Web Application Report

This report includes important security information about your web application.

OWASP Top 10 2013 Report

This report was created by IBM Security AppScan Standard 9.0.3.6, Rules: 10344
Scan started: 11/6/2017 10:42:40 AM

Regulations

OWASP Top Ten 2013 – The Ten Most Critical Web Application Security Risks

Summary Description

The goal of the Top 10 project is to raise awareness about application security by identifying some of the most critical risks facing organizations. Development projects should address these potential risks in their requirements documents and design, build and test their applications to ensure that they have taken the necessary measures to reduce these risks to the minimum. Project managers should include time and budget for application security activities including developer training, application security policy development, security mechanism design and development, penetration testing, and security code review as part over the overall effort to address the risks.

The primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most important web application security risks. The Top 10 provides basic guidance on how to address against these risks and where to go to learn more on how to address them.

Although setout as an education piece, rather than a standard or a regulation, it is important to note that several prominent industry and government regulators are referencing the OWASP top ten. These bodies include among others VISA USA, MasterCard International and the American Federal Trade Commission (FTC).

However, according to the OWASP team the OWASP top ten first and foremost an education piece, not a standard. The OWASP team suggests that any organization about to adopt the Top Ten paper as a policy or standard to consult with the OWASP team first.

The OWASP Top 10 for 2013 broadens one of the categories from the 2010 version to be more inclusive of common, important vulnerabilities, and reorders some of the others based on changing prevalence data. It also brings component security into the spotlight by creating a specific category for this risk, pulling it out of the obscurity of the fine print of the 2010 risk A6: Security Misconfiguration.

This version of OWASP Top 10 is based on 8 datasets from 7 firms that specialize in application security, including 4 consulting companies and 3 tool/SaaS vendors (1 static, 1 dynamic, and 1 with both). This data spans over 500,000 vulnerabilities across hundreds of organizations and thousands of applications. The Top 10 items are selected and prioritized according to this prevalence data, in combination with consensus estimates of exploitability, detectability, and impact estimates.

Covered Entities

All companies and other entities that develop any kind of web application code are encouraged to address the top ten

list as part of their over all security risk management. Adopting the OWASP Top Ten is an effective first step towards changing the software development culture within the organization into one that produces secure code.

For more information on OWASP Top Ten, please review the –OWASP Top Ten 2013 – The Ten Most Critical Web Application Security Risks, at http://www.owasp.org

For more information on securing web applications, please visit http://www-03.ibm.com/software/products/en/category/application-security

The information provided does not constitute legal advice. The results of a vulnerability assessment will demonstrate potential vulnerabilities in your application that should be corrected in order to reduce the likelihood that your information will be compromised. As legal advice must be tailored to the specific application of each law, and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent counsel. IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.

Violated Section

Issues detected across 9/10 sections of the regulation:

Sections	Number of Issues
A1 - Injection	16
A2 - Broken authentication and session management	16
A3 - Cross site scripting (XSS)	11
A4 - Insecure direct object reference	14
A5 - Security Misconfiguration	44
A6 - Sensitive Data Exposure	123
A7 - Missing Function Level Access Control	69
A8 - Cross site request forgery (CSRF)	16
A9 - Using Known Vulnerable Components	99
A10 - UnvalidatedRedirects and Forwards	0

Section Violation By Issue

215 Unique issues detected across 9/10 sections of the regulation:

URL	Entity	Issue Type	Sections
https://wso2.sbi.123pay.vn/	wso2.sbi.123pay.vn	SSL Certificate Domain Name Mismatch	A6, A7
https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/i18n/i18next-1.5.9.js	i18next-1.5.9.js	Missing "Content-Security-Policy" header	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/enjoyhint-3.1.0/js/cloud-enjoyhint-script-data.js	cloud-enjoyhint-script-data.js	Missing "Content-Security-Policy" header	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/the	handlebars.min.js	Missing "Content-	A5, A6,

mes/wso2/libs/handlebars.min.js		Security-Policy" header	A7, A9
https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/jquery-validation/jquery.validate.min.js	jquery.validate.min.js	Missing "Content-Security-Policy" header	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/select2_4.0.0/js/select2.full.min.js	select2.full.min.js	Missing "Content-Security-Policy" header	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/carbon/admin/index.jsp	index.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/		Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/publisher/site/pages/index.jag	index.jag	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/publisher/		Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/publisher/apis	apis	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/publisher/site/pages/login.jag	login.jag	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/templates/listing/js/samples.js	samples.js	Email Address Pattern Found	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/pages/all-statistics.jag	all-statistics.jag	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-add/ajax/add.jag	add.jag	Body Parameters Accepted in Query	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/templates/item-info/js/lodash.min.js	lodash.min.js	Web Application Source Code Disclosure Pattern Found	A4, A5, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	life-cycles.jag	Database Error Pattern Found	A1, A7
https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/jsonpath-0.15.0.js	jsonpath-0.15.0.js	Web Application Source Code Disclosure Pattern Found	A4, A5, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	life-cycles.jag	SQL Injection	A1, A7
https://wso2.sbi.123pay.vn/publisher/design	design	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/dagre-d3.min.js	dagre-d3.min.js	Web Application Source Code Disclosure Pattern Found	A4, A5, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/ajax/stats.jag	stats.jag	Body Parameters Accepted in Query	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/design	design	Email Address Pattern Found	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/1882cde30750506693b8.worker.js	1882cde30750506693b8.worker.js	Credit Card Number Pattern Found	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-subscriptions/ajax/stats.jag	stats.jag	Body Parameters Accepted in Query	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-last-access-times/ajax/stats.jag	stats.jag	Body Parameters Accepted in Query	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/the	jshint.js	Possible Server Path	A4, A5,

