



12-09-2021 05:33:54 (UTC+05:30)

Detailed Scan Report

<http://zero.webappsecurity.com/>

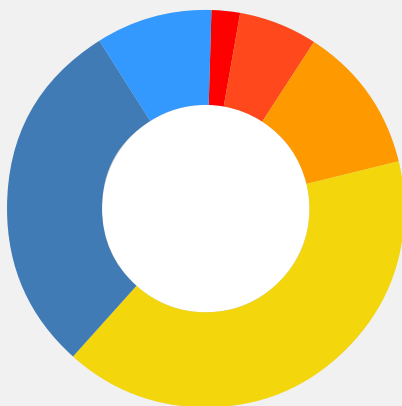
Scan Time	: 12-09-2021 05:01:06 (UTC+05:30)
Scan Duration	: 00:00:32:43
Total Requests	: 17,813
Average Speed	: 9.1r/s

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	3
High	8
Medium	15
Low	52
Best Practice	37
Information	12
TOTAL	127

Vulnerability	Suggested Action
 Out-of-date Version (Apache)	Fix immediately: With these vulnerabilities your website could be hacked right now.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.
 Out-of-date Version (OpenSSL)	Fix immediately: With these vulnerabilities your website could be hacked right now.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.
 Out-of-date Version (Tomcat)	Fix immediately: With these vulnerabilities your website could be hacked right now.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.
 [Possible] Server-Side Request Forgery (Apache Server Status)	Confirm 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.
 [Probable] Local File Inclusion	Confirm 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.
 Cross-site Scripting via Remote 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.
 Insecure Transportation Security Protocol Supported (SSLv2)	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.
 Apache Server-Status Detected	Fix soon: You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
 Frame Injection	Fix 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.
 Insecure Transportation Security Protocol Supported (SSLv3)	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.

Vulnerability	Suggested Action
 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] Backup File Disclosure	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	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.
 [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.
 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.
 Version Disclosure (Apache Coyote)	Consider fixing: These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
 Version Disclosure (Apache Module)	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 (mod_ssl)	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 (Tomcat)	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.
 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.
 [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.
 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.
 Default Page Detected (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.
 Default Page Detected (Tomcat)	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.
 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.

Compliance Summary

Compliance	Vulnerabilities
PCI DSS v3.2	38
OWASP 2013	92
OWASP 2017	92
HIPAA	51
ISO27001	126

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>