netsparker

10/18/2020 8:18:51 AM (UTC+05:30)

Detailed Scan Report

https://www.myndr.nl/

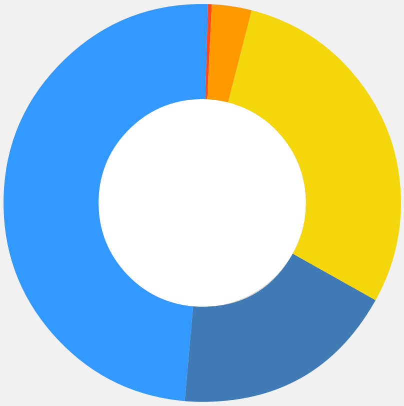
Scan Time	: 10/17/2020 1:08:00 AM (UTC+05:30)
Scan Duration	: 01:05:29:44
Total Requests	: 815,243
Average Speed	: 7.7r/s

Risk Level:
HIGH

Your website is insecure!

Some very serious vulnerabilities were identified on your website. You should address them as soon as possible.

Vulnerabilities



🟥	Critical	0
🟧	High	1
🟧	Medium	10
🟨	Low	91
🟦	Best Practice	56
🟦	Information	150
	TOTAL	**308**

Vulnerability	Suggested Action
Session Cookie Not Marked as Secure	**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.
HTTP Strict Transport Security (HSTS) Errors and Warnings	**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Out-of-date Version (jQuery)	**Fix soon:** You should fix them soon.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] Internal IP Address Disclosure	**Consider fixing after confirmed:** These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
[Possible] Phishing by Navigating Browser Tabs	**Consider fixing after confirmed:** These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
Apache MultiViews Enabled	**Consider fixing:** These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
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 Frame (External)	**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.
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.

Vulnerability	Suggested Action
💡 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.
💡 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.
💡 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.
ℹ [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.
ℹ 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.
ℹ Apache Web Server 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.
ℹ Cross-site Referrer Leakage through Referrer-Policy	**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.
ℹ 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.
ℹ 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.
ℹ 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.
ℹ 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.
ℹ 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.

Vulnerability	Suggested Action
ℹ 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.
ℹ Multiple Content Security Policy (CSP) Implementation 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.
ℹ 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.
ℹ Out-of-date Version (Bootstrap)	**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.
ℹ Robots.txt 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.
ℹ 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.
ℹ Unknown Option Used In Referrer-Policy	**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.
ℹ Wildcard Detected in Domain Portion of 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.
ℹ WordPress 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.

Compliance Summary

Compliance	Vulnerabilities
PCI DSS v3.2	46
OWASP 2013	133
OWASP 2017	144
HIPAA	55
ISO27001	308

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