Security Findings of Project "management-http"

Analysis Date: 2020-06-14 05:47:50

Analyzed Workspace:

Packages:	18	Total LOC:	31,898
Classes:	301	No. of Bytecode Instructions:	124,672

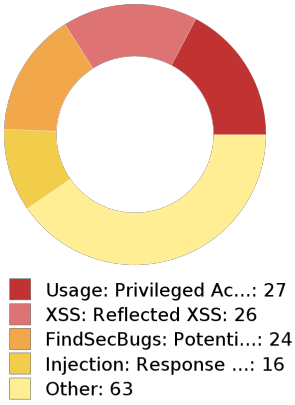
Computed Call Graph:

Classes not in Call Graph:	52	Methods not in Call Graph:	78

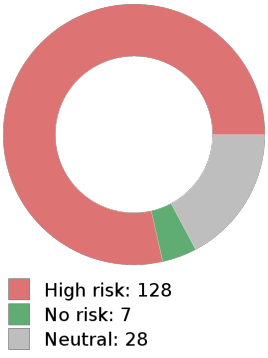
Findings in List:

All Findings:	163	Problematic Findings:	156

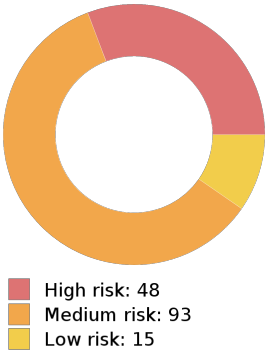
Finding Problem Types:



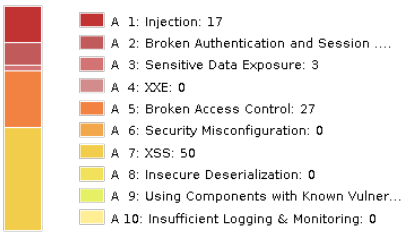
Finding Classifications:



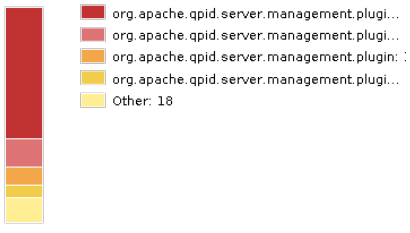
Finding Ratings:



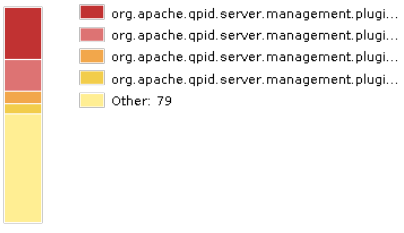
OWASP Top 10 2017



Hot Spots (Packages)



Hot Spots (Classes)



Findings List

Finding ID:	**47**	**Problem Type:**	Injection: Response Header Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):175 <- QueryServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):96		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Response Header Injection' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getParameter(java.lang.String) Matching pattern in taint sink kind 'Response Header Injection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Finding ID:	**46**	**Problem Type:**	Injection: Response Header Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):370 <- AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):101		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Response Header Injection' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'Response Header Injection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Finding ID:	**44**	**Problem Type:**	Injection: Response Header Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):370 <- SaslServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):134		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Response Header Injection' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getParameter(java.lang.String) Matching pattern in taint sink kind 'Response Header Injection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Findings List

Finding ID:	**45**	**Problem Type:**	Injection: Response Header Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):370 <- SaslServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):136		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Response Header Injection' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getParameter(java.lang.String) Matching pattern in taint sink kind 'Response Header Injection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Finding ID:	**48**	**Problem Type:**	Injection: Response Header Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):370 <- SaslServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):298		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Response Header Injection' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'Response Header Injection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Finding ID:	**43**	**Problem Type:**	Injection: Response Header Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):370 <- SaslServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):98		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Response Header Injection' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getRemoteUser() Matching pattern in taint sink kind 'Response Header Injection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Findings List

Finding ID:	**52**	**Problem Type:**	Injection: Response Header Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	4.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):294 <- ConfiguredObjectToMapConverter.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):180		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Response Header Injection' Matching pattern in taint source kind 'Property and Environment Input': static java.util.Map java.lang.System.getenv() Matching pattern in taint sink kind 'Response Header Injection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Finding ID:	**54**	**Problem Type:**	Injection: Response Header Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	4.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):294 <- ConfiguredObjectToMapConverter.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):181		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Response Header Injection' Matching pattern in taint source kind 'Property and Environment Input': static java.util.Properties java.lang.System.getProperties() Matching pattern in taint sink kind 'Response Header Injection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Finding ID:	**56**	**Problem Type:**	Injection: Response Header Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	4.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):294 <- LegacyConfiguredObjectToMapConverter.java (<Source Code>/org/apache/qpid/server/management/plugin/controller):165		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Response Header Injection' Matching pattern in taint source kind 'Property and Environment Input': static java.util.Map java.lang.System.getenv() Matching pattern in taint sink kind 'Response Header Injection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Findings List

Finding ID:	**58**	**Problem Type:**	Injection: Response Header Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	4.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):294 <- LegacyConfiguredObjectToMapConverter.java (<Source Code>/org/apache/qpid/server/management/plugin/controller):166		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Response Header Injection' Matching pattern in taint source kind 'Property and Environment Input': static java.util.Properties java.lang.System.getProperties() Matching pattern in taint sink kind 'Response Header Injection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Finding ID:	**49**	**Problem Type:**	Injection: Response Header Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	4.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):294 <- OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):331		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Response Header Injection' Matching pattern in taint source kind 'Servlet Request Input': java.lang.StringBuffer javax.servlet.ServletRequest.getRequestURL() Matching pattern in taint sink kind 'Response Header Injection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Finding ID:	**51**	**Problem Type:**	Injection: Response Header Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	4.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):370 <- ConfiguredObjectToMapConverter.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):180		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Response Header Injection' Matching pattern in taint source kind 'Property and Environment Input': static java.util.Map java.lang.System.getenv() Matching pattern in taint sink kind 'Response Header Injection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Findings List

Finding ID:	**53**	**Problem Type:**	Injection: Response Header Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	4.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):370 <- ConfiguredObjectToMapConverter.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):181		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Response Header Injection' Matching pattern in taint source kind 'Property and Environment Input': static java.util.Properties java.lang.System.getProperties() Matching pattern in taint sink kind 'Response Header Injection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Finding ID:	**55**	**Problem Type:**	Injection: Response Header Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	4.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):370 <- LegacyConfiguredObjectToMapConverter.java (<Source Code>/org/apache/qpid/server/management/plugin/controller):165		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Response Header Injection' Matching pattern in taint source kind 'Property and Environment Input': static java.util.Map java.lang.System.getenv() Matching pattern in taint sink kind 'Response Header Injection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Finding ID:	**57**	**Problem Type:**	Injection: Response Header Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	4.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):370 <- LegacyConfiguredObjectToMapConverter.java (<Source Code>/org/apache/qpid/server/management/plugin/controller):166		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Response Header Injection' Matching pattern in taint source kind 'Property and Environment Input': static java.util.Properties java.lang.System.getProperties() Matching pattern in taint sink kind 'Response Header Injection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Findings List

