

# invicti

10/20/2023 3:29:49 PM (UTC+05:30)

## Executive Summary Report

<https://dpisso.tserver.co.in/>

Scan Time : 10/19/2023 12:59:00 PM (UTC+05:30)  
 Scan Duration : 00:13:35:37  
 Total Requests : 134,283  
 Average Speed : 2.7r/s

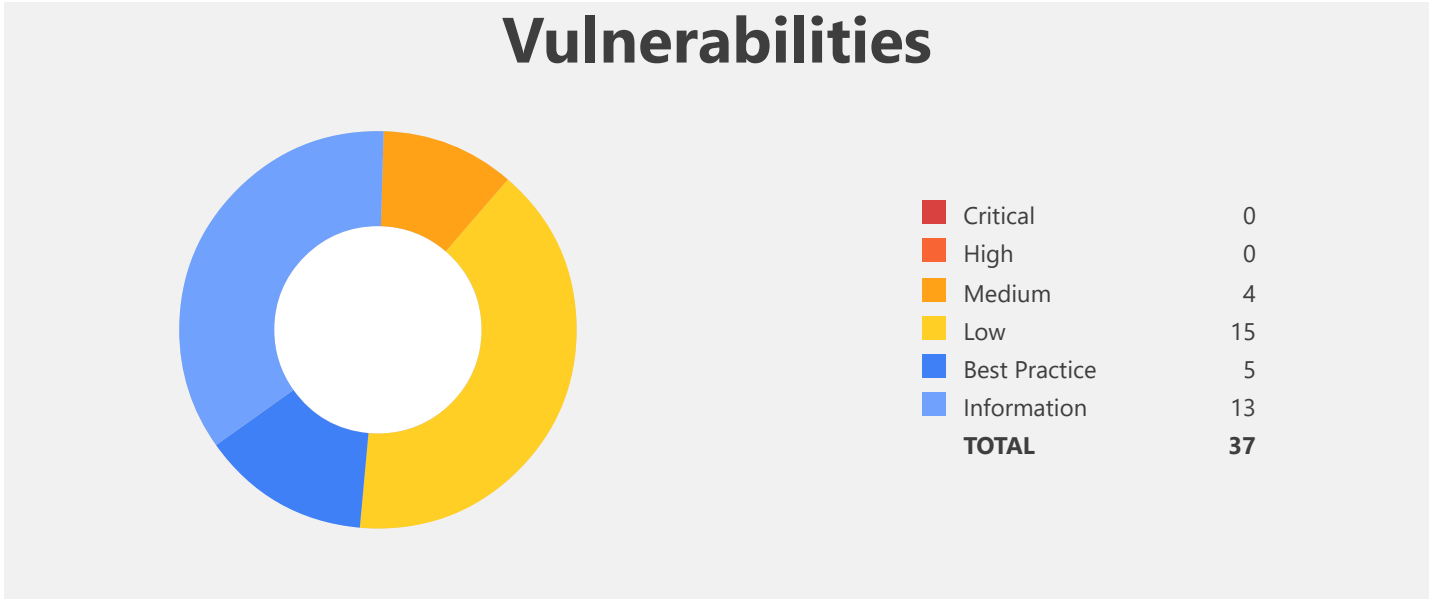
Risk Level:  
**MEDIUM**
















### Your website is fairly insecure!
















There are some problems on the application that need to be addressed but nothing that requires you to panic. Address the identified issues in timely manner.








### What's the Worst that could Happen?

An attacker could access user information sent over the internet or public Wi-Fi or a similar environment  
 This might include passwords, usernames, and the content of web pages viewed.









Vulnerability	Suggested Action
 HTTP Strict Transport Security (HSTS) Errors and Warnings	<b>Fix soon:</b> You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
 Out-of-date Version (jQuery)	<b>Fix soon:</b> You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
 Session Cookie Not Marked as Secure	<b>Fix soon:</b> You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
 Weak Ciphers Enabled	<b>Fix soon:</b> You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
 [Possible] Cross-site Request Forgery	<b>Consider fixing after confirmed:</b> These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 [Possible] Cross-site Request Forgery in Login Form	<b>Consider fixing after confirmed:</b> These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 [Possible] Internal IP Address Disclosure	<b>Consider fixing after confirmed:</b> These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Insecure Transportation Security Protocol Supported (TLS 1.0)	<b>Consider fixing:</b> These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Internal Server Error	<b>Consider fixing:</b> These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Missing X-Frame-Options Header	<b>Consider fixing:</b> These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Programming Error Message	<b>Consider fixing:</b> These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Stack Trace Disclosure (ASP.NET)	<b>Consider fixing:</b> These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Version Disclosure (ASP.NET)	<b>Consider fixing:</b> These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Version Disclosure (Bootstrapjs)	<b>Consider fixing:</b> These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Version Disclosure (BootstrapTable)	<b>Consider fixing:</b> These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.

