netsparker

6/4/2023 12:42:50 AM (UTC+05:30)

Detailed Scan Report

http://localhost/votesystem/admin/home.php

Scan Time	: 6/3/2023 5:57:14 PM (UTC+05:30)
Scan Duration	: 00:06:10:41
Total Requests	: 212,040
Average Speed	: 9.5r/s

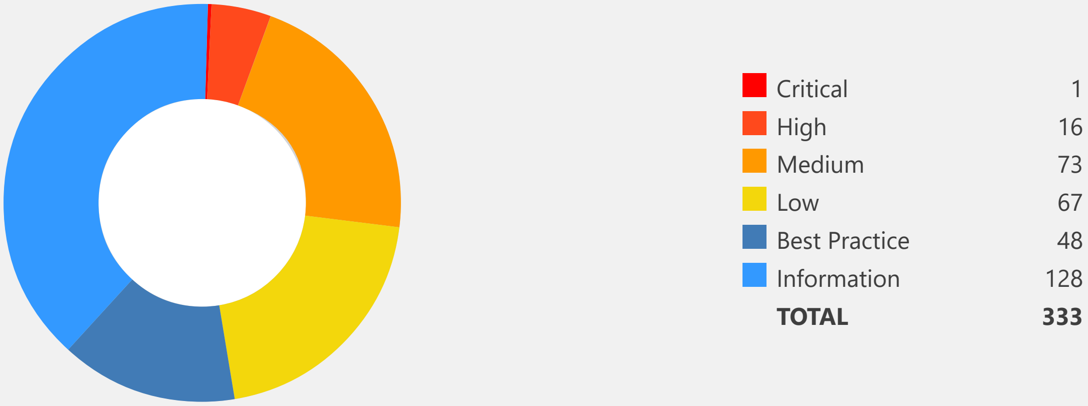
Risk Level:

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.

Vulnerabilities



🟥	Critical	1
🟥	High	16
🟧	Medium	73
🟨	Low	67
🟦	Best Practice	48
🟦	Information	128
	TOTAL	**333**

Vulnerability	Suggested Action
❗ SQL Injection	**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.
🚩 Certificate is Signed Using a Weak Signature Algorithm	**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.
🚩 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.
🚩 Database User Has Admin Privileges	**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.
🚩 Out-of-date Version (Moment.js)	**Fix immediately:** An attacker could use these vulnerabilities to hack your website.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.
⚑ [Possible] Cross-site Scripting	**Confirmed soon:** You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
⚑ [Possible] Source Code Disclosure (Generic)	**Confirmed 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.
⚑ Invalid SSL Certificate	**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.
⚑ Out-of-date Version (jQuery UI Autocomplete)	**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 UI Dialog)	**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 UI Tooltip)	**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.

Vulnerability	Suggested Action
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.
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.
Database Error Message Disclosure	**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.
Missing Content-Type Header	**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.
Open Redirection in POST method	**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.
TRACE/TRACK Method Detected	**Consider fixing:** These vulnerabilities aren’t very bad but they might help an attacker. You should think about fixing them.
Version Disclosure (Apache)	**Consider fixing:** These vulnerabilities aren’t very bad but they might help an attacker. You should think about fixing them.
Version Disclosure (OpenSSL)	**Consider fixing:** These vulnerabilities aren’t very bad but they might help an attacker. You should think about fixing them.
Version Disclosure (PHP)	**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.
💡 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.
💡 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] Administration Page 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 [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 [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.
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 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.
ℹ Database Detected (MySQL)	**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 Directory Listing (Apache)	**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 File Upload Functionality 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.

Vulnerability	Suggested Action
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 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 (Apache)	**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 (PHP)	**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 Unexpected Redirect Response Body (Too Large)	**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	170
OWASP 2013	240
OWASP 2017	238
HIPAA	191
ISO27001	322

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