() **from** bah.conference.appliation.web.Network.getSched ule2() **In** src/bah/conference/appliation/web/ Network.java:79	SCA
Local.java:555	**Sink:** android.database.sqlite.SQLiteDatabase.r awQuery() **Enclosing Method:** getExhibitor() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getBo othClicked() **In** src/bah/conference/appliation/ database/Local.java:539	SCA

Log Forging — High

Package: bah.conference.appliation

Location	Analysis Info	Analyzer
MainActivity.java:107		SCA

Log Forging		High
Package: bah.conference.appliation		
Location	**Analysis Info**	**Analyzer**
	Sink: android.util.Log.wtf() **Enclosing Method:** outputToFile() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getBo oths() **In** src/bah/conference/appliation/ database/Local.java:499	

SQL Injection		Low
Package: bah.conference.appliation.database		
Location	**Analysis Info**	**Analyzer**
Local.java:54	**Sink:** execSQL() **Enclosing Method:** excStatement()	SCA
Local.java:58	**Sink:** execSQL() **Enclosing Method:** excStatements()	SCA
Local.java:337	**Sink:** rawQuery() **Enclosing Method:** getFavoriteTimeSlots()	SCA
Local.java:349	**Sink:** rawQuery() **Enclosing Method:** getSchedule2Item()	SCA
Local.java:362	**Sink:** rawQuery() **Enclosing Method:** getSchedule2Now()	SCA
Local.java:373	**Sink:** rawQuery() **Enclosing Method:** getSchedule2Previous()	SCA
Local.java:384	**Sink:** rawQuery() **Enclosing Method:** getSchedule2Next()	SCA
Local.java:403	**Sink:** rawQuery() **Enclosing Method:** getSchedule2TimeSlots()	SCA
Local.java:566	**Sink:** rawQuery() **Enclosing Method:** isPopulated()	SCA

APP3540.1 CAT I

STIGID APP3540.1: CAT I states: "The Designer will ensure the application is not vulnerable to SQL injection."

SQL Injection	Low

Package: bah.conference.appliation.database

Location	Analysis Info	Analyzer
Local.java:54	**Sink:** execSQL() **Enclosing Method:** excStatement()	SCA
Local.java:58	**Sink:** execSQL() **Enclosing Method:** excStatements()	SCA
Local.java:337	**Sink:** rawQuery() **Enclosing Method:** getFavoriteTimeSlots()	SCA
Local.java:349	**Sink:** rawQuery() **Enclosing Method:** getSchedule2Item()	SCA
Local.java:362	**Sink:** rawQuery() **Enclosing Method:** getSchedule2Now()	SCA
Local.java:373	**Sink:** rawQuery() **Enclosing Method:** getSchedule2Previous()	SCA
Local.java:384	**Sink:** rawQuery() **Enclosing Method:** getSchedule2Next()	SCA
Local.java:403	**Sink:** rawQuery() **Enclosing Method:** getSchedule2TimeSlots()	SCA
Local.java:566	**Sink:** rawQuery() **Enclosing Method:** isPopulated()	SCA

APP3540.3 CAT II

STIGID APP3540.3: CAT II states: "The Designer will ensure the application does not use concatenation or replacement to build SQL queries."

SQL Injection	Low

Package: bah.conference.appliation.database

Location	Analysis Info	Analyzer
Local.java:54	**Sink:** execSQL() **Enclosing Method:** excStatement()	SCA
Local.java:58	**Sink:** execSQL() **Enclosing Method:** excStatements()	SCA
Local.java:337	**Sink:** rawQuery() **Enclosing Method:** getFavoriteTimeSlots()	SCA
Local.java:349	**Sink:** rawQuery() **Enclosing Method:** getSchedule2Item()	SCA

SQL Injection	Low

Package: bah.conference.appliation.database

Location	Analysis Info	Analyzer
Local.java:362	**Sink:** rawQuery() **Enclosing Method:** getSchedule2Now()	SCA
Local.java:373	**Sink:** rawQuery() **Enclosing Method:** getSchedule2Previous()	SCA
Local.java:384	**Sink:** rawQuery() **Enclosing Method:** getSchedule2Next()	SCA
Local.java:403	**Sink:** rawQuery() **Enclosing Method:** getSchedule2TimeSlots()	SCA
Local.java:566	**Sink:** rawQuery() **Enclosing Method:** isPopulated()	SCA

APP3550 CAT I

STIGID APP3550: CAT I states: "The Designer will ensure the application is not vulnerable to integer arithmetic issues."