mes/wso2/libs/codemirror/addon/jshint.js		Disclosure Pattern Found	A7, A9
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	add.jag	Email Address Pattern Found	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/apis	interactiveTutorial	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/pages/login.jag	pass	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	swagger-url	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/pages/login.jag	requestedPage	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	swagger-file	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	type	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	import-definition	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/design	name	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	action	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	action	Cross-Site Scripting	A2, A3, A7, A8
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	swagger-file	Potential File Upload	A1, A5, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/pages/login.jag	name	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	wsdl-url	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-add/ajax/add.jag	action	Cross-Site Scripting	A2, A3, A7, A8
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	version	Cross-Site Scripting	A2, A3, A7, A8
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	provider	Cross-Site Scripting	A2, A3, A7, A8
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	name	Cross-Site Scripting	A2, A3, A7, A8
https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	action	Cross-Site Scripting	A2, A3, A7, A8
https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	provider	Cross-Site Scripting	A2, A3, A7, A8
https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	status	Cross-Site Scripting	A2, A3, A7, A8
https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	version	Cross-Site Scripting	A2, A3, A7, A8
https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	name	Cross-Site Scripting	A2, A3, A7, A8
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	apiThumb	Potential File Upload	A1, A5, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	provider	Query Parameter in SSL Request	A6

https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	provider	MongoDB NoSQL Injection	A1, A7
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	name	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	version	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	techOwnerMail	Email Address in Hidden Parameter	A9
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	name	MongoDB NoSQL Injection	A1, A7
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	version	MongoDB NoSQL Injection	A1, A7
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	bizOwnerMail	Email Address in Hidden Parameter	A9
https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	action	MongoDB NoSQL Injection	A1, A7
https://wso2.sbi.123pay.vn/publisher/site/pages/stats-menu-list.jag	stats-menu-list.jag	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/dagre-d3.min.js	dagre-d3.min.js	Possible Server Path Disclosure Pattern Found	A4, A5, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/pages/add.jag	add.jag	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/publisher/subscriptions	subscriptions	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/bundle.js	bundle.js	Web Application Source Code Disclosure Pattern Found	A4, A5, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/blocks/usage/ajax/usage.jag	usage.jag	Body Parameters Accepted in Query	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/implement	implement	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/publisher/manage	manage	Email Address Pattern Found	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/dca2cc65b6f76f931d17.worker.js	dca2cc65b6f76f931d17.worker.js	Email Address Pattern Found	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/pages/design.jag	design.jag	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/bundle.js	bundle.js	Possible Server Path Disclosure Pattern Found	A4, A5, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/templates/item-implement/js/api-implementation.js	api-implementation.js	Web Application Source Code Disclosure Pattern Found	A4, A5, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/bundle.js	bundle.js	Email Address Pattern Found	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/manage	manage	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage-user/ajax/stats.jag	stats.jag	Body Parameters Accepted in Query	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-throttledcounts/ajax/stats.jag	stats.jag	Body Parameters Accepted in Query	A5, A6, A7, A9

https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage/ajax/stats.jag	stats.jag	Body Parameters Accepted in Query	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-top-users/ajax/stats.jag	stats.jag	Body Parameters Accepted in Query	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	name	Database Error Pattern Found	A1, A7
https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	JSESSIONID	Database Error Pattern Found	A1, A7
https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage-resource-path/ajax/stats.jag	stats.jag	Body Parameters Accepted in Query	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage-destination/ajax/stats.jag	stats.jag	Body Parameters Accepted in Query	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/subscriptions	name	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/info	provider	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/pages/add.jag	pass	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/subscriptions	pass	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/apis	page	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/pages/add.jag	name	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/design	pass	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/pages/all-statistics.jag	stat	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/pages/all-statistics.jag	page	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	life-cycles.jag	Body Parameters Accepted in Query	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/pages/stats-menu-list.jag	pass	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/pages/stats-menu-list.jag	name	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/faulty-invocations/ajax/stats.jag	stats.jag	Body Parameters Accepted in Query	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/developers-time/ajax/stats.jag	stats.jag	Body Parameters Accepted in Query	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/maps/vega.js	vega.js	Email Address Pattern Found	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/info	pass	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	provider	Database Error Pattern Found	A1, A7
https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	publishToGateway	SQL Injection	A1, A7
https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	requireResubscription	SQL Injection	A1, A7

https://wso2.sbi.123pay.vn/publisher/site/blocks/documentation/ajax/docs.jag	action	Cross-Site Scripting	A2, A3, A7, A8
https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	publishToGateway	Database Error Pattern Found	A1, A7
https://wso2.sbi.123pay.vn/carbon/dialog/js/jqueryui/jquery-ui.min.js	jquery-ui.min.js	Possible Server Path Disclosure Pattern Found	A4, A5, A7, A9
https://wso2.sbi.123pay.vn/publisher/apis	query	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/info	action	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/apis	tenant	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/info	version	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/pages/index.jag	pass	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/pages/index.jag	name	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/pages/index.jag	pass	MongoDB NoSQL Injection	A1, A7
https://wso2.sbi.123pay.vn/publisher/api-docs/admin/PizzaShackAPI/1.0.0	1.0.0	Email Address Pattern Found	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/info	name	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/blocks/documentation/ajax/docs.jag	docLocation	Potential File Upload	A1, A5, A7, A9
https://wso2.sbi.123pay.vn/publisher/version	pass	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/design	version	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/templates/documentation/download.jag	resourceUrl	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/userstore/add-user-role.jsp	region	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/design	provider	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/templates/documentation/download.jag	tenant	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/pages/design.jag	name	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/pages/design.jag	version	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/pages/design.jag	provider	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/apis-time/ajax/stats.jag	page	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/implement	version	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/implement	name	Query Parameter in SSL Request	A6

https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/src-noconflict/mode-javascript.js	mode-javascript.js	Possible Server Path Disclosure Pattern Found	A4, A5, A7, A9
https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	login.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/publisher/manage	version	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/implement	provider	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/manage	name	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/manage	provider	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/apis-time/ajax/stats.jag	stat	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/.modal	.modal	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/developers-time/ajax/stats.jag	page	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/developers-time/ajax/stats.jag	stat	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/admin/js/jquery.cookie.js	jquery.cookie.js	Email Address Pattern Found	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/publisher/version	version	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/version	name	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/version	provider	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/publisher/version	version	Body Parameters Accepted in Query	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/carbon/userstore/add-user-role.jsp	item	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/admin/js/cookies.js	cookies.js	Email Address Pattern Found	A5, A6, A7, A9
https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region1_configure_menu	Missing Secure Attribute in Encrypted Session (SSL) Cookie	A2, A6, A8
https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region1_manage_menu	Missing Secure Attribute in Encrypted Session (SSL) Cookie	A2, A6, A8
https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region5_tools_menu	Missing Secure Attribute in Encrypted Session (SSL) Cookie	A2, A6, A8
https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region3_registry_menu	Missing Secure Attribute in Encrypted Session (SSL) Cookie	A2, A6, A8
https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region4_monitor_menu	Missing Secure Attribute in Encrypted Session (SSL) Cookie	A2, A6, A8
https://wso2.sbi.123pay.vn/carbon/admin/admin/jsp/session-validate.jsp	session-validate.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/userstore	region	Query Parameter in	A6