Finding ID:	**50**	**Problem Type:**	Injection: Response Header Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	4.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):370 <- OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):331		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Response Header Injection' Matching pattern in taint source kind 'Servlet Request Input': java.lang.StringBuffer javax.servlet.ServletRequest.getRequestURL() Matching pattern in taint sink kind 'Response Header Injection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Finding ID:	**112**	**Problem Type:**	SpotBugs: HTTP Response splitting vulnerability (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	RewriteServlet.java (<Source Code>/org/apache/qpid/server/management/plugin):53		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: HTTP parameter directly written to HTTP header output in org.apache.qpid.server.management.plugin.RewriteServlet.service(HttpServletRequest, HttpServletResponse) - In method org.apache.qpid.server.management.plugin.RewriteServlet.service(HttpServletRequest, HttpServletResponse) - Local variable named location		

Finding ID:	**153**	**Problem Type:**	Hard-Coded Credentials: Username in Variables (Special Code)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	AbstractManagementController.java (<Source Code>/org/apache/qpid/server/management/plugin/controller):43		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Hard-Coded Credentials: Username in Variables'. Literal credential in field 'USER_PREFERENCES'		

Findings List

Finding ID:	**154**	**Problem Type:**	Hard-Coded Credentials: Username in Variables (Special Code)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	AbstractManagementController.java (<Source Code>/org/apache/qpid/server/management/plugin/controller):44		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Hard-Coded Credentials: Username in Variables'. Literal credential in field 'VISIBLE_USER_PREFERENCES'		

Finding ID:	**155**	**Problem Type:**	Hard-Coded Credentials: Username in Variables (Special Code)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	LegacyCategoryControllerFactory.java (<Source Code>/org/apache/qpid/server/management/plugin/controller/v6_1/category):44		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Hard-Coded Credentials: Username in Variables'. Literal credential in field 'CATEGORY_USER'		

Finding ID:	**156**	**Problem Type:**	Hard-Coded Credentials: Username in Variables (Special Code)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	LegacyCategoryControllerFactory.java (<Source Code>/org/apache/qpid/server/management/plugin/controller/v7_0/category):41		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Hard-Coded Credentials: Username in Variables'. Literal credential in field 'CATEGORY_USER'		

Finding ID:	**162**	**Problem Type:**	Hard-Coded Credentials: Username in Variables (Special Code)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	OAuth2InteractiveAuthenticatorTest.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):92		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Hard-Coded Credentials: Username in Variables'. Literal credential in field 'TEST_AUTHORIZED_USER'		

Findings List

Finding ID:	**163**	**Problem Type:**	Hard-Coded Credentials: Username in Variables (Special Code)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	OAuth2InteractiveAuthenticatorTest.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):93		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Hard-Coded Credentials: Username in Variables'. Literal credential in field 'TEST_UNAUTHORIZED_USER'		

Finding ID:	**157**	**Problem Type:**	Hard-Coded Credentials: Username in Variables (Special Code)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	OAuth2PreemptiveAuthenticatorTest.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):52		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Hard-Coded Credentials: Username in Variables'. Literal credential in field 'TEST_AUTHORIZED_USER'		

Finding ID:	**158**	**Problem Type:**	Hard-Coded Credentials: Username in Variables (Special Code)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	OAuth2PreemptiveAuthenticatorTest.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):53		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Hard-Coded Credentials: Username in Variables'. Literal credential in field 'TEST_UNAUTHORIZED_USER'		

Finding ID:	**159**	**Problem Type:**	Hard-Coded Credentials: Username in Variables (Special Code)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	RequestInfoParser.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):38		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Hard-Coded Credentials: Username in Variables'. Literal credential in field 'USER_PREFERENCES'		

Findings List

Finding ID:	**160**	**Problem Type:**	Hard-Coded Credentials: Username in Variables (Special Code)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	RequestInfoParser.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):39		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Hard-Coded Credentials: Username in Variables'. Literal credential in field 'VISIBLE_USER_PREFERENCES'		

Finding ID:	**161**	**Problem Type:**	Hard-Coded Credentials: Username in Variables (Special Code)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):68		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Hard-Coded Credentials: Username in Variables'. Literal credential in field 'MYUSER'		

Finding ID:	**37**	**Problem Type:**	Cryptography: Construction of Secure Random Numbers (Protocol Check Findings)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):354		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Cryptography: Construction of Secure Random Numbers'. The RNG being used has not been properly constructed. Violated protocol: Construction of Strong Random Numbers Protocol description: Constructing strong random numbers. Matching pattern in protocol check kind 'GenerateStronglyRandomBits': void java.security.SecureRandom.nextBytes(byte[])		

Findings List

Finding ID:	**38**	**Problem Type:**	Cryptography: Construction of Secure Random Numbers (Protocol Check Findings)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	SaslServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):116		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Cryptography: Construction of Secure Random Numbers'. The RNG being used has not been properly constructed. Violated protocol: Construction of Strong Random Numbers Protocol description: Constructing strong random numbers. Matching pattern in protocol check kind 'GenerateStronglyRandomBits': long java.security.SecureRandom.nextLong()		

Finding ID:	**36**	**Problem Type:**	Cryptography: Cryptographic Algorithms Used in Project (Special Code)
Classification:	Information	**Date:**	2020-06-14 05:47:50 - new
Rating:	0.00	**Reviewed State:**	Not Reviewed
Location:	ServletConnectionPrincipal.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet):61		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Cryptography: Cryptographic Algorithms Used in Project'. Declared in: java.security.MessageDigest Matching pattern in special code kind 'Cryptography: Cryptographic Algorithms Used in Project': static java.security.** java.security.**.getInstance(java.lang.String)		

Finding ID:	**5**	**Problem Type:**	Cryptography: Cryptographic Algorithms w/o Specified Crypto-Provider (Special Code)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	1.00	**Reviewed State:**	Not Reviewed
Location:	ServletConnectionPrincipal.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet):61		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Cryptography: Cryptographic Algorithms w/o Specified Crypto-Provider'. Declared in: java.security.MessageDigest Matching pattern in special code kind 'Cryptography: Cryptographic Algorithms w/o Specified Crypto-Provider': static java.security.** java.security.**.getInstance(java.lang.String)		

Findings List

Finding ID:	**14**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	AuthenticationCheckFilter.java (<Source Code>/org/apache/qpid/server/management/plugin/filter): 157		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.filter.AuthenticationCheckFilter$1 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedExceptionAction.run()		

Finding ID:	**6**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	LoginLogoutReporter.java (<Source Code>/org/apache/qpid/server/management/plugin/session):75		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.session.LoginLogoutReporter$1 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Finding ID:	**15**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	LoginLogoutReporter.java (<Source Code>/org/apache/qpid/server/management/plugin/session):90		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.session.LoginLogoutReporter$2 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Findings List

Finding ID:	**27**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):117		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$1 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Finding ID:	**22**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):154		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$2 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Finding ID:	**7**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):185		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$3 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Findings List

