



5/18/2023 2:52:23 PM (UTC+07:00)

Detailed Scan Report

<https://uigradients.com/>

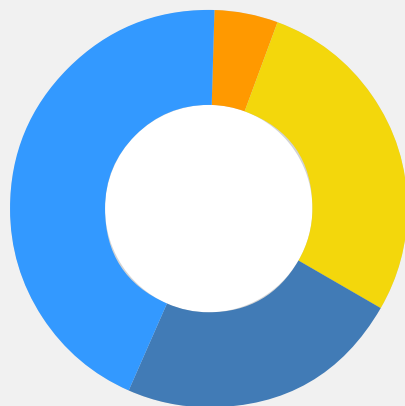
Scan Time	: 5/17/2023 7:27:17 PM (UTC+07:00)
Scan Duration	: 00:00:03:46
Total Requests	: 982
Average Speed	: 4.3 r/s

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	2
Low	11
Best Practice	9
Information	17
TOTAL	39

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.
 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.
 Cookie Not Marked as HttpOnly	Consider fixing: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Cookie Not Marked as Secure	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.
 Misconfigured Access-Control-Allow-Origin Header	Consider fixing after confirmed: 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.
 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.
 Expect-CT Not Enabled	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.
 Missing X-XSS-Protection Header	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.
 An Unsafe Content Security Policy (CSP) Directive in Use	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
 data: Used in a Content Security Policy (CSP) Directive	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.
 default-src Used in Content Security Policy (CSP)	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.
 Disabled X-XSS-Protection Header	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.
 Missing object-src in CSP Declaration	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 (Vue.js)	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	5
OWASP 2013	16
OWASP 2017	16
HIPAA	7
ISO27001	39

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 5.8.1.28119-master-bca4e4e
<https://www.netsparker.com>