_config/userstore-config.jsp		SSL Request	
https://wso2.sbi.123pay.vn/publisher/site/pages/stats-menu-list.jag	li><a class="substats" title="API Response Times"	HTML Comments Sensitive Information Disclosure	A4, A6
https://wso2.sbi.123pay.vn/carbon/docs/sign in_userguide.html	~ Copyright (c) 2005-2011, WSO2 Inc. (http://www.wso2.org) All Rights Reserved.	HTML Comments Sensitive Information Disclosure	A4, A6
https://wso2.sbi.123pay.vn/carbon/product/about.html	~ Copyright (c) 2005-2010, WSO2 Inc. (http://wso2.com) All Rights Reserved.	HTML Comments Sensitive Information Disclosure	A4, A6
https://wso2.sbi.123pay.vn/carbon/admin/docs/userguide.html	~ Copyright (c) 2005-2011, WSO2 Inc. (http://www.wso2.org) All Rights Reserved.	HTML Comments Sensitive Information Disclosure	A4, A6
https://wso2.sbi.123pay.vn/carbon/admin/jsp/session-validate.jsp	session-validate.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/idpmgt/idp-mgt-list.jsp	idp-mgt-list.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/userstore_config/index.jsp	index.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/ndatasource/index.jsp	index.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/userstore/add-user-role.jsp	add-user-role.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/identity-claim-mgt/list.jsp	item	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/userstore_config/userstore-config.jsp	userstore-config.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/identity-claim-mgt/add.jsp	item	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/admin/index.jsp	loginStatus	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/userstore_config/userstore-config.jsp	item	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/userstore_config/index.jsp	region	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/userstore_config/index.jsp	item	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/application/load-service-provider.jsp	load-service-provider.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/feature-mgt/index.jsp	index.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/ndatasource/index.jsp	region	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/idpmgt/idp-mgt-edit-load-local.jsp	idp-mgt-edit-load-local.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/log-admin/log-admin.jsp	item	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/ndatasource/index.jsp	item	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/identity-claim-mgt/list.jsp	list.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/application/list-service-providers.jsp	list-service-providers.jsp	Unsafe third-party link (target="_blank")	A9

https://wso2.sbi.123pay.vn/carbon/application/add-service-provider.jsp	add-service-provider.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/identity-claim-mgt/add.jsp	add.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/eventstream/index.jsp	index.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/feature-mgt/index.jsp	item	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/identity-claim-mgt/add.jsp	region	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/identity-claim-mgt/list.jsp	region	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/idpmgt/idp-mgt-edit-load-local.jsp	item	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/application/add-service-provider.jsp	region	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/log-admin/log-admin.jsp	log-admin.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/application/add-service-provider.jsp	item	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/application/list-service-providers.jsp	region	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/application/list-service-providers.jsp	item	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/application/load-service-provider.jsp	spName	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/application/load-service-provider.jsp	?region	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/application/load-service-provider.jsp	item	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/log-admin/log-admin.jsp	region	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/idpmgt/idp-mgt-list.jsp	region	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/feature-mgt/index.jsp	region	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/idpmgt/idp-mgt-list.jsp	item	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/tenant-mgt/add_tenant.jsp	add_tenant.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/idpmgt/idp-mgt-edit-load-local.jsp	region	Query Parameter in SSL Request	A6
https://wso2.sbi.123pay.vn/carbon/bampubsvcstat/configure_message_tracing.jsp	configure_message_tracing.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/webapp-mgt/upload.jsp	upload.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/webapp-list/index.jsp	index.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/tenant-mgt/view_tenants.jsp	view_tenants.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/lcm/lcm.jsp	lcm.jsp	Unsafe third-party link (target="_blank")	A9

https://wso2.sbi.123pay.vn/carbon/configadmin/index.jsp	index.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/generic/add_edit.jsp	add_edit.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/jaggeryapp-mgt/uploadjaggeryapp.jsp	uploadjaggeryapp.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/carbonapps/index.jsp	index.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/server-admin/index.jsp	index.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/eventpublisher/index.jsp	index.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/keystore mgt/add-keystore-step1.jsp	add-keystore-step1.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/carbonapps/app_upload.jsp	app_upload.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/roles-mgt/server-roles-mgt.jsp	server-roles-mgt.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/eventprocessor/index.jsp	index.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/generic/generic_artifact.jsp	generic_artifact.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/resources/resource.jsp	resource.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/extensions/add_extensions.jsp	add_extensions.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/search/advancedSearch.jsp	advancedSearch.jsp	Unsafe third-party link (target="_blank")	A9
https://wso2.sbi.123pay.vn/carbon/generic/list.jsp	list.jsp	Unsafe third-party link (target="_blank")	A9

Detailed Security Issues by Sections

H A1 - Injection 16

MongoDB NoSQL Injection

Risk:	It is possible to view, modify or delete database entries and tables
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Ensure user input is of the correct type and escape it properly

Severity	URL	Entity
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	provider
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	name
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	version
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	action
High	https://wso2.sbi.123pay.vn/publisher/site/pages/index.jag	pass

SQL Injection

Risk:	It is possible to view, modify or delete database entries and tables
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Severity	URL	Entity
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	life-cycles.jag
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	publishToGateway
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	requireResubscription

Database Error Pattern Found

Risk:	It is possible to view, modify or delete database entries and tables
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	life-cycles.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	name
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	JSESSIONID
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	provider
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	publishToGateway

Potential File Upload

Risk:	It is possible to run remote commands on the web server. This usually means complete compromise of the server and its contents It is possible to upload, modify or delete web pages, scripts and files on the web server
Causes:	Insecure web application programming or configuration
Fix:	Restrict user capabilities and permissions during the file upload process