No Issues

APP3560 CAT I

STIGID APP3560: CAT I states: "The Designer will ensure the application does not contain format string vulnerabilities."

No Issues

APP3570 CAT I

STIGID APP3570: CAT I states: "The Designer will ensure the application does not allow command injection."

No Issues

APP3580 CAT I

STIGID APP3580: CAT I states: "The Designer will ensure the application does not have XSS vulnerabilities."

Cross-Site Scripting: Persistent		Critical
Package: bah.conference.appliation.database.quick		
Location	**Analysis Info**	**Analyzer**
TouchImageView.java:360	**Sink:** android.widget.Toast.setText() **Enclosing Method:** doWork() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getEx hibitor() **In** src/bah/conference/appliation/ database/Local.java:555	SCA

APP3585 CAT II

STIGID APP3585: CAT II states: "The Designer will ensure the application does not have CSRF vulnerabilities."

No Issues

APP3590.1 CAT I

STIGID APP3590.1: CAT I states: "The Designer will ensure the application does not have buffer overflows."

No Issues

APP3590.2 CAT II

STIGID APP3590.2: CAT I states: "The Designer will ensure the application does not use functions known to be vulnerable to buffer overflows."

No Issues

APP3600 CAT II

STIGID APP3600: CAT II states: "The Designer will ensure the application has no canonical representation vulnerabilities."

No Issues

APP3610 CAT I

STIGID APP3610: CAT I states: "The Designer will ensure the application does not use hidden fields to control user access privileges or as a part of a security mechanism."

No Issues

APP3620 CAT II

STIGID APP3620: CAT II states: "The Designer will ensure the application does not disclose unnecessary information to users."

Poor Logging Practice: Use of a System Output Stream		Low
Package: bah.conference.appliation		
Location	**Analysis Info**	**Analyzer**
MainActivity.java:108	**Sink:** FunctionCall: println **Enclosing Method:** outputToFile()	SCA
Package: bah.conference.appliation.web		
Location	**Analysis Info**	**Analyzer**
Network.java:170	**Sink:** FunctionCall: println **Enclosing Method:** getExhibitors()	SCA
Network.java:172	**Sink:** FunctionCall: println **Enclosing Method:** getExhibitors()	SCA
Network.java:173	**Sink:** FunctionCall: print **Enclosing Method:** getExhibitors()	SCA

System Information Leak		Low
Package: bah.conference.appliation		
Location	**Analysis Info**	**Analyzer**
MainActivity.java:122	**Sink:** printStackTrace() **Enclosing Method:** outputToFile()	SCA
Package: bah.conference.appliation.dataStructures		
Location	**Analysis Info**	**Analyzer**
BioItem.java:49	**Sink:** printStackTrace() **Enclosing Method:** setWithJSON()	SCA
BoothLocation.java:100	**Sink:** printStackTrace() **Enclosing Method:** fromJson()	SCA
NewsItem.java:56	**Sink:** printStackTrace() **Enclosing Method:** setWithJSON()	SCA
Package: bah.conference.appliation.dialogs		
Location	**Analysis Info**	**Analyzer**
BioDetails.java:67	**Sink:** printStackTrace() **Enclosing Method:** getResId()	SCA
BioDetails.java:75	**Sink:** printStackTrace() **Enclosing Method:** getBio()	SCA
Package: bah.conference.appliation.web		
Location	**Analysis Info**	**Analyzer**
Network.java:114	**Sink:** printStackTrace() **Enclosing Method:** grabBios()	SCA
Network.java:117	**Sink:** printStackTrace() **Enclosing Method:** grabBios()	SCA
Network.java:141	**Sink:** printStackTrace() **Enclosing Method:** grabBoothLocations()	SCA
Network.java:144	**Sink:** printStackTrace() **Enclosing Method:** grabBoothLocations()	SCA

APP3630.1 CAT II

STIGID APP3630.1: CAT II states: "The Designer will ensure the application is not vulnerable to race conditions."

No Issues

APP3680.4 CAT II

STIGID APP3680.4: CAT II states: "The Designer will ensure the application's sensitive data audit records include:
- Userid
- Successful and unsuccessful attempts to access security files
- Date and time of the event
- Type of event
- Success or failure of event
- Successful and unsuccessful logons
- Denial of access resulting from excessive number of logon attempts
- Blocking or blacklisting a userid, terminal or access port and the reason for the action
- Activities that might modify, bypass, or negate safeguards controlled by the system."

