WP Malware Guard Security Report

Site: https://swadhinkhan.com
Generated: 2026-07-04 03:45:49
Plugin version: 0.4.0 | WordPress: 7.0
License: Active / Pro

Executive Snapshot

Total events: 167
Events in last 24 hours: 167
High and critical events: 82
Active blocked IPs: 1

Protection Settings

Firewall mode: monitor
Block threshold: 80
Rate limit enabled: Enabled
Rate limit requests: 120
Rate limit window: 60
Login fail limit: 5
Disable xmlrpc: Disabled
Restrict rest: Disabled
Hide wp version: Enabled
Login slug enabled: Disabled
Disable directory indexing: Disabled
Security headers enabled: Enabled
Scanner max files: 3500
Cloudflare enabled: Disabled
Siem enabled: Disabled

Hardening Status

Xmlrpc: Disabled
Rest: Disabled
Version hidden: Enabled
File edit disabled: Enabled
Custom login url:
Directory indexing: not managed
Security headers: Enabled
Author archives: enabled
Ssl admin: Enabled
Debug display: Enabled

Last File Integrity Scan

Scanned at: 2026-07-04 02:33:04
Files scanned: 3500
Findings: 684
Core checksum: Checked
[HIGH] Writable core file - wp-admin/css/colors/blue/colors-rtl.css

[HIGH] Writable core file - wp-admin/css/colors/blue/colors-rtl.min.css
[HIGH] Writable core file - wp-admin/css/colors/blue/colors.css
[HIGH] Writable core file - wp-admin/css/colors/blue/colors.min.css
[HIGH] Writable core file - wp-admin/css/colors/blue/colors.scss
[HIGH] Writable core file - wp-admin/css/colors/coffee/colors-rtl.css
[HIGH] Writable core file - wp-admin/css/colors/coffee/colors-rtl.min.css
[HIGH] Writable core file - wp-admin/css/colors/coffee/colors.css
[HIGH] Writable core file - wp-admin/css/colors/coffee/colors.min.css
[HIGH] Writable core file - wp-admin/css/colors/coffee/colors.scss
[HIGH] Writable core file - wp-admin/css/colors/ectoplasm/colors-rtl.css
[HIGH] Writable core file - wp-admin/css/colors/ectoplasm/colors-rtl.min.css

Correlated Sessions

41.220.201.54 | CRITICAL | events 27 | risk 2165 | last 2026-07-04 03:45:47
41.220.201.54 | CRITICAL | events 19 | risk 1535 | last 2026-07-04 03:44:30
41.220.201.54 | CRITICAL | events 3 | risk 285 | last 2026-07-04 03:44:41
103.78.226.130 | HIGH | events 12 | risk 260 | last 2026-07-04 02:32:26
103.78.226.130 | HIGH | events 11 | risk 255 | last 2026-07-04 03:18:55
41.220.201.54 | CRITICAL | events 2 | risk 190 | last 2026-07-04 03:45:24
41.220.201.54 | CRITICAL | events 2 | risk 190 | last 2026-07-04 03:34:21
41.220.201.54 | CRITICAL | events 2 | risk 190 | last 2026-07-04 03:32:55

Recent Security Events

2026-07-04 03:45:47 | CRITICAL | firewall | 41.220.201.54 | risk 95
Blocked request from 41.220.201.54.
post /xmlrpc.php
2026-07-04 03:45:24 | CRITICAL | firewall | 41.220.201.54 | risk 95
Blocked request from 41.220.201.54.
post /xmlrpc.php
2026-07-04 03:45:15 | CRITICAL | firewall | 41.220.201.54 | risk 95
Blocked request from 41.220.201.54.
post /xmlrpc.php
2026-07-04 03:45:06 | INFO | authentication | 103.78.226.130 | risk 10
Successful login for "wpmgdeploy1783115091" from 103.78.226.130.
post /wp-login.php
2026-07-04 03:45:06 | LOW | authentication | 103.78.226.130 | risk 10 | A07:2021 Identification and Authentication Failures, MITRE T1110
Suspicious request detected: WordPress login probing
post /wp-login.php
2026-07-04 03:44:51 | CRITICAL | firewall | 41.220.201.54 | risk 95
Blocked request from 41.220.201.54.
post /xmlrpc.php
2026-07-04 03:44:51 | LOW | enumeration | 103.78.226.130 | risk 20 | A01:2021 Broken Access Control, MITRE T1589
Suspicious request detected: WordPress user enumeration
post /wp-json/wp/v2/users
2026-07-04 03:44:41 | CRITICAL | firewall | 41.220.201.54 | risk 95

Blocked request from 41.220.201.54.
post /xmlrpc.php

2026-07-04 03:44:36 | LOW | enumeration | 103.78.226.130 | risk 20 | A01:2021 Broken Access Control, MITRE T1589

Suspicious request detected: WordPress user enumeration
delete /wp-json/wp/v2/users/50?force=true&reassign=1

2026-07-04 03:44:30 | CRITICAL | firewall | 41.220.201.54 | risk 95

Blocked request from 41.220.201.54.
post /xmlrpc.php

2026-07-04 03:44:28 | INFO | license | 103.78.226.130 | risk 10

Commercial license activated.
post /wp-admin/admin-post.php

2026-07-04 03:44:23 | CRITICAL | firewall | 41.220.201.54 | risk 95

Blocked request from 41.220.201.54.
post /xmlrpc.php

2026-07-04 03:44:18 | MEDIUM | authentication | 37.140.223.104 | risk 30

Failed login for "minibooksbd" from 37.140.223.104.
post /wp-login.php

2026-07-04 03:44:18 | INFO | authentication | 103.78.226.130 | risk 10

Successful login for "wpmgdeploy1783115042" from 103.78.226.130.
post /wp-login.php

2026-07-04 03:44:18 | MEDIUM | authentication | 193.36.225.86 | risk 40

Failed login for "admin" from 193.36.225.86.
post /wp-login.php

2026-07-04 03:44:18 | LOW | authentication | 37.140.223.104 | risk 10 | A07:2021 Identification and Authentication Failures, MITRE T1110

Suspicious request detected: WordPress login probing
post /wp-login.php

2026-07-04 03:44:18 | LOW | authentication | 193.36.225.86 | risk 10 | A07:2021 Identification and Authentication Failures, MITRE T1110

Suspicious request detected: WordPress login probing
post /wp-login.php

2026-07-04 03:44:18 | LOW | authentication | 103.78.226.130 | risk 10 | A07:2021 Identification and Authentication Failures, MITRE T1110

Suspicious request detected: WordPress login probing
post /wp-login.php

2026-07-04 03:44:18 | LOW | authentication | 103.78.226.130 | risk 10 | A07:2021 Identification and Authentication Failures, MITRE T1110

Suspicious request detected: WordPress login probing
get /wp-login.php

2026-07-04 03:44:03 | LOW | enumeration | 103.78.226.130 | risk 20 | A01:2021 Broken Access Control, MITRE T1589

Suspicious request detected: WordPress user enumeration
post /wp-json/wp/v2/users