Severity	URL	Entity
Informational	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	swagger-file
Informational	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	apiThumb
Informational	https://wso2.sbi.123pay.vn/publisher/site/blocks/documentation/ajax/docs.jag	docLocation

H A2 - Broken authentication and session management 16

Cross-Site Scripting

Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Severity	URL	Entity
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	action
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-add/ajax/add.jag	action
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	version
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	provider
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	name
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	action
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	provider
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	status
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	version
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	name
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/documentation/ajax/docs.jag	action

Missing Secure Attribute in Encrypted Session (SSL) Cookie

Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Causes:	The web application sends non-secure cookies over SSL
Fix:	Add the 'Secure' attribute to all sensitive cookies

Severity	URL	Entity
Medium	https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region1_configure_menu
Medium	https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region1_manage_menu
Medium	https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region5_tools_menu
Medium	https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region3_registry_menu
Medium	https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region4_monitor_menu

H A3 - Cross site scripting (XSS) 11

Cross-Site Scripting

Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Severity	URL	Entity
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	action
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-add/ajax/add.jag	action
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	version
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	provider
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	name
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	action
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	provider
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	status
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	version
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	name
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/documentation/ajax/docs.jag	action

L A4 - Insecure direct object reference 14

Web Application Source Code Disclosure Pattern Found

Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Latest patches or hotfixes for 3rd. party products were not installed Temporary files were left in production environment Debugging information was left by the programmer in web pages
Fix:	Remove source code files from your web-server and apply any relevant patches

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/templates/item-info/js/lodash.min.js	lodash.min.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/jsonpath-0.15.0.js	jsonpath-0.15.0.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/dagre-d3.min.js	dagre-d3.min.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/bundle.js	bundle.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/templates/item-implement/js/api-implementation.js	api-implementation.js

HTML Comments Sensitive Information Disclosure

Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Debugging information was left by the programmer in web pages
Fix:	Remove sensitive information from HTML comments

Severity	URL	Entity
Informational	https://wso2.sbi.123pay.vn/publisher/site/pages/stats-menu-list.jag	li><a class="substats" title="API Response Times"
Informational	https://wso2.sbi.123pay.vn/carbon/docs/signin_userguide.html	~ Copyright (c) 2005-2011, WSO2 Inc. (http://www.wso2.org) All Rights Reserved.
Informational	https://wso2.sbi.123pay.vn/carbon/product/about.html	~ Copyright (c) 2005-2010, WSO2 Inc. (http://wso2.com) All Rights Reserved.
Informational	https://wso2.sbi.123pay.vn/carbon/admin/docs/userguide.html	~ Copyright (c) 2005-2011, WSO2 Inc. (http://www.wso2.org) All Rights Reserved.

Possible Server Path Disclosure Pattern Found

Risk:	It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application
Causes:	Latest patches or hotfixes for 3rd. party products were not installed
Fix:	Download the relevant security patch for your web server or web application.

Severity	URL	Entity
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/codemirror/addon/jshint.js	jshint.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/dagre-d3.min.js	dagre-d3.min.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/bundle.js	bundle.js
Informational	https://wso2.sbi.123pay.vn/carbon/dialog/js/jqueryui/jquery-ui.min.js	jquery-ui.min.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/src-noconflict/mode-javascript.js	mode-javascript.js

L A5 - Security Misconfiguration 44

Body Parameters Accepted in Query

Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Do not accept body parameters that are sent in the query string

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-add/ajax/add.jag	add.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-subscriptions/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-last-access-times/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/usage/ajax/usage.jag	usage.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage-user/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-throttledcounts/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-top-users/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage-resource-path/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage-destination/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	life-cycles.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/faulty-invocations/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/developers-time/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/version	version

Credit Card Number Pattern Found

Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove credit card numbers from your website

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/1882cde30750506693b8.worker.js	1882cde30750506693b8.worker.js

Missing "Content-Security-Policy" header

Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/i18n/i18next-1.5.9.js	i18next-1.5.9.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/enjoyhint-3.1.0/js/cloud-enjoyhint-script-data.js	cloud-enjoyhint-script-data.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/handlebars.min.js	handlebars.min.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/jquery-validation/jquery.validate.min.js	jquery.validate.min.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/select2_4.0.0/js/select2.full.min.js	select2.full.min.js

Web Application Source Code Disclosure Pattern Found

Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Latest patches or hotfixes for 3rd. party products were not installed Temporary files were left in production environment Debugging information was left by the programmer in web pages
Fix:	Remove source code files from your web-server and apply any relevant patches

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/templates/item-info/js/lodash.min.js	lodash.min.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/jsonpath-0.15.0.js	jsonpath-0.15.0.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/dagre-d3.min.js	dagre-d3.min.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/bundle.js	bundle.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/templates/item-implement/js/api-implementation.js	api-implementation.js

Email Address Pattern Found

Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Severity	URL	Entity
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/templates/listing/js/samples.js	samples.js
Informational	https://wso2.sbi.123pay.vn/publisher/design	design
Informational	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	add.jag
Informational	https://wso2.sbi.123pay.vn/publisher/manage	manage
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/dca2cc65b6f76f931d17.worker.js	dca2cc65b6f76f931d17.worker.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/bundle.js	bundle.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/maps/vega.js	vega.js
Informational	https://wso2.sbi.123pay.vn/publisher/api-docs/admin/PizzaShackAPI/1.0.0	1.0.0
Informational	https://wso2.sbi.123pay.vn/carbon/admin/js/jquery.cookie.js	jquery.cookie.js
Informational	https://wso2.sbi.123pay.vn/carbon/admin/js/cookies.js	cookies.js

Possible Server Path Disclosure Pattern Found

Risk:	It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application
Causes:	Latest patches or hotfixes for 3rd. party products were not installed
Fix:	Download the relevant security patch for your web server or web application.