Finding ID:	**28**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):215		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$4 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Finding ID:	**20**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):242		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$5 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Finding ID:	**18**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):270		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$6 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Findings List

Finding ID:	**9**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):307		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$7 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Finding ID:	**21**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):336		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$8 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Finding ID:	**8**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):389		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$9 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Findings List

Finding ID:	**29**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):415		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$10 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Finding ID:	**26**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):449		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$11 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Finding ID:	**16**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):484		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$12 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Findings List

Finding ID:	**13**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):523		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$13 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Finding ID:	**30**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):556		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$14 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Finding ID:	**12**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):586		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$15 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Findings List

Finding ID:	**19**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):631		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$16 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Finding ID:	**23**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):688		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$17 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Finding ID:	**31**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):794		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$18 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Findings List

Finding ID:	**25**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):829		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$19 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Finding ID:	**24**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):875		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$20 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Finding ID:	**17**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):910		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$21 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Findings List

Finding ID:	**10**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):950		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$22 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Finding ID:	**32**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):985		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$23 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Finding ID:	**11**	**Problem Type:**	Usage: Privileged Action (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestUserPreferenceHandlerTest.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):1012		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Privileged Action'. Declared in: org.apache.qpid.server.management.plugin.servlet.rest.RestUserPreferenceHandlerTest$24 Matching pattern in special code kind 'Usage: Privileged Action': ** java.security.PrivilegedAction.run()		

Findings List

Finding ID:	**133**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):139		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of java/io/PrintWriter.println(Ljava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.rest.ApiDocsServlet.doGet(HttpServletRequest, HttpServletResponse, ConfiguredObject) - Sink method java/io/PrintWriter.println(Ljava/lang/String;)V - Sink parameter 0 - Unknown source javax/servlet/http/HttpServletRequest.getServletPath()Ljava/lang/String; - Unknown source java/lang/Class.getSimpleName()Ljava/lang/String;		

Finding ID:	**138**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):140		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of java/io/PrintWriter.println(Ljava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.rest.ApiDocsServlet.doGet(HttpServletRequest, HttpServletResponse, ConfiguredObject) - Sink method java/io/PrintWriter.println(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/model/ManagedObject.description()Ljava/lang/String;		

Finding ID:	**141**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):205		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of java/io/PrintWriter.println(Ljava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.rest.ApiDocsServlet.writeCategoryDescription(PrintWriter, Class) - Sink method java/io/PrintWriter.println(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/model/ManagedObject.description()Ljava/lang/String;		

Findings List

Finding ID:	**134**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):216		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of java/io/PrintWriter.print(Ljava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.rest.ApiDocsServlet.writeUsage(PrintWriter, HttpServletRequest, Class[], Class) - Sink method java/io/PrintWriter.print(Ljava/lang/String;)V - Sink parameter 0 - Unknown source javax/servlet/http/HttpServletRequest.getServletPath()Ljava/lang/String;		

Finding ID:	**135**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):229		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of java/io/PrintWriter.print(Ljava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.rest.ApiDocsServlet.writeUsage(PrintWriter, HttpServletRequest, Class[], Class) - Sink method java/io/PrintWriter.print(Ljava/lang/String;)V - Sink parameter 0 - Unknown source javax/servlet/http/HttpServletRequest.getServletPath()Ljava/lang/String;		

Finding ID:	**136**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):236		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of java/io/PrintWriter.print(Ljava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.rest.ApiDocsServlet.writeUsage(PrintWriter, HttpServletRequest, Class[], Class) - Sink method java/io/PrintWriter.print(Ljava/lang/String;)V - Sink parameter 0 - Unknown source javax/servlet/http/HttpServletRequest.getServletPath()Ljava/lang/String;		

Findings List

Finding ID:	**137**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):244		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of java/io/PrintWriter.print(Ljava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.rest.ApiDocsServlet.writeUsage(PrintWriter, HttpServletRequest, Class[], Class) - Sink method java/io/PrintWriter.print(Ljava/lang/String;)V - Sink parameter 0 - Unknown source javax/servlet/http/HttpServletRequest.getServletPath()Ljava/lang/String;		

Finding ID:	**149**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):273		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of java/io/PrintWriter.print(Ljava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.rest.ApiDocsServlet.writeTypes(PrintWriter, Model, List) - Sink method java/io/PrintWriter.print(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/management/plugin/servlet/rest/ApiDocsServlet.getTypeName(Ljava/lang/Class;Lorg/apache/qpid/server/model/Model;)Ljava/lang/String;		

Findings List

Finding ID:	**150**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):275		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of java/io/PrintWriter.print(Ljava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.rest.ApiDocsServlet.writeTypes(PrintWriter, Model, List) - Sink method java/io/PrintWriter.print(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/model/ManagedObject.description()Ljava/lang/String;		

Finding ID:	**139**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):308		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of java/io/PrintWriter.println(Ljava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.rest.ApiDocsServlet.writeAttributes(PrintWriter, Class, Model, List) - Sink method java/io/PrintWriter.println(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/management/plugin/servlet/rest/ApiDocsServlet.getTypeName(Ljava/lang/Class;Lorg/apache/qpid/server/model/Model;)Ljava/lang/String;		

Findings List

Finding ID:	**140**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):345		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of java/io/PrintWriter.println(Ljava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.rest.ApiDocsServlet.writeAttributesTable(PrintWriter, Collection) - Sink method java/io/PrintWriter.println(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/model/ConfiguredObjectAttribute.getDescription()Ljava/lang/String; - Unknown source org/apache/qpid/server/model/ConfiguredObjectAttribute.getName()Ljava/lang/String; - Unknown source org/apache/qpid/server/management/plugin/servlet/rest/ApiDocsServlet.renderType(Lorg/apache/qpid/server/model/ConfiguredObjectAttributeOrStatistic;)Ljava/lang/String;		

Finding ID:	**147**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):376		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of java/io/PrintWriter.println(Ljava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.rest.ApiDocsServlet.writeStatistics(PrintWriter, Class, Model, List) - Sink method java/io/PrintWriter.println(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/management/plugin/servlet/rest/ApiDocsServlet.getTypeName(Ljava/lang/Class;Lorg/apache/qpid/server/model/Model;)Ljava/lang/String;		

Findings List

Finding ID:	**148**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):393		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of java/io/PrintWriter.println(Ljava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.rest.ApiDocsServlet.writeStatisticsTable(PrintWriter, Collection) - Sink method java/io/PrintWriter.println(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/model/ConfiguredObjectStatistic.getDescription()Ljava/lang/String; - Unknown source org/apache/qpid/server/model/ConfiguredObjectStatistic.getUnits()Lorg/apache/qpid/server/model/StatisticUnit; - Unknown source org/apache/qpid/server/model/ConfiguredObjectStatistic.getStatisticType()Lorg/apache/qpid/server/model/StatisticType; - Unknown source org/apache/qpid/server/management/plugin/servlet/rest/ApiDocsServlet.renderType(Lorg/apache/qpid/server/model/ConfiguredObjectAttributeOrStatistic;)Ljava/lang/String; - Unknown source org/apache/qpid/server/model/ConfiguredObjectStatistic.getName()Ljava/lang/String;		

