netsparker

13-01-2024 11:25:50 AM (UTC+05:30)

# Detailed Scan Report

http://testasp.vulnweb.com/

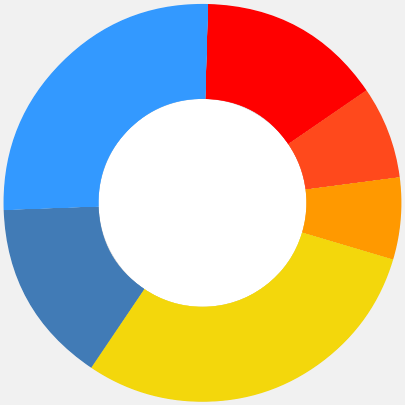
| | |
|---|---|
| **Scan Time** | : 12-01-2024 06:44:50 PM (UTC+05:30) |
| **Scan Duration** | : 00:01:11:47 |
| **Total Requests** | : 14,359 |
| **Average Speed** | : 3.3r/s |

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 | 4 |
| 🟥 | High | 2 |
| 🟧 | Medium | 2 |
| 🟨 | Low | 8 |
| 🟦 | Best Practice | 4 |
| 🟦 | Information | 7 |
| | **TOTAL** | **27** |

| Vulnerability | Suggested Action |
|---|---|
| Boolean Based 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. |
| Local File Inclusion | **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. |
| Out-of-date Version (IIS) | **Fix soon:** You should fix them soon. Once you've done this, you may want to rescan to check they're gone. |
| SSL/TLS Not Implemented | **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. |
| 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. |
| 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. |
| 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. |
| Version Disclosure (ASP.NET) | **Consider fixing:** These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them. |
| Windows Short Filename | **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. |
| 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. |

| Vulnerability | Suggested Action |
|---|---|
| 💡 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. |
| 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 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. |
| 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 (Microsoft SQL Server) | **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 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 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 | 11 |
| OWASP 2013 | 19 |
| OWASP 2017 | 19 |
| HIPAA | 13 |
| ISO27001 | 26 |

**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