invicti

10-10-2025 15:32:17 (UTC+05:30)

Executive Summary 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

Your website is very insecure!

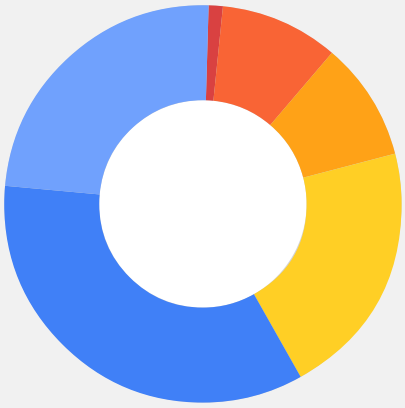
Critical vulnerabilities were identified on your website. You need to act now to address these problems otherwise your application will likely get hacked and possibly attackers will be able to steal data. These issues need to be addressed urgently.

What's the Worst that could Happen?

An attacker could access and control logged in user or admin accounts if attack succeeds

An attacker can abuse a vulnerability on the website to attack individual users of the website. If this attack succeeds, the attacker can hijack their session. This would enable them to take any action that those users can take and to steal their information. For example, an admin might have complete access to the database and the ability to change the website.

Vulnerabilities



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

Vulnerability	Suggested Action
Out-of-date Version (Tomcat)	**Fix immediately:** With these vulnerabilities your website could be hacked right now. You should make it your highest priority to fix them immediately. Once you've done this, you should rescan to make sure you've eliminated them.
Cross-site Scripting	**Fix immediately:** An attacker could use these vulnerabilities to hack your website. You should fix them immediately. Once you've done this, you should rescan to make sure you've eliminated them.
Insecure Transportation Security Protocol Supported (TLS 1.0)	**Fix immediately:** An attacker could use these vulnerabilities to hack your website. You should fix them immediately. Once you've done this, you should rescan to make sure you've eliminated them.
Password Transmitted over HTTP	**Fix immediately:** An attacker could use these vulnerabilities to hack your website. You should fix them immediately. Once you've done this, you should rescan to make sure you've eliminated them.
Frame Injection	**Fix soon:** You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
HTTP Strict Transport Security (HSTS) Policy Not Enabled	**Fix soon:** You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
Open Redirection	**Fix soon:** You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
SSL Certificate Name Hostname Mismatch	**Fix soon:** You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
Stack Trace Disclosure (Java)	**Fix soon:** You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
Weak Ciphers Enabled	**Fix soon:** You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
[Possible] SQL Injection	**Consider fixing after confirmed:** These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
Database Error Message Disclosure	**Consider fixing:** These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
Internal Server Error	**Consider fixing:** These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
Missing X-Content-Type-Options Header	**Consider fixing:** These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
Version Disclosure (Apache Coyote)	**Consider fixing:** These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.

Vulnerability	Suggested Action
Version Disclosure (SwaggerUI)	**Consider fixing:** These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
Version Disclosure (Tomcat)	**Consider fixing:** These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
Content Security Policy (CSP) Not Implemented	**No action required:** 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)	**No action required:** 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	**No action required:** 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.
SameSite Cookie Not Implemented	**No action required:** 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	**No action required:** 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.
[Possible] Cross-site Scripting	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
[Possible] Internal Path Disclosure (Windows)	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
[Possible] Login Page Identified	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Apache Coyote Identified	**No action required:** 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)	**No action required:** 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	**No action required:** 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	**No action required:** 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 (Swagger UI)	**No action required:** 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
SwaggerUI Identified	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Tomcat Identified	**No action required:** 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
Critical	**An attacker could access and control logged in user or admin accounts if attack succeeds** An attacker can abuse a vulnerability on the website to attack individual users of the website. If this attack succeeds, the attacker can hijack their session. This would enable them to take any action that those users can take and to steal their information. For example, an admin might have complete access to the database and the ability to change the website.
Critical	**An attacker could access your database** This would allow them to acquire user and admin information and make changes (e.g. delete all user accounts).
High	**The software that powers your website is out of date - your version is known to contain vulnerabilities**
High	**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.
Medium	**An attacker could use your website to trick your users into providing them with sensitive information** This could include usernames, passwords and credit card details. This could be done by redirecting users from your site to separate web pages that look like your site.
Medium	**An attacker could access users' data without having the credentials** This may let them view sensitive information. This attack requires attacker to target individual users.
Low	**An attacker could view information about your system that helps them find or exploit vulnerabilities** 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	**An attacker could access information that helps them to exploit other vulnerabilities** This information gives them a better understanding of your system.
Low	**People using a web browser after one of your users could see sensitive information that has been entered into your site** For example, username, password, credit card details. This is possible because browser autocomplete is not disabled.

Compliance Summary

Compliance	Vulnerabilities
PCI DSS v3.2	21
OWASP 2013	51
OWASP 2017	54
OWASP API Top Ten 2019	21
OWASP Top Ten 2021	43
OWASP API Top 10 2023	28
WASC	67
HIPAA	22
ISO27001	81
ASVS 4.0	80
NIST SP 800-53	82
DISA STIG	82
ISO27001 2022	114

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.