Finding ID:	**144**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):429		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of java/io/PrintWriter.println(Ljava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.rest.ApiDocsServlet.writeOperations(PrintWriter, Class, Model, List) - Sink method java/io/PrintWriter.println(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/management/plugin/servlet/rest/ApiDocsServlet.getTypeName(Ljava/lang/Class;Lorg/apache/qpid/server/model/Model;)Ljava/lang/String;		

Findings List

Finding ID:	**145**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):447		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of java/io/PrintWriter.println(Ljava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.rest.ApiDocsServlet.writeOperationsTables(PrintWriter, Collection) - Sink method java/io/PrintWriter.println(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/management/plugin/servlet/rest/ApiDocsServlet.renderType(Lorg/apache/qpid/server/model/ConfiguredObjectOperation;)Ljava/lang/String; - Unknown source org/apache/qpid/server/model/ConfiguredObjectOperation.getName()Ljava/lang/String; - Unknown source org/apache/qpid/server/model/ConfiguredObjectOperation.getDescription()Ljava/lang/String;		

Finding ID:	**146**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):456		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of java/io/PrintWriter.println(Ljava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.rest.ApiDocsServlet.writeOperationsTables(PrintWriter, Collection) - Sink method java/io/PrintWriter.println(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/management/plugin/servlet/rest/ApiDocsServlet.renderParameters(Ljava/util/List;)Ljava/lang/String;		

Findings List

Finding ID:	**142**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):613		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of java/io/PrintWriter.println(Ljava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.rest.ApiDocsServlet.writeContext(PrintWriter, Class, Model, List) - Sink method java/io/PrintWriter.println(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/management/plugin/servlet/rest/ApiDocsServlet.getTypeName(Ljava/lang/Class;Lorg/apache/qpid/server/model/Model;)Ljava/lang/String;		

Finding ID:	**143**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):632		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of java/io/PrintWriter.println(Ljava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.rest.ApiDocsServlet.writeContextDefaults(PrintWriter, Collection) - Sink method java/io/PrintWriter.println(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/model/ManagedContextDefault.description()Ljava/lang/String; - Unknown source org/apache/qpid/server/model/ManagedContextDefault.name()Ljava/lang/String;		

Findings List

Finding ID:	**129**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	DefinedFileServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet):94		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of javax/servlet/http/HttpServletResponse.sendError(ILjava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.DefinedFileServlet.doGet(HttpServletRequest, HttpServletResponse) - Sink method javax/servlet/http/HttpServletResponse.sendError(ILjava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/management/plugin/servlet/DefinedFileServlet._filename		

Finding ID:	**119**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):398		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of javax/servlet/http/HttpServletResponse.sendError(ILjava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.auth.OAuth2InteractiveAuthenticator$FailedAuthenticationHandler.handleAuthentication(HttpServletResponse) - Sink method javax/servlet/http/HttpServletResponse.sendError(ILjava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/management/plugin/auth/OAuth2InteractiveAuthenticator$FailedAuthenticationHandler._message - Unknown source org/apache/qpid/server/management/plugin/auth/OAuth2InteractiveAuthenticator$FailedAuthenticationHandler._throwable		

Findings List

Finding ID:	**120**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):402		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of javax/servlet/http/HttpServletResponse.sendError(ILjava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.auth.OAuth2InteractiveAuthenticator$FailedAuthenticationHandler.handleAuthentication(HttpServletResponse) - Sink method javax/servlet/http/HttpServletResponse.sendError(ILjava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/management/plugin/auth/OAuth2InteractiveAuthenticator$FailedAuthenticationHandler._message		

Finding ID:	**123**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	OAuth2InteractiveAuthenticatorTest.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):287		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of javax/servlet/http/HttpServletResponse.sendError(ILjava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.auth.OAuth2InteractiveAuthenticatorTest.testUnauthorizedAuthorizationCode() - Sink method javax/servlet/http/HttpServletResponse.sendError(ILjava/lang/String;)V - Sink parameter 0 - Unknown source org/mockito/ArgumentMatchers.any(Ljava/lang/Class;)Ljava/lang/Object;		

Findings List

Finding ID:	**151**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	QueueReportServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest): 79		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of java/io/PrintWriter.write(Ljava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.rest.QueueReportServlet.doGet(HttpServletRequest, HttpServletResponse, ConfiguredObject) - Sink method java/io/PrintWriter.write(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/management/plugin/report/ReportRunner.runReport(Lorg/apache/qpid/server/model/Queue;)Ljava/lang/Object;		

Finding ID:	**130**	**Problem Type:**	FindSecBugs: Potential XSS in Servlet (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	RootServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet):76		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: This use of javax/servlet/http/HttpServletResponse.sendError(ILjava/lang/String;)V could be vulnerable to XSS - In method org.apache.qpid.server.management.plugin.servlet.RootServlet.doGet(HttpServletRequest, HttpServletResponse) - Sink method javax/servlet/http/HttpServletResponse.sendError(ILjava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/management/plugin/servlet/RootServlet._filename		

Finding ID:	**97**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):138 <- AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):101		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.println(java.lang.String)		

Findings List

Finding ID:	**98**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):139 <- AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):101		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.println(java.lang.String)		

Finding ID:	**104**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):140 <- AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):101		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.println(java.lang.String)		

Finding ID:	**96**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):196 <- AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):101		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.print(java.lang.String)		

Findings List

Finding ID:	**102**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):204 <- AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):101		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.println(java.lang.String)		

Finding ID:	**101**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):205 <- AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):101		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.println(java.lang.String)		

Finding ID:	**105**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):221 <- AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):101		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.print(java.lang.String)		

Findings List

Finding ID:	**100**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):233 <- AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):101		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.print(java.lang.String)		

Finding ID:	**94**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):241 <- AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):101		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.print(java.lang.String)		

Finding ID:	**99**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):248 <- AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):101		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.print(java.lang.String)		

Findings List

Finding ID:	**95**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):273 <- AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):101		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.print(java.lang.String)		

Finding ID:	**92**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):275 <- AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):101		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.print(java.lang.String)		

Finding ID:	**103**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):308 <- AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):101		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.println(java.lang.String)		

Findings List

Finding ID:	**93**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):345 <- AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):101		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.println(java.lang.String)		

Finding ID:	**87**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	DefinedFileServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet):109 <- DefinedFileServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet):107		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getScheme() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.OutputStream.write(byte[])		

Finding ID:	**88**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	DefinedFileServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet):109 <- DefinedFileServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet):108		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.OutputStream.write(byte[])		

Findings List

Finding ID:	**90**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RootServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet):92 <- RootServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet):90		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getScheme() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.OutputStream.write(byte[])		

Finding ID:	**91**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RootServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet):92 <- RootServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet):91		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.OutputStream.write(byte[])		

Finding ID:	**111**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	4.00	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):345 <- OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):331		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.StringBuffer javax.servlet.ServletRequest.getRequestURL() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.println(java.lang.String)		

