Security Report for Brandname.com

Alerts and Notifications

Status	Group	Scan Name	Scan Details	Actions
Alert	Patch	APSB23-17	APSB23-17 security updates available for Adobe Commerce and Magento Open Source Affected versions: 2.4.4-p2 and earlier, 2.4.5-p1 and earlier. For more information please visit the Security Release page.	Apply the Security Update immediately. Please ignore this notification if you have already applied the patch.

Failed Scans

Status	Group	Scan Name	Scan Details	Actions
Fail	Compromise	Compromise Injection	Your site contains scripts with similar behavior to typical malware code (159). Suspected malicious code detected in these resources: https://brandname.com/ pub/static/version1666893249/ frontend/RV/ en_US/jquery.min.js Please ensure all scripts are legitimate. If you think this is a false positive - please let us know at: securityscan@magento.com.	Review your site for signs of compromise and apply Security Best Practices.

Fail	Vulnerability	Base /pub/	Your Web server is configured to run from %MAGENTO_ROOT% directory. It is recommended to set %MAGENTO_ROOT%/pub as a Web server root directory.	Follow Security Best Practices.
Fail	Patch	XS Vulnerability	XS Vulnerability - Failed.XSS Patch not detected (APPSEC-2143).	Apply the Magento 2.2.7/2.1.16 Security Update immediately. Review your site for signs of compromise. Find more information about Security Best Practices.
Fail	Vulnerability	SSL TLS	Your server supports TLSv1.0. Please update your configuration to discontinue TLSv1.0 support.	

Unidentified Results

Status	Group	Scan Name	Scan Details	Actions
Unknown	Vulnerability	Cloud-Specific Security Check	[INFO]: Applicable to Adobe Cloud 'Production' instance only.	

Unknown	Other	Two factor authentication	Can't determine if your server uses 2FA.	Follow Security Best Practices.
Unknown	Vulnerability	Brute Force	We were unable to perform one or more Brute Force checks. This may expose your installation to Brute Force attacks.Error occurred while checking URL(s): /catalog/Adminhtml_category /catalog/AdminHtml_category /catalog/AdminHtml_CategorY /cms/Adminhtml_block /cms/Adminhtml_block/index /cms/Adminhtml_Block/Index /cms/Adminhtml_block/edit /cms/Adminhtml_bloCk/ediT /cms/Adminhtml_page /cms/Adminhtml_pAge /customer/Adminhtml_inDex Check that access to this URL(s) is restricted at the web server configuration level.	Review your site for signs of compromise. Protect your Admin panel and other access points against password guessing and apply Security Best Practices.

Security Report for Brandname.com

Successful Scans

Status	Group	Scan Name	Scan Details
Pass	Compromise	BotNet Suspect	Your domain has not been noticed in BotNet activities.
Pass	Vulnerability	Cloud-Specific Security Check	[INFO]: Applicable to Adobe Cloud 'Production' instance only.
Pass	Patch	Abuse Protection	Abuse Protection - Passed. (1)
Pass	Vulnerability	Information Leakage	Information Leakage - Passed. (3)
Pass	Patch	JS Libraries	Outdated JS Libraries - Passed. (2)
Pass	Vulnerability	RCE Vulnerability	No known RCE Vulnerability found (404)
Pass	Vulnerability	Unprotected XML	Your installation's configuration files are protected.
Pass	Vulnerability	Vulnerable Extensions	Vulnerable Extensions - Not found
Pass	Vulnerability	SSL Basic	Your server uses a valid SSL certificate and SSL chain certificate.
Pass	Vulnerability	SSL Frontend	All secure URL checks passed. Your installation uses SSL for secure URLs.
Pass	Vulnerability	Full Time SSL	Your installation appears to redirect all unsecured traffic to HTTPS.
Pass	Compromise	Visbot Malware	Malware was not detected on your installation.