Vulnerability	Suggested Action
 Version Disclosure (IIS)	<b>Consider fixing:</b> These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Version Disclosure (Jquery)	<b>Consider fixing:</b> These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Version Disclosure (Lodash)	<b>Consider fixing:</b> These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Version Disclosure (Popper.js)	<b>Consider fixing:</b> These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Content Security Policy (CSP) Not Implemented	<b>No action required:</b> Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
 Insecure Transportation Security Protocol Supported (TLS 1.1)	<b>No action required:</b> Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
 Missing X-XSS-Protection Header	<b>No action required:</b> Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
 Referrer-Policy Not Implemented	<b>No action required:</b> Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
 Subresource Integrity (SRI) Not Implemented	<b>No action required:</b> Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
 ASP.NET Identified	<b>No action required:</b> These items are just for your information. You don't need to take any action on them but they might be useful to know.
 Autocomplete Enabled (Password Field)	<b>No action required:</b> These items are just for your information. You don't need to take any action on them but they might be useful to know.
 Bootstrapjs Identified	<b>No action required:</b> These items are just for your information. You don't need to take any action on them but they might be useful to know.
 BootstrapTable Identified	<b>No action required:</b> These items are just for your information. You don't need to take any action on them but they might be useful to know.
 Cdnjs Identified	<b>No action required:</b> These items are just for your information. You don't need to take any action on them but they might be useful to know.
 Email Address Disclosure	<b>No action required:</b> These items are just for your information. You don't need to take any action on them but they might be useful to know.

Vulnerability	Suggested Action
 Forbidden Resource	<b>No action required:</b> These items are just for your information. You don't need to take any action on them but they might be useful to know.
 IIS Identified	<b>No action required:</b> These items are just for your information. You don't need to take any action on them but they might be useful to know.
 jQuery Identified	<b>No action required:</b> These items are just for your information. You don't need to take any action on them but they might be useful to know.
 Lodash Identified	<b>No action required:</b> These items are just for your information. You don't need to take any action on them but they might be useful to know.
 OPTIONS Method Enabled	<b>No action required:</b> These items are just for your information. You don't need to take any action on them but they might be useful to know.
 Out-of-date Version (Bootstrap)	<b>No action required:</b> These items are just for your information. You don't need to take any action on them but they might be useful to know.
 Popper.js Identified	<b>No action required:</b> These items are just for your information. You don't need to take any action on them but they might be useful to know.

# Impacts

Severity	Impact
 High	<b>An attacker could access user information sent over the internet or public Wi-Fi or a similar environment</b> This might include passwords, usernames, and the content of web pages viewed.
 High	<b>The software that powers your website is out of date - your version is known to contain vulnerabilities</b>
 Medium	<b>Depending on the website's feature an attacker can access users' data or worse</b> This may enable them take control of website, see confidential data but it all depends on the website and what's supported. Therefore these issues need to be investigated further manually to understand the real impact.
 Low	<b>An attacker could view information about your system that helps them find or exploit vulnerabilities</b> This may enable them to take control of your website and access sensitive user and admin information. These issues mostly indicates the lack of the security best practice implementation.
 Low	<b>An attacker could access information that helps them to exploit other vulnerabilities</b> This information gives them a better understanding of your system.
 Low	<b>People using a web browser after one of your users could see sensitive information that has been entered into your site</b> For example, username, password, credit card details. This is possible because browser autocomplete is not disabled.

# Compliance Summary

Compliance	Vulnerabilities
PCI DSS v3.2	10
OWASP 2013	23
OWASP 2017	31
OWASP API Top Ten 2019	20
OWASP Top Ten 2021	29
WASC	31
HIPAA	16
ISO27001	37
ASVS 4.0	34
NIST SP 800-53	36
DISA STIG	36
ISO27001 2022	35

**PCI compliance data is generated based on the classifications and it has no validity. PCI DSS scans must be performed by an approved scanning vendor.**

This report created with 23.8.0.41720-release\_is-23.8.0-a9dc73c

<https://www.invicti.com>

SFA Technologies