Findings List

Finding ID:	**106**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	3.50	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):139 <- ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):82		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServletPath() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.println(java.lang.String)		

Finding ID:	**107**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	3.50	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):216 <- ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):216		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServletPath() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.print(java.lang.String)		

Finding ID:	**108**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	3.50	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):229 <- ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):230		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServletPath() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.print(java.lang.String)		

Findings List

Finding ID:	**109**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	3.50	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):236 <- ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):238		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServletPath() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.print(java.lang.String)		

Finding ID:	**110**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	3.50	**Reviewed State:**	Not Reviewed
Location:	ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):244 <- ApiDocsServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):245		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServletPath() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.PrintWriter.print(java.lang.String)		

Finding ID:	**86**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	3.50	**Reviewed State:**	Not Reviewed
Location:	DefinedFileServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet):109 <- DefinedFileServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet):105		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServletPath() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.OutputStream.write(byte[])		

Findings List

Finding ID:	**89**	**Problem Type:**	XSS: Reflected XSS (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	3.50	**Reviewed State:**	Not Reviewed
Location:	RootServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet):92 <- RootServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet):88		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: Reflected XSS' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServletPath() Matching pattern in taint sink kind 'XSS - Generic Output Used for Response': void java.io.OutputStream.write(byte[])		

Finding ID:	**152**	**Problem Type:**	FindSecBugs: Predictable pseudorandom number generator (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	SaslServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):116		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: The use of java.util.Random is predictable - In method org.apache.qpid.server.management.plugin.servlet.rest.SaslServlet.getRandom(HttpServletRequest) - Value java.util.Random		

Findings List

Finding ID:	**114**	**Problem Type:**	FindSecBugs: Unvalidated Redirect (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	AnonymousInteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):80		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: The following redirection could be used by an attacker to redirect users to a phishing website. - In method org.apache.qpid.server.management.plugin.auth.AnonymousInteractiveAuthenticator.lambda$getAuthenticationHandler$1(HttpManagementConfiguration, HttpServletRequest, Port, HttpServletResponse) - Sink method javax/servlet/http/HttpServletResponse.sendRedirect(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/management/plugin/auth/AnonymousInteractiveAuthenticator.getOriginalRequestUri(Ljavax/servlet/http/HttpServletRequest;)Ljava/lang/String; - Unknown source java/lang/StringBuffer.append(Ljava/lang/String;)Ljava/lang/StringBuffer; - Unknown source javax/servlet/http/HttpServletRequest.getRequestURL()Ljava/lang/StringBuffer; - Unknown source java/lang/StringBuffer.toString()Ljava/lang/String; - Unknown source javax/servlet/http/HttpServletRequest.getQueryString()Ljava/lang/String;		

Finding ID:	**116**	**Problem Type:**	FindSecBugs: Unvalidated Redirect (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):137		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: The following redirection could be used by an attacker to redirect users to a phishing website. - In method org.apache.qpid.server.management.plugin.auth.OAuth2InteractiveAuthenticator.lambda$getAuthenticationHandler$0(HttpManagementConfiguration, HttpServletRequest, OAuth2AuthenticationProvider, String, HttpServletResponse) - Sink method javax/servlet/http/HttpServletResponse.sendRedirect(Ljava/lang/String;)V - Sink parameter 0 - Method usage not detected		

Findings List

Finding ID:	**117**	**Problem Type:**	FindSecBugs: Unvalidated Redirect (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):178		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: The following redirection could be used by an attacker to redirect users to a phishing website. - In method org.apache.qpid.server.management.plugin.auth.OAuth2InteractiveAuthenticator$1.handleAuthentication(HttpServletResponse) - Sink method javax/servlet/http/HttpServletResponse.sendRedirect(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/management/plugin/auth/OAuth2InteractiveAuthenticator$1.val$originalRequestUri		

Finding ID:	**118**	**Problem Type:**	FindSecBugs: Unvalidated Redirect (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):241		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: The following redirection could be used by an attacker to redirect users to a phishing website. - In method org.apache.qpid.server.management.plugin.auth.OAuth2InteractiveAuthenticator$2.handleLogout(HttpServletResponse) - Sink method javax/servlet/http/HttpServletResponse.sendRedirect(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/management/plugin/auth/OAuth2InteractiveAuthenticator$2.val$postLogoutRedirect		

Findings List

Finding ID:	**121**	**Problem Type:**	FindSecBugs: Unvalidated Redirect (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	OAuth2InteractiveAuthenticatorTest.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):133		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: The following redirection could be used by an attacker to redirect users to a phishing website. - In method org.apache.qpid.server.management.plugin.auth.OAuth2InteractiveAuthenticatorTest.testInitialRedirect() - Sink method javax/servlet/http/HttpServletResponse.sendRedirect(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/mockito/ArgumentCaptor.capture()Ljava/lang/Object;		

Finding ID:	**122**	**Problem Type:**	FindSecBugs: Unvalidated Redirect (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	OAuth2InteractiveAuthenticatorTest.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):169		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: The following redirection could be used by an attacker to redirect users to a phishing website. - In method org.apache.qpid.server.management.plugin.auth.OAuth2InteractiveAuthenticatorTest.testValidLogin() - Sink method javax/servlet/http/HttpServletResponse.sendRedirect(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/mockito/ArgumentCaptor.capture()Ljava/lang/Object;		

Finding ID:	**127**	**Problem Type:**	FindSecBugs: Unvalidated Redirect (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	RedirectFilter.java (<Source Code>/org/apache/qpid/server/management/plugin/filter):50		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: The following redirection could be used by an attacker to redirect users to a phishing website. - In method org.apache.qpid.server.management.plugin.filter.RedirectFilter.doFilter(ServletRequest, ServletResponse, FilterChain) - Sink method javax/servlet/http/HttpServletResponse.sendRedirect(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/management/plugin/filter/RedirectFilter._redirectURI		

Findings List

Finding ID:	**113**	**Problem Type:**	FindSecBugs: Unvalidated Redirect (SpotBugs Security Issues)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	RewriteServlet.java (<Source Code>/org/apache/qpid/server/management/plugin):53		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: The following redirection could be used by an attacker to redirect users to a phishing website. - In method org.apache.qpid.server.management.plugin.RewriteServlet.service(HttpServletRequest, HttpServletResponse) - Sink method javax/servlet/http/HttpServletResponse.sendRedirect(Ljava/lang/String;)V - Sink parameter 0 - Unknown source org/apache/qpid/server/management/plugin/RewriteServlet._replacement - Unknown source javax/servlet/http/HttpServletRequest.getRequestURI()Ljava/lang/String; - Unknown source javax/servlet/http/HttpServletRequest.getQueryString()Ljava/lang/String;		

Finding ID:	**40**	**Problem Type:**	Injection: Reflection Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	ReportRunner.java (<Source Code>/org/apache/qpid/server/management/plugin/report):109 <- QueueReportServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest): 70		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Reflection Injection' Matching pattern in taint source kind 'Servlet Request Input': java.util.Map javax.servlet.ServletRequest.getParameterMap() Matching pattern in taint sink kind 'Reflection Injection': java.lang.reflect.Method java.lang.Class.getMethod(java.lang.String, java.lang.Class[])		

