



Using WordPress
Security Logs to
Secure Your Site



Adding WP Security Logs

You can use some of the [developer functions and filters](#) that WordPress provides to create a logging system, but the easiest way to start a security log is to install a [WordPress security plugin](#) like iThemes Security that will automatically keep track of site and user activity.

Once you've installed and activated the iThemes Security plugin, **enable the following features** in iThemes Security to get the most out of your security logs:



Local Brute Force Protection



Banned Users



Database Backups



File Change Detection



Malware Scan Scheduling **PRO**



User Logging **PRO**

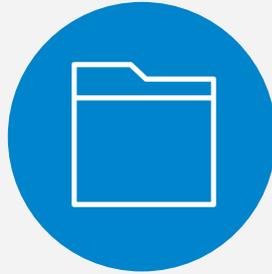


Version Management **PRO**

4 Important Events to Monitor in WordPress Security Logs



WordPress
Brute Force
Attacks



File
Changes



Malware
Scans



User
Activity

1. WordPress Brute Force Attacks

The screenshot shows the iThemes Security dashboard in a WordPress environment. The top navigation bar includes 'Moore Introspection', 'New', 'Security', and 'Maintenance Mode'. The dashboard header features 'iThemes Security' with links for 'Manage Settings' and 'Support'. A sidebar on the left contains various WordPress management options, with 'Security' highlighted in red. The main content area displays a table of security events, filtered to 'Brute Force' attacks. The table has columns for Module, Type, Description, Time, Host, User, and Details. The events listed are all 'Invalid Login' notices from the host 85.93.20.246. On the right, there are three informational panels: 'Malware Scan' (powered by Sucuri SiteCheck), 'Active Lockouts' (none active), and 'Need Help Securing Your Site?' (with a 'Create a Support Ticket' button).

Moore Introspection 0 + New Security Maintenance Mode Login Alerts Clear Cache Howdy, mmooore Screen Options

iThemes Security [Manage Settings](#) [Support](#)

Important Events (41) | All Events (523) | Warnings (41) | Actions (37) | Notices (445)

Brute Force Filter 159 items 1 of 8

Module	Type	Description	Time	Host	User	Details
Brute Force	Notice	Banned Use of "admin" Username	2018-10-18 10:26:33 - 24 hours ago	216.185.36.46		View Details
Brute Force	Notice	Invalid Login	2018-10-13 16:19:02 - 6 days ago	85.93.20.246		View Details
Brute Force	Notice	Invalid Login	2018-10-13 15:06:03 - 6 days ago	85.93.20.246		View Details
Brute Force	Notice	Invalid Login	2018-10-13 13:53:43 - 6 days ago	85.93.20.246		View Details
Brute Force	Notice	Invalid Login	2018-10-13 12:41:13 - 6 days ago	85.93.20.246		View Details
Brute Force	Notice	Invalid Login	2018-10-13 08:55:36 - 6 days ago	85.93.20.246		View Details
Brute Force	Notice	Invalid Login	2018-10-13 08:20:54 - 6 days ago	85.93.20.246		View Details
Brute Force	Notice	Invalid Login	2018-10-13 07:22:52 - 6 days ago	85.93.20.246		View Details
Brute Force	Notice	Invalid Login	2018-10-13 05:43:34 - 6 days ago	85.93.20.246		View Details
Brute Force	Notice	Invalid Login	2018-10-13 04:33:06 - 6 days ago	85.93.20.246		View Details
Brute Force	Notice	Invalid Login	2018-10-13 02:50:30 - 6 days ago	85.93.20.246		View

Malware Scan

This malware scan is powered by [Sucuri SiteCheck](#). It checks for known malware, blacklisting status, website errors and out-of-date software. Although the Sucuri team does its best to provide thorough results, 100% accuracy is not realistic and is not guaranteed.

Results of previous malware scans can be found on the [logs page](#).

[Scan Homepage for Malware](#)

Active Lockouts

There are no active lockouts at this time.

Need Help Securing Your Site?

As an iThemes Security Pro customer, you can create a support ticket now. Our team of experts is ready to help.

[Create a Support Ticket](#)



1. WordPress Brute Force Attacks

Brute force attacks refer to the trial and error method used to discover usernames and passwords in order to hack into a website. WordPress doesn't track any user login activity, so there isn't anything built into WordPress to protect you from a brute force attack. It is up to you to monitor your login security to protect your WordPress site.

If you see that a single username or IP has consecutive multiple failed login attempts, the chances are you are under a brute force attacks.

Identifying when you are under a brute force attack is a great start, but there is still more work to be done. You can increase the WordPress login security by limiting the number of failed login attempts a single user or IP is allowed to have before they are blocked from making any more attempts.

