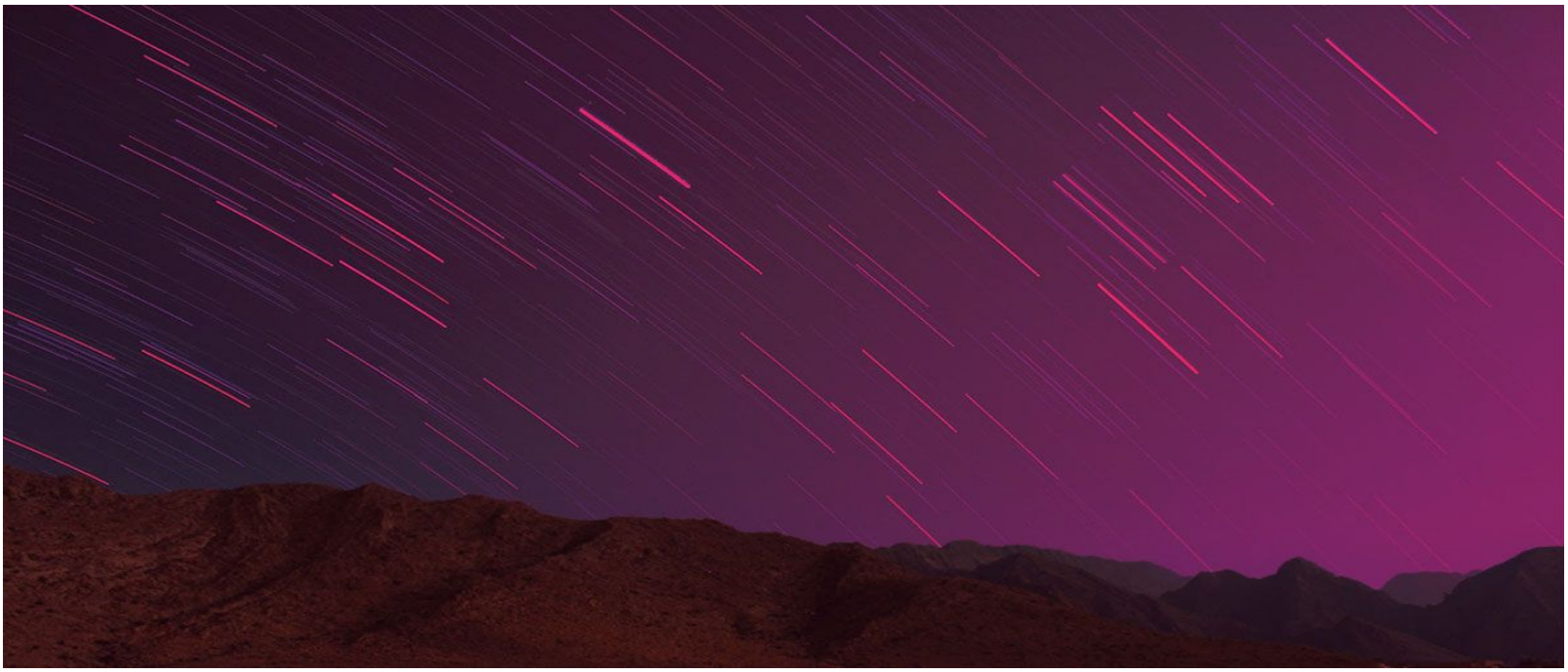
WordPress Security SecuPress Checklist

Secure Your WordPress Now!



The ultimate 32 items to improve the security

SecuPress

Part 1: Users

- [ ] 1. Ban login attempts on non-existing usernames
- [ ] 2. Set a non-login time slot
- [ ] 3. Avoid Double Logins
- [ ] 4. Reduce session window time
- [ ] 5. Set a password lifespan
- [ ] **6. Forbid usernames like admin, administrator, www, etc**
- [ ] **7. Use HTTPS all over your website to protect the data transfer**

Part 2: Plugins & Themes

- [ ] 8. Forbid .zip uploads
- [ ] 9. Be alerted when you're using a vulnerable plugin
- [ ] 10. Be alerted when you're using a vulnerable theme

Part 3: WordPress Core

- [ ] 11. Allow the automatic major updates
- [ ] 12. Disable the file editor
- [ ] 13. Disallow unfiltered HTML
- [ ] 14. Disallow unfiltered uploads
- [ ] 15. Disallow navigation in the /uploads folder
- [ ] 16. Hide login errors
- [ ] 17. Hide the WordPress and PHP version

Part 4: Sensitive Data

- [ ] 18. Prevent the hotlinking of for your content
- [ ] 19. Prevent access to readme/changelog files
- [ ] 20. Prevent bad url access
- [ ] 21. Prevent bad bot visiting your website
- [ ] 22. Prevent bad user agent to visit your site
- [ ] 23. Prevent bad method requests to be used on your site
- [ ] 24. Block bad url content
- [ ] 25. Protect your WordPress profile page

Part 5: Don't forget to...

- [ ] 26. Schedule a file monitor to detect malwares
- [ ] 27. Use SSH or SFTP to connect to your server

Part 6: Post Hack Aftermath

- [ ] 28. Know what to do after a hack
- [ ] 29. Learn how to react in front of a hack
- [ ] 30. Hire a professional to help you
- [ ] **31. Install a plugin able to protect your site by taking care of a maximum of items from this security list**
- [ ] 32. Learn from previous mistakes and reinforce your WordPress

TRY SECUPRESS NOW