Finding ID:	**39**	**Problem Type:**	Injection: Reflection Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	ReportRunner.java (<Source Code>/org/apache/qpid/server/management/plugin/report):121 <- QueueReportServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest): 70		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Reflection Injection' Matching pattern in taint source kind 'Servlet Request Input': java.util.Map javax.servlet.ServletRequest.getParameterMap() Matching pattern in taint sink kind 'Reflection Injection': java.lang.reflect.Method java.lang.Class.getMethod(java.lang.String, java.lang.Class[])		

Findings List

Finding ID:	**42**	**Problem Type:**	Injection: Reflection Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	4.00	**Reviewed State:**	Not Reviewed
Location:	ReportRunner.java (<Source Code>/org/apache/qpid/server/management/plugin/report):109 <- OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):331		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Reflection Injection' Matching pattern in taint source kind 'Servlet Request Input': java.lang.StringBuffer javax.servlet.ServletRequest.getRequestURL() Matching pattern in taint sink kind 'Reflection Injection': java.lang.reflect.Method java.lang.Class.getMethod(java.lang.String, java.lang.Class[])		

Finding ID:	**41**	**Problem Type:**	Injection: Reflection Injection (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	4.00	**Reviewed State:**	Not Reviewed
Location:	ReportRunner.java (<Source Code>/org/apache/qpid/server/management/plugin/report):121 <- OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):331		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Injection: Reflection Injection' Matching pattern in taint source kind 'Servlet Request Input': java.lang.StringBuffer javax.servlet.ServletRequest.getRequestURL() Matching pattern in taint sink kind 'Reflection Injection': java.lang.reflect.Method java.lang.Class.getMethod(java.lang.String, java.lang.Class[])		

Finding ID:	**59**	**Problem Type:**	Resource Leak: IO Stream Resource Leak (Resource Leaks)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):440		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified Resource Leak: IO Stream Resource Leak Matching pattern in open resource kind 'IO Stream Opened': java.io.InputStream javax.servlet.http.Part.getInputStream()		

Findings List

Finding ID:	**60**	**Problem Type:**	Resource Leak: IO Stream Resource Leak (Resource Leaks)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):440		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified Resource Leak: IO Stream Resource Leak Matching pattern in open resource kind 'IO Stream Opened': java.io.InputStream javax.servlet.http.Part.getInputStream()		

Finding ID:	**61**	**Problem Type:**	Resource Leak: IO Stream Resource Leak (Resource Leaks)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	RestServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):440		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified Resource Leak: IO Stream Resource Leak Matching pattern in open resource kind 'IO Stream Opened': java.io.InputStream javax.servlet.http.Part.getInputStream()		

Finding ID:	**131**	**Problem Type:**	SpotBugs: Field should be moved out of an interface and made package protected (SpotBugs Malicious Code Vulnerabilities)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	ConfiguredObjectFilterParserConstants.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/query):89		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: org.apache.qpid.server.management.plugin.servlet.query.ConfiguredObjectFilterParserConstants.tokenImage should be moved out of an interface and made package protected - Field org.apache.qpid.server.management.plugin.servlet.query.ConfiguredObjectFilterParserConstants.tokenImage		

Findings List

Finding ID:	**132**	**Problem Type:**	SpotBugs: Field should be package protected (SpotBugs Malicious Code Vulnerabilities)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	ConfiguredObjectFilterParserTokenManager.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/query):930		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: org.apache.qpid.server.management.plugin.servlet.query.ConfiguredObjectFilterParserTokenManager.jjstrLiteralImages should be package protected - Field org.apache.qpid.server.management.plugin.servlet.query.ConfiguredObjectFilterParserTokenManager.jjstrLiteralImages		

Finding ID:	**124**	**Problem Type:**	SpotBugs: Load of known null value (SpotBugs Dodgy Code)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	AbstractLegacyConfiguredObjectController.java (<Source Code>/org/apache/qpid/server/management/plugin/controller):270		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: Load of known null value in org.apache.qpid.server.management.plugin.controller.AbstractLegacyConfiguredObjectController.getRequestType(ManagementRequest) - In method org.apache.qpid.server.management.plugin.controller.AbstractLegacyConfiguredObjectController.getRequestType(ManagementRequest) - Value loaded from category		

Finding ID:	**115**	**Problem Type:**	SpotBugs: Load of known null value (SpotBugs Dodgy Code)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):147		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: Load of known null value in org.apache.qpid.server.management.plugin.auth.OAuth2InteractiveAuthenticator.getAuthenticationHandler(HttpServletRequest, HttpManagementConfiguration) - In method org.apache.qpid.server.management.plugin.auth.OAuth2InteractiveAuthenticator.getAuthenticationHandler(HttpServletRequest, HttpManagementConfiguration) - Value loaded from state		

Findings List

Finding ID:	**128**	**Problem Type:**	SpotBugs: May expose internal representation by incorporating reference to mutable object (SpotBugs Malicious Code Vulnerabilities)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	TestTextReport.java (<Source Code>/org/apache/qpid/server/management/plugin/report):80		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: org.apache.qpid.server.management.plugin.report.TestTextReport.setStringArrayParam(String[]) may expose internal representation by storing an externally mutable object into TestTextReport._stringArrayParam - In method org.apache.qpid.server.management.plugin.report.TestTextReport.setStringArrayParam(String[]) - Field org.apache.qpid.server.management.plugin.report.TestTextReport._stringArrayParam - Local variable named value		

Finding ID:	**126**	**Problem Type:**	SpotBugs: May expose internal representation by returning reference to mutable object (SpotBugs Malicious Code Vulnerabilities)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	8.00	**Reviewed State:**	Not Reviewed
Location:	LegacyCategoryController.java (<Source Code>/org/apache/qpid/server/management/plugin/controller/v6_1/category):54		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: org.apache.qpid.server.management.plugin.controller.v6_1.category.LegacyCategoryController.getParentCategories() may expose internal representation by returning LegacyCategoryController._parentCategories - In method org.apache.qpid.server.management.plugin.controller.v6_1.category.LegacyCategoryController.getParentCategories() - Field org.apache.qpid.server.management.plugin.controller.v6_1.category.LegacyCategoryController._parentCategories		

Findings List

Finding ID:	**125**	**Problem Type:**	SpotBugs: Method call passes null for non-null parameter (SpotBugs Correctness)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	6.00	**Reviewed State:**	Not Reviewed
Location:	AbstractLegacyConfiguredObjectController.java (<Source Code>/org/apache/qpid/server/management/plugin/controller):271		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	A finding identified by the external 'SpotBugs' plugin: Null passed for non-null parameter of getCategoryMapping(String) in org.apache.qpid.server.management.plugin.controller.AbstractLegacyConfiguredObjectController.getRequestType(ManagementRequest) - In method org.apache.qpid.server.management.plugin.controller.AbstractLegacyConfiguredObjectController.getRequestType(ManagementRequest) - Called method org.apache.qpid.server.management.plugin.controller.AbstractLegacyConfiguredObjectController.getCategoryMapping(String) - Value loaded from category - Argument 1 is definitely null but must not be null - Definite null passed to dangerous method call target org.apache.qpid.server.management.plugin.controller.AbstractLegacyConfiguredObjectController.getCategoryMapping(String)		