2. File Changes

sync 0 + New Security Howdy, mmoore

Dashboard

Posts

Media

Pages

Comments

Appearance

Plugins

Users

Tools

Settings

Security

Settings

Security Check

Grade Report

Logs

Debug

Collapse menu

Important Events (14) | All Events (147) | Fatal Errors (3) | **Warnings (11)** | Actions (2) | Notices (131)

All Modules Filter 11 items

Module	Type	Description	Time	Host	User	Details
File Change	Warning	5 Added, 0 Removed, 0 Changed	2018-10-19 14:06:16 - 1 hour ago			View Details
File Change	Warning	144 Added, 0 Removed, 0 Changed	2018-10-09 13:48:39 - 1 week ago			View Details
File Change	Warning	0 Added, 1302 Removed, 0 Changed	2018-10-09 13:18:12 - 1 week ago			View Details
File Change	Warning	1 Added, 0 Removed, 0 Changed	2018-10-04 16:28:53 - 2 weeks ago			View Details
File Change	Warning	1 Added, 0 Removed, 0 Changed	2018-10-03 14:16:58 - 2 weeks ago			View Details
File Change	Warning	24 Added, 0 Removed, 22 Changed	2018-10-01 19:44:37 - 3 weeks ago		mmoore	View Details
File Change	Warning	103 Added, 0 Removed, 54 Changed	2018-10-01 15:45:40 - 3 weeks ago			View Details
File Change	Warning	127 Added, 0 Removed, 2 Changed	2018-09-28 15:18:52 - 3 weeks ago		mmoore	View Details
File Change	Warning	511 Added, 62 Removed, 207 Changed	2018-09-26 17:53:12 - 3 weeks ago			View Details
File Change	Warning	1 Added, 0 Removed, 0 Changed	2018-09-25 13:12:33 - 3 weeks ago			View Details
File Change	Warning	0 Added, 0 Removed, 32 Changed	2018-08-23 19:49:05 - 2 months ago			View Details

Module Type Description Time Host User Details

Malware Scan

This malware scan is powered by [Sucuri SiteCheck](#). It checks for known malware, blacklisting status, website errors and out-of-date software. Although the Sucuri team does its best to provide thorough results, 100% accuracy is not realistic and is not guaranteed.

Results of previous malware scans can be found on the [logs page](#).

[Scan Homepage for Malware](#)

Active Lockouts

There are no active lockouts at this time.

Complete Your Security Strategy With BackupBuddy



BackupBuddy is the complete backup, restore and migration solution for your WordPress site. Schedule automated backups, store your backups safely off-site and restore your site quickly & easily.

[Get BackupBuddy](#)

2. File Changes

There are several legitimate reasons you would see new file change activity in your logs, but if the changes made were unexpected, you should take the time to assure the changes were not malicious.

Comparing File Changes

WordPress provides [WP-CLI commands](#) to compare the file hashes of core and plugin files easily. For comparing WordPress core files use the [wp core verify-checksums command](#), and for plugins, you can use the [wp plugin verify-checksums command](#). There currently isn't a WP-CLI command to compare theme file hashes, [but it is on the roadmap](#).

Enable the Compare Files Online option in the iThemes Security Pro File Change settings to automatically compare .org and iThemes file hashes.

Compare file changes by comparing differences in a Text Editor.

3. Malware Scans

WordPress dashboard header: sync 0 + New Security Howdy, mmoore

Dashboard sidebar: Dashboard, Posts, Media, Pages, Comments, Appearance, Plugins, Users, Tools, Settings, **Security**, Settings, Security Check, Grade Report, Logs, Debug, Collapse menu

iThemes Security [Manage Settings](#) [Support](#) Screen Options

Important Events (14) | All Events (147) | Fatal Errors (3) | Warnings (11) | Actions (2) | Notices (131)

Malware Scan Filter 42 items

Module	Type	Description	Time	Host	User	Details
Malware Scan	Notice	Clean	2018-10-03 14:04:58 - 2 weeks ago	2607:3f00:1:6::2		View Details
Malware Scan	Notice	Clean	2018-10-02 15:17:11 - 2 weeks ago	2607:3f00:1:6::2		View Details
Malware Scan	Notice	Clean	2018-10-01 15:44:24 - 3 weeks ago	2607:3f00:1:6::2		View Details
Malware Scan	Notice	Clean	2018-09-28 15:01:17 - 3 weeks ago	69.167.144.233	mmoore	View Details
Malware Scan	Notice	Clean	2018-09-26 16:45:08 - 3 weeks ago	2607:3f00:1:6::2		View Details
Malware Scan	Notice	Clean	2018-09-26 12:24:12 - 3 weeks ago	2607:3f00:1:6::2		View Details
Malware Scan	Notice	Clean	2018-09-25 13:00:19 - 3 weeks ago	2607:3f00:1:6::2		View Details
Malware Scan	Notice	Clean	2018-09-24 20:45:53 - 4 weeks ago	69.167.144.233	mmoore	View Details
Malware Scan	Notice	Clean	2018-09-13 13:35:34 - 1 month ago	2607:3f00:1:6::2		View Details
Malware Scan	Notice	Clean	2018-09-12 15:06:27 - 1 month ago	2607:3f00:1:6::2		View Details
Malware Scan	Notice	Clean	2018-09-12 13:14:02 - 1 month ago	2607:3f00:1:6::2		View