Severity	URL	Entity
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/codemirror/addon/jshint.js	jshint.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/dagre-d3.min.js	dagre-d3.min.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/bundle.js	bundle.js
Informational	https://wso2.sbi.123pay.vn/carbon/dialog/js/jqueryui/jquery-ui.min.js	jquery-ui.min.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/src-noconflict/mode-javascript.js	mode-javascript.js

Potential File Upload

Risk:	It is possible to run remote commands on the web server. This usually means complete compromise of the server and its contents It is possible to upload, modify or delete web pages, scripts and files on the web server
Causes:	Insecure web application programming or configuration
Fix:	Restrict user capabilities and permissions during the file upload process

Severity	URL	Entity
Informational	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	swagger-file
Informational	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	apiThumb
Informational	https://wso2.sbi.123pay.vn/publisher/site/blocks/documentation/ajax/docs.jag	docLocation

M A6 - Sensitive Data Exposure 123

Missing Secure Attribute in Encrypted Session (SSL) Cookie

Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Causes:	The web application sends non-secure cookies over SSL
Fix:	Add the 'Secure' attribute to all sensitive cookies

Severity	URL	Entity
Medium	https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region1_configure_menu
Medium	https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region1_manage_menu
Medium	https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region5_tools_menu
Medium	https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region3_registry_menu
Medium	https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region4_monitor_menu

Body Parameters Accepted in Query

Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Do not accept body parameters that are sent in the query string

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-add/ajax/add.jag	add.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-subscriptions/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-last-access-times/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/usage/ajax/usage.jag	usage.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage-user/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-throttledcounts/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-top-users/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage-resource-path/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage-destination/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	life-cycles.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/faulty-invocations/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/developers-time/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/version	version

Credit Card Number Pattern Found

Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove credit card numbers from your website

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/1882cde30750506693b8.worker.js	1882cde30750506693b8.worker.js

Missing "Content-Security-Policy" header

Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/i18n/i18next-1.5.9.js	i18next-1.5.9.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/enjoyhint-3.1.0/js/cloud-enjoyhint-script-data.js	cloud-enjoyhint-script-data.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/handlebars.min.js	handlebars.min.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/jquery-validation/jquery.validate.min.js	jquery.validate.min.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/select2_4.0.0/js/select2.full.min.js	select2.full.min.js

Query Parameter in SSL Request

Risk: It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Causes: Query parameters were passed over SSL, and may contain sensitive information

Fix: Always use SSL and POST (body) parameters when sending sensitive information.

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/publisher/apis	interactiveTutorial
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/login.jag	pass
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	swagger-url
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/login.jag	requestedPage
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	swagger-file
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	type
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	import-definition
Low	https://wso2.sbi.123pay.vn/publisher/design	name
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	action
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/login.jag	name
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	wsdl-url
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	provider
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	name
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	version
Low	https://wso2.sbi.123pay.vn/publisher/subscriptions	name
Low	https://wso2.sbi.123pay.vn/publisher/info	provider
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/add.jag	pass
Low	https://wso2.sbi.123pay.vn/publisher/subscriptions	pass
Low	https://wso2.sbi.123pay.vn/publisher/apis	page
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/add.jag	name

Low	https://wso2.sbi.123pay.vn/publisher/design	pass
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/all-statistics.jag	stat
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/all-statistics.jag	page
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/stats-menu-list.jag	pass
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/stats-menu-list.jag	name
Low	https://wso2.sbi.123pay.vn/publisher/info	pass
Low	https://wso2.sbi.123pay.vn/publisher/apis	query
Low	https://wso2.sbi.123pay.vn/publisher/info	action
Low	https://wso2.sbi.123pay.vn/publisher/apis	tenant
Low	https://wso2.sbi.123pay.vn/publisher/info	version
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/index.jag	pass
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/index.jag	name
Low	https://wso2.sbi.123pay.vn/publisher/info	name
Low	https://wso2.sbi.123pay.vn/publisher/version	pass
Low	https://wso2.sbi.123pay.vn/publisher/design	version
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/templates/documentation/download.jag	resourceUrl
Low	https://wso2.sbi.123pay.vn/carbon/userstore/add-user-role.jsp	region
Low	https://wso2.sbi.123pay.vn/publisher/design	provider
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/templates/documentation/download.jag	tenant
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/design.jag	name
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/design.jag	version
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/design.jag	provider
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/apis-time/ajax/stats.jag	page
Low	https://wso2.sbi.123pay.vn/publisher/implement	version
Low	https://wso2.sbi.123pay.vn/publisher/implement	name

Low	https://wso2.sbi.123pay.vn/publisher/manage	version
Low	https://wso2.sbi.123pay.vn/publisher/implement	provider
Low	https://wso2.sbi.123pay.vn/publisher/manage	name
Low	https://wso2.sbi.123pay.vn/publisher/manage	provider
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/apis-time/ajax/stats.jag	stat
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/developers-time/ajax/stats.jag	page
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/developers-time/ajax/stats.jag	stat
Low	https://wso2.sbi.123pay.vn/publisher/version	version
Low	https://wso2.sbi.123pay.vn/publisher/version	name
Low	https://wso2.sbi.123pay.vn/publisher/version	provider
Low	https://wso2.sbi.123pay.vn/carbon/userstore/add-user-role.jsp	item
Low	https://wso2.sbi.123pay.vn/carbon/userstore_config/userstore-config.jsp	region
Low	https://wso2.sbi.123pay.vn/carbon/identity-claim-mgt/list.jsp	item
Low	https://wso2.sbi.123pay.vn/carbon/identity-claim-mgt/add.jsp	item
Low	https://wso2.sbi.123pay.vn/carbon/admin/index.jsp	loginStatus
Low	https://wso2.sbi.123pay.vn/carbon/userstore_config/userstore-config.jsp	item
Low	https://wso2.sbi.123pay.vn/carbon/userstore_config/index.jsp	region
Low	https://wso2.sbi.123pay.vn/carbon/userstore_config/index.jsp	item
Low	https://wso2.sbi.123pay.vn/carbon/ndatasource/index.jsp	region
Low	https://wso2.sbi.123pay.vn/carbon/log-admin/log-admin.jsp	item
Low	https://wso2.sbi.123pay.vn/carbon/ndatasource/index.jsp	item
Low	https://wso2.sbi.123pay.vn/carbon/feature-mgt/index.jsp	item
Low	https://wso2.sbi.123pay.vn/carbon/identity-claim-mgt/add.jsp	region

