

Site security audit report for www.jasarat.com

July 16, 2024 at 8:56 PM UTC

Summary



Issues found
on your
website :(

13

Infected
files

-

Infected fields in
database

42

Active Vulnerabilities

This is a summary website scan report - the result of multilayer scan for website malware and vulnerabilities.

Reactive scan result and the website health status: Security issues

Website Antivirus

Antivirus scan all website files (not just CMS' files), themes, plugins, PHP, JS, HTML, images, files with no type, any binary files and system files, .htaccess, and files with custom types and archives and website database for malware, malicious redirects, Trojans, backdoors, shell scripts, malicious codes, bad URLs and SEO spam, defaces, code injections, browser coin miners and for known security vulnerabilities.

File scan result:

● 13 infected files

● File: **wp-class.php**

Infections: Eval.b64.235

Path: /disablepersonaward/wp-content/plugins/press

● File: **wp-init.php**

Infections: Trojan.Inject.473

Path: /

● File: **PIA-1-534x462.jpg**

Infections: Trojan.PHP.ImgFake

Path: /en_bk/wp-content/uploads/2016/10

● File: **main.php**

Infections: Eval.b64.27

Path: /en_bk/wp-content/themes/bk/twentytwentyone/inc

● File: **PIA-1-534x462.jpg**

Infections: Trojan.PHP.ImgFake

Path: /en/wp-content/uploads/2016/10

● File: **inc.php**

Infections: Trojan.Inject.473

Path: /hyderabad.jasarat.com

● File: **wp-init.php**

Infections: Trojan.Inject.473

Path: /new.jasarat.com

● File: **wp-include.php**

Infections: Trojan.Inject.473

Path: /sunday

● File: **wp-class.php**

Infections: Eval.b64.235

Path: /tv/wp-content/plugins/press

● File: **fusion-optimizer-pro.php**

Infections: WP.Inject.218

Path: /wp-content/plugins/fusion-optimizer-pro

● File: **online-324x235.jpg**

Path: /wp-content/uploads/2020/02

Infections: Trojan.PHP.ImgFake

● File: **pexels-photo-1598507-741x486.jpeg**

Path: /wp-content/uploads/2020/01

Infections: Trojan.PHP.ImgFake

● File: **Pic18-082_SubjectPHOTOS-75-TO-84_ID2322876_11-768x493.jpg**

Path: /wp-content/uploads/2019/02

Infections: Trojan.PHP.ImgFake

Database scan result:

● No data

Patch Manager

The security system detects not only viruses, but also website vulnerabilities. 100+ frameworks, 1000+ plug-ins, 10,000+ vulnerabilities. Works with popular CMSs like WordPress, Joomla, Drupal, DLE, PrestaShop and others. Thousands of vulnerable plug-ins and components are covered. Website vulnerabilities may have been cause of an infection or may further cause of an infection.

Vulnerabilities scan result:

● 42 vulnerabilities

● WP.FileManager.3.E.CVE

● WP.FileManager.4.E.CVE

● WP.Core.6.2.0.CVE

- WP.ComingSoon.2.E.CVE

- WP.YoastSEO.5.E.CVE

- WP.Core.5.8.2.CVE

- WP.FastestCache.CVE

- WP.Editor.CVE

- WP.FastestCache.5.E.CVE

- WP.Core.5.7.1.CVE

- WP.Core.5.5.2.CVE

- WP.Core.5.0.CVE

- WP.Core.6.2.0.CVE

- WP.Core.6.4.3.CVE

- WP.Core.6.5.5.CVE

- WP.Core.6.3.2.CVE

- WP.Core.6.5.2.CVE

- WP.Editor.CVE

- WP.YoastSEO.4.E.CVE

- WP.YoastSEO.5.E.CVE
- WP.ComingSoon.CVE
- WP.ComingSoon.2.E.CVE
- WP.PopupMaker.CVE
- WP.FileManager.4.E.CVE
- WP.FileManager.3.E.CVE
- WP.AllinOneSEOPack.5.E.CVE
- WP.PopupMaker.CVE
- WP.Jetpack.2.E.CVE
- WP.Jetpack.3.E.CVE
- WP.AllinOneSEOPack.4.CVE
- WP.AdvancedDatabaseCleaner.CVE
- WP.Core.5.4.2.CVE
- WP.Stringlocator.CVE
- WP.AdvancedDatabaseCleaner.CVE
- WP.WPCookieConsent.E.CVE

- WP.Smush.CVE

- WP.PostGrid.3.CVE

- WP.YoastSEO.3.CVE

- WP.YoastSEO.5.E.CVE

- WP.YoastSEO.4.E.CVE

- WP.Timber.E.CVE

- WP.YoastSEO.2.CVE

Website security report powered by Virusdie website security tools.