



04-06-2025 13:10:45 (UTC-08:00)

Detailed Scan Report

<https://ggihaldia.com/>

Scan Time	: 04-06-2025 11:22:29 (UTC-08:00)
Scan Duration	: 00:01:48:01
Total Requests	: 26,828
Average Speed	: 4.1 r/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.

Vulnerabilities



Critical	0
High	0
Medium	4
Low	11
Best Practice	4
Information	10
TOTAL	29

Vulnerability	Suggested Action
 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.
 Out-of-date Version (jQuery Migrate)	Fix soon: You should fix them soon.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 Out-of-date Version (jQuery)	Fix soon: You should fix them soon.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] Cross-site Request Forgery	Consider fixing after confirmed: 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	Consider fixing after confirmed: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Autocomplete is Enabled	Consider fixing: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Insecure Frame (External)	Consider fixing: 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)	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-Frame-Options Header	Consider fixing: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Programming Error Message	Consider fixing: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Stack Trace Disclosure (ASP.NET)	Consider fixing: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Version Disclosure (ASP.NET)	Consider fixing: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 ViewState is not Encrypted	Consider fixing: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.

Vulnerability	Suggested Action
 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.
 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] 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.
 ASP.NET 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.
 Forbidden Resource	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.
 Generic 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 (Modernizr)	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.
 Sitemap Detected	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.
 Version Disclosure (IIS)	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.

Compliance Summary

Compliance	Vulnerabilities
PCI DSS v3.2	10
OWASP 2013	18
OWASP 2017	20
HIPAA	13
ISO27001	29

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 5.8.2.28358-master-3d7991d
<https://www.netsparker.com>