Low	https://wso2.sbi.123pay.vn/carbon/identity-claim-mgt/list.jsp	region
Low	https://wso2.sbi.123pay.vn/carbon/idpmgt/idp-mgt-edit-load-local.jsp	item
Low	https://wso2.sbi.123pay.vn/carbon/application/add-service-provider.jsp	region
Low	https://wso2.sbi.123pay.vn/carbon/application/add-service-provider.jsp	item
Low	https://wso2.sbi.123pay.vn/carbon/application/list-service-providers.jsp	region
Low	https://wso2.sbi.123pay.vn/carbon/application/list-service-providers.jsp	item
Low	https://wso2.sbi.123pay.vn/carbon/application/load-service-provider.jsp	spName
Low	https://wso2.sbi.123pay.vn/carbon/application/load-service-provider.jsp	?region
Low	https://wso2.sbi.123pay.vn/carbon/application/load-service-provider.jsp	item
Low	https://wso2.sbi.123pay.vn/carbon/log-admin/log-admin.jsp	region
Low	https://wso2.sbi.123pay.vn/carbon/idpmgt/idp-mgt-list.jsp	region
Low	https://wso2.sbi.123pay.vn/carbon/feature-mgt/index.jsp	region
Low	https://wso2.sbi.123pay.vn/carbon/idpmgt/idp-mgt-list.jsp	item
Low	https://wso2.sbi.123pay.vn/carbon/idpmgt/idp-mgt-edit-load-local.jsp	region

Email Address Pattern Found

Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Severity	URL	Entity
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/templates/listing/js/samples.js	samples.js
Informational	https://wso2.sbi.123pay.vn/publisher/design	design
Informational	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	add.jag
Informational	https://wso2.sbi.123pay.vn/publisher/manage	manage
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/dca2cc65b6f76f931d17.worker.js	dca2cc65b6f76f931d17.worker.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/bundle.js	bundle.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/maps/vega.js	vega.js
Informational	https://wso2.sbi.123pay.vn/publisher/api-docs/admin/PizzaShackAPI/1.0.0	1.0.0
Informational	https://wso2.sbi.123pay.vn/carbon/admin/js/jquery.cookie.js	jquery.cookie.js
Informational	https://wso2.sbi.123pay.vn/carbon/admin/js/cookies.js	cookies.js

HTML Comments Sensitive Information Disclosure

Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Debugging information was left by the programmer in web pages
Fix:	Remove sensitive information from HTML comments

Severity	URL	Entity
Informational	https://wso2.sbi.123pay.vn/publisher/site/pages/stats-menu-list.jag	li><a class="substats" title="API Response Times"
Informational	https://wso2.sbi.123pay.vn/carbon/docs/signin_userguide.html	~ Copyright (c) 2005-2011, WSO2 Inc. (http://www.wso2.org) All Rights Reserved.
Informational	https://wso2.sbi.123pay.vn/carbon/product/about.html	~ Copyright (c) 2005-2010, WSO2 Inc. (http://wso2.com) All Rights Reserved.
Informational	https://wso2.sbi.123pay.vn/carbon/admin/docs/userguide.html	~ Copyright (c) 2005-2011, WSO2 Inc. (http://www.wso2.org) All Rights Reserved.

SSL Certificate Domain Name Mismatch

Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to prevent the web application from serving other users (denial of service)
Causes:	The web server or application server are configured in an insecure way
Fix:	Update your SSL certificate, and make sure that all attributes are valid

Severity	URL	Entity
Informational	https://wso2.sbi.123pay.vn/	wso2.sbi.123pay.vn

H A7 - Missing Function Level Access Control 69

Cross-Site Scripting

Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Severity	URL	Entity
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	action
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-add/ajax/add.jag	action
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	version
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	provider
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	name
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	action
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	provider
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	status
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	version
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	name
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/documentation/ajax/docs.jag	action

MongoDB NoSQL Injection

Risk:	It is possible to view, modify or delete database entries and tables
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Ensure user input is of the correct type and escape it properly

Severity	URL	Entity
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	provider
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	name
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	version
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	action
High	https://wso2.sbi.123pay.vn/publisher/site/pages/index.jag	pass

SQL Injection

Risk:	It is possible to view, modify or delete database entries and tables
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Severity	URL	Entity
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	life-cycles.jag
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	publishToGateway
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	requireResubscription

Body Parameters Accepted in Query

Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Do not accept body parameters that are sent in the query string

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-add/ajax/add.jag	add.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-subscriptions/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-last-access-times/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/usage/ajax/usage.jag	usage.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage-user/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-throttledcounts/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-top-users/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage-resource-path/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage-destination/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	life-cycles.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/faulty-invocations/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/developers-time/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/version	version

Credit Card Number Pattern Found

Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove credit card numbers from your website

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/1882cde30750506693b8.worker.js	1882cde30750506693b8.worker.js

Database Error Pattern Found

Risk:	It is possible to view, modify or delete database entries and tables
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	life-cycles.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	name
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	JSESSIONID
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	provider
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	publishToGateway

Missing "Content-Security-Policy" header

Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/i18n/i18next-1.5.9.js	i18next-1.5.9.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/enjoyhint-3.1.0/js/cloud-enjoyhint-script-data.js	cloud-enjoyhint-script-data.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/handlebars.min.js	handlebars.min.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/jquery-validation/jquery.validate.min.js	jquery.validate.min.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/select2_4.0.0/js/select2.full.min.js	select2.full.min.js

Web Application Source Code Disclosure Pattern Found

Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Latest patches or hotfixes for 3rd. party products were not installed Temporary files were left in production environment Debugging information was left by the programmer in web pages
Fix:	Remove source code files from your web-server and apply any relevant patches

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/templates/item-info/js/lodash.min.js	lodash.min.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/jsonpath-0.15.0.js	jsonpath-0.15.0.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/dagre-d3.min.js	dagre-d3.min.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/bundle.js	bundle.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/templates/item-implement/js/api-implementation.js	api-implementation.js

Email Address Pattern Found

Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Severity	URL	Entity
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/templates/listing/js/samples.js	samples.js
Informational	https://wso2.sbi.123pay.vn/publisher/design	design
Informational	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	add.jag
Informational	https://wso2.sbi.123pay.vn/publisher/manage	manage
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/dca2cc65b6f76f931d17.worker.js	dca2cc65b6f76f931d17.worker.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/bundle.js	bundle.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/maps/vega.js	vega.js
Informational	https://wso2.sbi.123pay.vn/publisher/api-docs/admin/PizzaShackAPI/1.0.0	1.0.0
Informational	https://wso2.sbi.123pay.vn/carbon/admin/js/jquery.cookie.js	jquery.cookie.js
Informational	https://wso2.sbi.123pay.vn/carbon/admin/js/cookies.js	cookies.js

Possible Server Path Disclosure Pattern Found

Risk:	It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application
Causes:	Latest patches or hotfixes for 3rd. party products were not installed
Fix:	Download the relevant security patch for your web server or web application.