Finding ID:	**73**	**Problem Type:**	Trust Boundary Violation: HTTP Session (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	HttpManagementUtil.java (<Source Code>/org/apache/qpid/server/management/plugin):342 <- AnonymousInteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):66		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Trust Boundary Violation: HTTP Session' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'HTTP Session': void javax.servlet.http.HttpSession.setAttribute(java.lang.String, java.lang.Object)		

Findings List

Finding ID:	**66**	**Problem Type:**	Trust Boundary Violation: HTTP Session (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	HttpManagementUtil.java (<Source Code>/org/apache/qpid/server/management/plugin):342 <- OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):163		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Trust Boundary Violation: HTTP Session' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'HTTP Session': void javax.servlet.http.HttpSession.setAttribute(java.lang.String, java.lang.Object)		

Finding ID:	**67**	**Problem Type:**	Trust Boundary Violation: HTTP Session (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	HttpManagementUtil.java (<Source Code>/org/apache/qpid/server/management/plugin):342 <- OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):197		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Trust Boundary Violation: HTTP Session' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'HTTP Session': void javax.servlet.http.HttpSession.setAttribute(java.lang.String, java.lang.Object)		

Finding ID:	**65**	**Problem Type:**	Trust Boundary Violation: HTTP Session (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	HttpManagementUtil.java (<Source Code>/org/apache/qpid/server/management/plugin):342 <- SSLClientCertPreemptiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):55		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Trust Boundary Violation: HTTP Session' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'HTTP Session': void javax.servlet.http.HttpSession.setAttribute(java.lang.String, java.lang.Object)		

Findings List

Finding ID:	**62**	**Problem Type:**	Trust Boundary Violation: HTTP Session (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	HttpManagementUtil.java (<Source Code>/org/apache/qpid/server/management/plugin):342 <- SaslServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):134		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Trust Boundary Violation: HTTP Session' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getParameter(java.lang.String) Matching pattern in taint sink kind 'HTTP Session': void javax.servlet.http.HttpSession.setAttribute(java.lang.String, java.lang.Object)		

Finding ID:	**63**	**Problem Type:**	Trust Boundary Violation: HTTP Session (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	HttpManagementUtil.java (<Source Code>/org/apache/qpid/server/management/plugin):342 <- SaslServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):136		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Trust Boundary Violation: HTTP Session' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getParameter(java.lang.String) Matching pattern in taint sink kind 'HTTP Session': void javax.servlet.http.HttpSession.setAttribute(java.lang.String, java.lang.Object)		

Finding ID:	**64**	**Problem Type:**	Trust Boundary Violation: HTTP Session (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	HttpManagementUtil.java (<Source Code>/org/apache/qpid/server/management/plugin):342 <- SaslServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):298		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Trust Boundary Violation: HTTP Session' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'HTTP Session': void javax.servlet.http.HttpSession.setAttribute(java.lang.String, java.lang.Object)		

Findings List

Finding ID:	**71**	**Problem Type:**	Trust Boundary Violation: HTTP Session (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	HttpManagementUtil.java (<Source Code>/org/apache/qpid/server/management/plugin):342 <- SpnegoInteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):57		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Trust Boundary Violation: HTTP Session' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getHeader(java.lang.String) Matching pattern in taint sink kind 'HTTP Session': void javax.servlet.http.HttpSession.setAttribute(java.lang.String, java.lang.Object)		

Finding ID:	**72**	**Problem Type:**	Trust Boundary Violation: HTTP Session (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	HttpManagementUtil.java (<Source Code>/org/apache/qpid/server/management/plugin):342 <- SpnegoInteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):75		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Trust Boundary Violation: HTTP Session' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'HTTP Session': void javax.servlet.http.HttpSession.setAttribute(java.lang.String, java.lang.Object)		

Finding ID:	**70**	**Problem Type:**	Trust Boundary Violation: HTTP Session (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):264 <- OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):296		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Trust Boundary Violation: HTTP Session' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getQueryString() Matching pattern in taint sink kind 'HTTP Session': void javax.servlet.http.HttpSession.setAttribute(java.lang.String, java.lang.Object)		

Findings List

Finding ID:	**68**	**Problem Type:**	Trust Boundary Violation: HTTP Session (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	4.00	**Reviewed State:**	Not Reviewed
Location:	OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):262 <- OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):331		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Trust Boundary Violation: HTTP Session' Matching pattern in taint source kind 'Servlet Request Input': java.lang.StringBuffer javax.servlet.ServletRequest.getRequestURL() Matching pattern in taint sink kind 'HTTP Session': void javax.servlet.http.HttpSession.setAttribute(java.lang.String, java.lang.Object)		

Finding ID:	**69**	**Problem Type:**	Trust Boundary Violation: HTTP Session (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	4.00	**Reviewed State:**	Not Reviewed
Location:	OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):264 <- OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):295		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'Trust Boundary Violation: HTTP Session' Matching pattern in taint source kind 'Servlet Request Input': java.lang.StringBuffer javax.servlet.ServletRequest.getRequestURL() Matching pattern in taint sink kind 'HTTP Session': void javax.servlet.http.HttpSession.setAttribute(java.lang.String, java.lang.Object)		

Finding ID:	**4**	**Problem Type:**	Usage: Java Reflection (Special Code)
Classification:	Information	**Date:**	2020-06-14 05:47:50 - new
Rating:	0.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):349		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Java Reflection'. Declared in: java.lang.reflect.Method Matching pattern in special code kind 'Usage: Java Reflection': java.lang.Object java.lang.reflect.Method.invoke(java.lang.Object, java.lang.Object[])		

Findings List

Finding ID:	**2**	**Problem Type:**	Usage: Java Reflection (Special Code)
Classification:	Information	**Date:**	2020-06-14 05:47:50 - new
Rating:	0.00	**Reviewed State:**	Not Reviewed
Location:	ReportRunner.java (<Source Code>/org/apache/qpid/server/management/plugin/report):110		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Java Reflection'. Declared in: java.lang.reflect.Method Matching pattern in special code kind 'Usage: Java Reflection': java.lang.Object java.lang.reflect.Method.invoke(java.lang.Object, java.lang.Object[])		

Finding ID:	**3**	**Problem Type:**	Usage: Java Reflection (Special Code)
Classification:	Information	**Date:**	2020-06-14 05:47:50 - new
Rating:	0.00	**Reviewed State:**	Not Reviewed
Location:	ReportRunner.java (<Source Code>/org/apache/qpid/server/management/plugin/report):122		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Java Reflection'. Declared in: java.lang.reflect.Method Matching pattern in special code kind 'Usage: Java Reflection': java.lang.Object java.lang.reflect.Method.invoke(java.lang.Object, java.lang.Object[])		