Malware Scan

This malware scan is powered by [Sucuri SiteCheck](#). It checks for known malware, blacklisting status, website errors and out-of-date software. Although the Sucuri team does its best to provide thorough results, 100% accuracy is not realistic and is not guaranteed.

Results of previous malware scans can be found on the [logs page](#).

[Scan Homepage for Malware](#)

Active Lockouts

There are no active lockouts at this time.

Complete Your Security Strategy With BackupBuddy



BackupBuddy is the complete backup, restore and migration solution for your WordPress site. Schedule automated backups, store your backups safely off-

3. Malware Scans

Make sure you have enabled Malware Scan Scheduling in your iThemes Security Pro settings.

It is crucial to be alerted as quickly as possible of a breach to your site. The longer it takes for you to know about a hack the more damage it will do.

Not only should you run malware scans, you should also be recording the results of every malware scan in your WordPress security logs.

Not knowing the scans are failing could result in your site not being regularly scanned for malware.

4. User Activity

- Dashboard
- Posts
- Media
- Pages
- Comments
- Appearance
- Plugins
- Users
- Tools
- Settings
- BackupBuddy
- Gutenberg
- Security**
- Settings
 - Security Check
 - Grade Report
- Logs
 - Collapse menu

Important Events (48) | All Events (519) | Warnings (48) | Actions (37) | Notices (434)

User Logging 32 items << < 1 of 2 > >>

Module	Type	Description	Time	Host	User	Details
User Logging	Notice	mmoore Logged In	2018-10-22 08:59:54 - 14 mins ago	207.246.249.202	mmoore	View Details
User Logging	Notice	mmoore Logged In	2018-10-18 09:49:51 - 4 days ago	207.246.249.202	mmoore	View Details
User Logging	Notice	mmoore Logged In	2018-10-16 09:10:27 - 6 days ago	69.167.144.233	mmoore	View Details
User Logging	Notice	mmoore Logged In	2018-10-16 09:10:21 - 6 days ago	69.167.144.233	mmoore	View Details
User Logging	Notice	Activated iThemes Sync Plugin	2018-10-16 09:06:57 - 6 days ago	207.246.249.199	mmoore	View Details
User Logging	Notice	mmoore Logged In	2018-10-16 09:04:13 - 6 days ago	207.246.249.197	mmoore	View Details
User Logging	Notice	mmoore Logged Out	2018-10-16 09:04:07 - 6 days ago	207.246.249.199	mmoore	View Details
User Logging	Notice	mmoore Logged In	2018-10-16 09:03:34 - 6 days ago	207.246.249.202	mmoore	View Details

Malware Scan

This malware scan is powered by [Sucuri SiteCheck](#). It checks for known malware, blacklisting status, website errors and out-of-date software. Although the Sucuri team does its best to provide thorough results, 100% accuracy is not realistic and is not guaranteed.

Results of previous malware scans can be found on the [logs page](#).

[Scan Homepage for Malware](#)

Active Lockouts

There are no active lockouts at this time.

Need Help Securing Your Site?

As an iThemes Security Pro customer, you can create a support ticket now. Our team of experts is ready to help.

[Create a Support Ticket](#)

4. Type of User Activity to Record



1. Log In / Log Out



3. Adding & Removing Plugins



2. User Creation



4. Changes to Posts & Pages

As we can see, having the right information can help stop an attack, alert you of a breach, pinpoint the time of the breach, access the damage, and help you with cleanup. Use the checklist below to aid you in monitoring your WordPress security logs:



1. Brute Force Activity



2. File Changes



3. Malware Scans



4. User Logging

Download Events to Monitor Infographic.

<https://ithemes.com/wp-content/uploads/2018/10/WordPress-Security-Logs.png>

Check out WP Security Logs blog post.

<https://ithemes.com/2018/10/25/how-to-wordpress-security-logs/>

We have a YouTube channel!

<http://ithemes.com/youtube>