Severity	URL	Entity
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/codemirror/addon/jshint.js	jshint.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/dagre-d3.min.js	dagre-d3.min.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/bundle.js	bundle.js
Informational	https://wso2.sbi.123pay.vn/carbon/dialog/js/jqueryui/jquery-ui.min.js	jquery-ui.min.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/src-noconflict/mode-javascript.js	mode-javascript.js

Potential File Upload

Risk:	It is possible to run remote commands on the web server. This usually means complete compromise of the server and its contents It is possible to upload, modify or delete web pages, scripts and files on the web server
Causes:	Insecure web application programming or configuration
Fix:	Restrict user capabilities and permissions during the file upload process

Severity	URL	Entity
Informational	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	swagger-file
Informational	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	apiThumb
Informational	https://wso2.sbi.123pay.vn/publisher/site/blocks/documentation/ajax/docs.jag	docLocation

SSL Certificate Domain Name Mismatch

Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to prevent the web application from serving other users (denial of service)
Causes:	The web server or application server are configured in an insecure way
Fix:	Update your SSL certificate, and make sure that all attributes are valid

Severity	URL	Entity
Informational	https://wso2.sbi.123pay.vn/	wso2.sbi.123pay.vn

H A8 - Cross site request forgery (CSRF) 16

Cross-Site Scripting

Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Severity	URL	Entity
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	action
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-add/ajax/add.jag	action
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	version
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	provider
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	name
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	action
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	provider
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	status
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	version
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	name
High	https://wso2.sbi.123pay.vn/publisher/site/blocks/documentation/ajax/docs.jag	action

Missing Secure Attribute in Encrypted Session (SSL) Cookie

Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Causes:	The web application sends non-secure cookies over SSL
Fix:	Add the 'Secure' attribute to all sensitive cookies

Severity	URL	Entity
Medium	https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region1_configure_menu
Medium	https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region1_manage_menu
Medium	https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region5_tools_menu
Medium	https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region3_registry_menu
Medium	https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	region4_monitor_menu

L A9 - Using Known Vulnerable Components 99

Body Parameters Accepted in Query

Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Do not accept body parameters that are sent in the query string

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-add/ajax/add.jag	add.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-subscriptions/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-last-access-times/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/usage/ajax/usage.jag	usage.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage-user/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-throttledcounts/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-top-users/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage-resource-path/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/api-usage-destination/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/life-cycles/ajax/life-cycles.jag	life-cycles.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/faulty-invocations/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/blocks/stats/developers-time/ajax/stats.jag	stats.jag
Low	https://wso2.sbi.123pay.vn/publisher/version	version

Credit Card Number Pattern Found

Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove credit card numbers from your website

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/1882cde30750506693b8.worker.js	1882cde30750506693b8.worker.js

Missing "Content-Security-Policy" header

Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc. It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/i18n/i18next-1.5.9.js	i18next-1.5.9.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/enjoyhint-3.1.0/js/cloud-enjoyhint-script-data.js	cloud-enjoyhint-script-data.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/handlebars.min.js	handlebars.min.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/jquery-validation/jquery.validate.min.js	jquery.validate.min.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/select2_4.0.0/js/select2.full.min.js	select2.full.min.js

Unsafe third-party link (target="_blank")

Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	The rel attribute in the link element is not set to "noopener noreferrer".
Fix:	Add the attribute rel = "noopener noreferrer" to each link element with target="_blank"

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/carbon/admin/index.jsp	index.jsp
Low	https://wso2.sbi.123pay.vn/	
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/index.jag	index.jag
Low	https://wso2.sbi.123pay.vn/publisher/	
Low	https://wso2.sbi.123pay.vn/publisher/apis	apis
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/login.jag	login.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/all-statistics.jag	all-statistics.jag
Low	https://wso2.sbi.123pay.vn/publisher/design	design
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/stats-menu-list.jag	stats-menu-list.jag
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/add.jag	add.jag
Low	https://wso2.sbi.123pay.vn/publisher/subscriptions	subscriptions
Low	https://wso2.sbi.123pay.vn/publisher/implement	implement
Low	https://wso2.sbi.123pay.vn/publisher/site/pages/design.jag	design.jag
Low	https://wso2.sbi.123pay.vn/publisher/manage	manage
Low	https://wso2.sbi.123pay.vn/carbon/admin/login.jsp	login.jsp
Low	https://wso2.sbi.123pay.vn/.modal	.modal
Low	https://wso2.sbi.123pay.vn/carbon/admin/admin/jsp/session-validate.jsp	session-validate.jsp
Low	https://wso2.sbi.123pay.vn/carbon/admin/jsp/session-validate.jsp	session-validate.jsp
Low	https://wso2.sbi.123pay.vn/carbon/idpmgt/idp-mgt-list.jsp	idp-mgt-list.jsp
Low	https://wso2.sbi.123pay.vn/carbon/userstore_config/index.jsp	index.jsp