Finding ID:	**1**	**Problem Type:**	Usage: Java Reflection (Special Code)
Classification:	Information	**Date:**	2020-06-14 05:47:50 - new
Rating:	0.00	**Reviewed State:**	Not Reviewed
Location:	ReportRunner.java (<Source Code>/org/apache/qpid/server/management/plugin/report):176		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Java Reflection'. Declared in: java.lang.Class Matching pattern in special code kind 'Usage: Java Reflection': java.lang.Object java.lang.Class.newInstance()		

Findings List

Finding ID:	**35**	**Problem Type:**	Usage: Java Servlet Forward and Include (Special Code)
Classification:	Information	**Date:**	2020-06-14 05:47:50 - new
Rating:	0.00	**Reviewed State:**	Not Reviewed
Location:	SpnegoInteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):82		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Java Servlet Forward and Include'. Declared in: javax.servlet.RequestDispatcher Matching pattern in special code kind 'Usage: Java Servlet Forward and Include': void javax.servlet.RequestDispatcher.forward(javax.servlet.ServletRequest, javax.servlet.ServletResponse)		

Finding ID:	**34**	**Problem Type:**	Usage: Java Servlet Forward and Include (Special Code)
Classification:	Information	**Date:**	2020-06-14 05:47:50 - new
Rating:	0.00	**Reviewed State:**	Not Reviewed
Location:	UsernamePasswordInteractiveLogin.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):55		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: Java Servlet Forward and Include'. Declared in: javax.servlet.RequestDispatcher Matching pattern in special code kind 'Usage: Java Servlet Forward and Include': void javax.servlet.RequestDispatcher.forward(javax.servlet.ServletRequest, javax.servlet.ServletResponse)		

Finding ID:	**33**	**Problem Type:**	Usage: java.util.Random (Special Code)
Classification:	Manual Review Required	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.00	**Reviewed State:**	Not Reviewed
Location:	SaslServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):116		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified location for problem type 'Usage: java.util.Random'. Declared in: java.util.Random Matching pattern in special code kind 'Usage: java.util.Random': java.util.Random(long)		

Findings List

Finding ID:	**85**	**Problem Type:**	XSS: URL Redirection Abuse (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	6.50	**Reviewed State:**	Not Reviewed
Location:	AnonymousInteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):80 <- AnonymousInteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):126		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: URL Redirection Abuse' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getQueryString() Matching pattern in taint sink kind 'URL Redirection': void javax.servlet.http.HttpServletResponse.sendRedirect(java.lang.String)		

Finding ID:	**81**	**Problem Type:**	XSS: URL Redirection Abuse (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	6.50	**Reviewed State:**	Not Reviewed
Location:	OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):137 <- OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):255		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: URL Redirection Abuse' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'URL Redirection': void javax.servlet.http.HttpServletResponse.sendRedirect(java.lang.String)		

Finding ID:	**75**	**Problem Type:**	XSS: URL Redirection Abuse (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	6.50	**Reviewed State:**	Not Reviewed
Location:	RewriteServlet.java (<Source Code>/org/apache/qpid/server/management/plugin):53 <- RewriteServlet.java (<Source Code>/org/apache/qpid/server/management/plugin):51		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: URL Redirection Abuse' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getQueryString() Matching pattern in taint sink kind 'URL Redirection': void javax.servlet.http.HttpServletResponse.sendRedirect(java.lang.String)		

Findings List

Finding ID:	**84**	**Problem Type:**	XSS: URL Redirection Abuse (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.50	**Reviewed State:**	Not Reviewed
Location:	AnonymousInteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):80 <- AnonymousInteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):125		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: URL Redirection Abuse' Matching pattern in taint source kind 'Servlet Request Input': java.lang.StringBuffer javax.servlet.ServletRequest.getRequestURL() Matching pattern in taint sink kind 'URL Redirection': void javax.servlet.http.HttpServletResponse.sendRedirect(java.lang.String)		

Finding ID:	**74**	**Problem Type:**	XSS: URL Redirection Abuse (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	5.50	**Reviewed State:**	Not Reviewed
Location:	RewriteServlet.java (<Source Code>/org/apache/qpid/server/management/plugin):53 <- RewriteServlet.java (<Source Code>/org/apache/qpid/server/management/plugin):48		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: URL Redirection Abuse' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getRequestURI() Matching pattern in taint sink kind 'URL Redirection': void javax.servlet.http.HttpServletResponse.sendRedirect(java.lang.String)		

Finding ID:	**79**	**Problem Type:**	XSS: URL Redirection Abuse (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	3.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):370 <- AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):101		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: URL Redirection Abuse' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'URL Redirection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Findings List

Finding ID:	**77**	**Problem Type:**	XSS: URL Redirection Abuse (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	3.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):370 <- SaslServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):134		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: URL Redirection Abuse' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getParameter(java.lang.String) Matching pattern in taint sink kind 'URL Redirection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Finding ID:	**78**	**Problem Type:**	XSS: URL Redirection Abuse (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	3.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):370 <- SaslServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):136		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: URL Redirection Abuse' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getParameter(java.lang.String) Matching pattern in taint sink kind 'URL Redirection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Finding ID:	**80**	**Problem Type:**	XSS: URL Redirection Abuse (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	3.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):370 <- SaslServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):298		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: URL Redirection Abuse' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getServerName() Matching pattern in taint sink kind 'URL Redirection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Findings List

Finding ID:	**76**	**Problem Type:**	XSS: URL Redirection Abuse (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	3.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):370 <- SaslServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):98		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: URL Redirection Abuse' Matching pattern in taint source kind 'Servlet Request Input': java.lang.String javax.servlet.ServletRequest.getRemoteUser() Matching pattern in taint sink kind 'URL Redirection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Finding ID:	**82**	**Problem Type:**	XSS: URL Redirection Abuse (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	2.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):294 <- OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):331		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: URL Redirection Abuse' Matching pattern in taint source kind 'Servlet Request Input': java.lang.StringBuffer javax.servlet.ServletRequest.getRequestURL() Matching pattern in taint sink kind 'URL Redirection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		

Finding ID:	**83**	**Problem Type:**	XSS: URL Redirection Abuse (Taint Paths)
Classification:	Warning	**Date:**	2020-06-14 05:47:50 - new
Rating:	2.00	**Reviewed State:**	Not Reviewed
Location:	AbstractServlet.java (<Source Code>/org/apache/qpid/server/management/plugin/servlet/rest):370 <- OAuth2InteractiveAuthenticator.java (<Source Code>/org/apache/qpid/server/management/plugin/auth):331		
Tags:	no tags assigned		
Comment:	*no comment*		
Description:	An identified taint path for the problem type 'XSS: URL Redirection Abuse' Matching pattern in taint source kind 'Servlet Request Input': java.lang.StringBuffer javax.servlet.ServletRequest.getRequestURL() Matching pattern in taint sink kind 'URL Redirection': void javax.servlet.http.HttpServletResponse.setHeader(java.lang.String, java.lang.String)		