No Issues

APP3680.5 CAT II

STIGID APP3680.5: CAT II states: "The Designer will ensure the application's classified data audit records include:
- Userid
- Successful and unsuccessful attempts to access security file
- Date and time of the event
- Type of event
- Success or failure of event
- Successful and unsuccessful logons
- Denial of access resulting from excessive number of logon attempts
- Blocking or blacklisting a userid, terminal or access port, and the reason for the action
- Activities that might modify, bypass, or negate safeguards controlled by the system
- Data required to audit the possible use of covert channel mechanisms
- Privileged activities and other system-level access
- Starting and ending time for access to the system
- Security relevant actions associated with periods of activity where security labels or categories of information are processed or changed."

No Issues

APP3690.2 CAT II

STIGID APP3690.2: CAT II states: "The Designer will ensure the audit trail is protected against modification or deletion except by the application and auditors."

Log Forging		High
Package: bah.conference.appliation		
Location	**Analysis Info**	**Analyzer**
MainActivity.java:107	**Sink:** android.util.Log.wtf() **Enclosing Method:** outputToFile() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getBo oths() **In** src/bah/conference/appliation/ database/Local.java:499	SCA

APP3690.4 CAT II

STIGID APP3690.4: CAT II states: "The IAO will ensure the audit trail is protected against modification or deletion except by application administrators and auditors."

Log Forging		High
Package: bah.conference.appliation		
Location	**Analysis Info**	**Analyzer**
MainActivity.java:107	**Sink:** android.util.Log.wtf() **Enclosing Method:** outputToFile() **Source:** android.database.sqlite.SQLiteDatabase .rawQue () **from** bah.conference.appliation.database.Local.getBo oths() **In** src/bah/conference/appliation/ database/Local.java:499	SCA

APP3810 CAT I

STIGID APP3810: CAT I states: "The Designer will ensure the application is not vulnerable to XML injection."

No Issues

APP6080 CAT II

STIGID APP6080: CAT II states: "The IAO will ensure protections against DoS attacks are implemented."

Unreleased Resource: Streams		High
Package: bah.conference.appliation		
Location	**Analysis Info**	**Analyzer**
MainActivity.java:92	**Sink:** writer = new BufferedWriter(new java.io. FileWriter()) **Enclosing Method:** outputToFile()	SCA

Redundant Null Check		Low
Package: bah.conference.appliation.dialogs		
Location	**Analysis Info**	**Analyzer**
ComboDialog.java:87	**Sink:** Dereferenced : details **Enclosing Method:** initialize()	SCA
ComboDialog.java:89	**Sink:** Dereferenced : speaker **Enclosing Method:** initialize()	SCA
ComboDialog.java:92	**Sink:** Dereferenced : notes **Enclosing Method:** initialize()	SCA

Appendix A - Description of Key Terminology

Likelihood and Impact

Likelihood
Likelihood is the probability that a vulnerability will be accurately identified and successfully exploited.

Impact
Impact is the potential damage an attacker could do to assets by successfully exploiting a vulnerability. This damage can be in the form of, but not limited to, financial loss, compliance violation, loss of brand reputation, and negative publicity.

Fortify Priority Order

Critical
Critical-priority issues have high impact and high likelihood. Critical-priority issues are easy to detect and exploit and result in large asset damage. These issues represent the highest security risk to the application. As such, they should be remediated immediately.

SQL Injection is an example of a critical issue.

High
High-priority issues have high impact and low likelihood. High-priority issues are often difficult to detect and exploit, but can result in large asset damage. These issues represent a high security risk to the application. High-priority issues should be remediated in the next scheduled patch release.

Password Management: Hardcoded Password is an example of a high issue.

Medium
Medium-priority issues have low impact and high likelihood. Medium-priority issues are easy to detect and exploit, but typically result in small asset damage. These issues represent a moderate security risk to the application. Medium-priority issues should be remediated in the next scheduled product update.

Path Manipulation is an example of a medium issue.

Low
Low-priority issues have low impact and low likelihood. Low-priority issues can be difficult to detect and exploit and typically result in small asset damage. These issues represent a minor security risk to the application. Low-priority issues should be remediated as time allows.

Dead Code is an example of a low issue.