Low	https://wso2.sbi.123pay.vn/carbon/ndatasource/index.jsp	index.jsp
Low	https://wso2.sbi.123pay.vn/carbon/userstore/add-user-role.jsp	add-user-role.jsp
Low	https://wso2.sbi.123pay.vn/carbon/userstore_config/userstore-config.jsp	userstore-config.jsp
Low	https://wso2.sbi.123pay.vn/carbon/application/load-service-provider.jsp	load-service-provider.jsp
Low	https://wso2.sbi.123pay.vn/carbon/feature-mgt/index.jsp	index.jsp
Low	https://wso2.sbi.123pay.vn/carbon/idpmgt/idp-mgt-edit-load-local.jsp	idp-mgt-edit-load-local.jsp
Low	https://wso2.sbi.123pay.vn/carbon/identity-claim-mgt/list.jsp	list.jsp
Low	https://wso2.sbi.123pay.vn/carbon/application/list-service-providers.jsp	list-service-providers.jsp
Low	https://wso2.sbi.123pay.vn/carbon/application/add-service-provider.jsp	add-service-provider.jsp
Low	https://wso2.sbi.123pay.vn/carbon/identity-claim-mgt/add.jsp	add.jsp
Low	https://wso2.sbi.123pay.vn/carbon/eventstream/index.jsp	index.jsp
Low	https://wso2.sbi.123pay.vn/carbon/log-admin/log-admin.jsp	log-admin.jsp
Low	https://wso2.sbi.123pay.vn/carbon/tenant-mgt/add_tenant.jsp	add_tenant.jsp
Low	https://wso2.sbi.123pay.vn/carbon/bampubsvcstat/configure_message_tracing.jsp	configure_message_tracing.jsp
Low	https://wso2.sbi.123pay.vn/carbon/webapp-mgt/upload.jsp	upload.jsp
Low	https://wso2.sbi.123pay.vn/carbon/webapp-list/index.jsp	index.jsp
Low	https://wso2.sbi.123pay.vn/carbon/tenant-mgt/view_tenants.jsp	view_tenants.jsp
Low	https://wso2.sbi.123pay.vn/carbon/lcm/lcm.jsp	lcm.jsp
Low	https://wso2.sbi.123pay.vn/carbon/configadmin/index.jsp	index.jsp
Low	https://wso2.sbi.123pay.vn/carbon/generic/add_edit.jsp	add_edit.jsp
Low	https://wso2.sbi.123pay.vn/carbon/jaggeryapp-mgt/uploadjaggeryapp.jsp	uploadjaggeryapp.jsp
Low	https://wso2.sbi.123pay.vn/carbon/carbonapps/index.jsp	index.jsp
Low	https://wso2.sbi.123pay.vn/carbon/server-admin/index.jsp	index.jsp

Low	https://wso2.sbi.123pay.vn/carbon/eventpublisher/index.jsp	index.jsp
Low	https://wso2.sbi.123pay.vn/carbon/keystore mgt/add-keystore-step1.jsp	add-keystore-step1.jsp
Low	https://wso2.sbi.123pay.vn/carbon/carbonapps/app_upload.jsp	app_upload.jsp
Low	https://wso2.sbi.123pay.vn/carbon/roles-mgt/server-roles-mgt.jsp	server-roles-mgt.jsp
Low	https://wso2.sbi.123pay.vn/carbon/eventprocessor/index.jsp	index.jsp
Low	https://wso2.sbi.123pay.vn/carbon/generic/generic_artifact.jsp	generic_artifact.jsp
Low	https://wso2.sbi.123pay.vn/carbon/resources/resource.jsp	resource.jsp
Low	https://wso2.sbi.123pay.vn/carbon/extensions/add_extensions.jsp	add_extensions.jsp
Low	https://wso2.sbi.123pay.vn/carbon/search/advancedSearch.jsp	advancedSearch.jsp
Low	https://wso2.sbi.123pay.vn/carbon/generic/list.jsp	list.jsp

Web Application Source Code Disclosure Pattern Found

Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Latest patches or hotfixes for 3rd. party products were not installed Temporary files were left in production environment Debugging information was left by the programmer in web pages
Fix:	Remove source code files from your web-server and apply any relevant patches

Severity	URL	Entity
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/templates/item-info/js/lodash.min.js	lodash.min.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/jsonpath-0.15.0.js	jsonpath-0.15.0.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/dagre-d3.min.js	dagre-d3.min.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/bundle.js	bundle.js
Low	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/templates/item-implement/js/api-implementation.js	api-implementation.js

Email Address in Hidden Parameter

Risk:	It is possible to send e-mails through your web application, using spoofed e-mail addresses
Causes:	Parameter values were 'hardcoded' in the HTML as a read-only parameter
Fix:	Remove the recipient e-mail address hidden parameter

Severity	URL	Entity
Informational	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	techOwnerMail
Informational	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	bizOwnerMail

Email Address Pattern Found

Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Severity	URL	Entity
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/templates/listing/js/samples.js	samples.js
Informational	https://wso2.sbi.123pay.vn/publisher/design	design
Informational	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	add.jag
Informational	https://wso2.sbi.123pay.vn/publisher/manage	manage
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/dca2cc65b6f76f931d17.worker.js	dca2cc65b6f76f931d17.worker.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/bundle.js	bundle.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/maps/vega.js	vega.js
Informational	https://wso2.sbi.123pay.vn/publisher/api-docs/admin/PizzaShackAPI/1.0.0	1.0.0
Informational	https://wso2.sbi.123pay.vn/carbon/admin/js/jquery.cookie.js	jquery.cookie.js
Informational	https://wso2.sbi.123pay.vn/carbon/admin/js/cookies.js	cookies.js

Possible Server Path Disclosure Pattern Found

Risk:	It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application
Causes:	Latest patches or hotfixes for 3rd. party products were not installed
Fix:	Download the relevant security patch for your web server or web application.

Severity	URL	Entity
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/codemirror/addon/jshint.js	jshint.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/dagre-d3.min.js	dagre-d3.min.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/swagger-editor/dist/bundle.js	bundle.js
Informational	https://wso2.sbi.123pay.vn/carbon/dialog/js/jqueryui/jquery-ui.min.js	jquery-ui.min.js
Informational	https://wso2.sbi.123pay.vn/publisher/site/themes/wso2/libs/src-noconflict/mode-javascript.js	mode-javascript.js

Potential File Upload

Risk:	It is possible to run remote commands on the web server. This usually means complete compromise of the server and its contents It is possible to upload, modify or delete web pages, scripts and files on the web server
Causes:	Insecure web application programming or configuration
Fix:	Restrict user capabilities and permissions during the file upload process

Severity	URL	Entity
Informational	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	swagger-file
Informational	https://wso2.sbi.123pay.vn/publisher/site/blocks/item-design/ajax/add.jag	apiThumb
Informational	https://wso2.sbi.123pay.vn/publisher/site/blocks/documentation/ajax/docs.jag	docLocation

A10 - UnvalidatedRedirects and Forwards 0