



# WordPress Security for Beginners



Simple tips to secure your WP  
websites



# Did you know...

---

- On average, there are 30,000 new websites are hacked every day. (Source: Forbes)
- The most common way websites get hacked is by automated tools.
- The average time to identify a breach in 2020 was 228 days.
- Online threats have increased by as much as 6 times their usual levels during the COVID-19 pandemic. (Source: Info Security Magazine)

# What we will cover today

---

- Why websites get hacked?
- How they get hacked?
- Secure them with simple techniques

# Hi! I'm Vannkorn

---

I am a freelance Web Developer. I've been using WordPress for almost 10 years.

I've built website projects with passions and love from e-commerce, company profiles, news agencies, NGOs to Database Management System using WordPress.

[www.vannkorn.com](http://www.vannkorn.com)  
[vannkorn@gmail.com](mailto:vannkorn@gmail.com)



# Why website get hacked?

---

- Fun
- Traffic
- Competition
- Data
- To use as a staging point for watering hole attacks.

# How websites get hacked?

---

- Access control
- Software vulnerabilities
- Third-party integrations

# Tips to Secure them

---

# 1. Secure Ecosystems

---





# 1. Secure Ecosystems

---

- Avoid using default credentials.  
`root, admin, user, password, ...`
- Use strong password
- Enforce multi-factor authentication (MFA)



## 2. Plugins & Themes

- Use only from the official WordPress website or some trusted market places
- Always update & Remove unused



### Contact Form 7

Just another contact form plugin. Simple but flexible.

By *Takayuki Miyoshi*

★★★★☆ (1,953)

5+ Million Active Installations

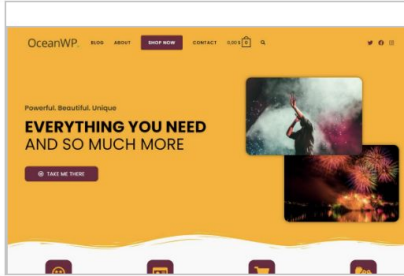
Last Updated: 3 weeks ago

✓ **Compatible** with your version of WordPress

[More Details](#)  
[Active](#)

### OceanWP

By oceanwp

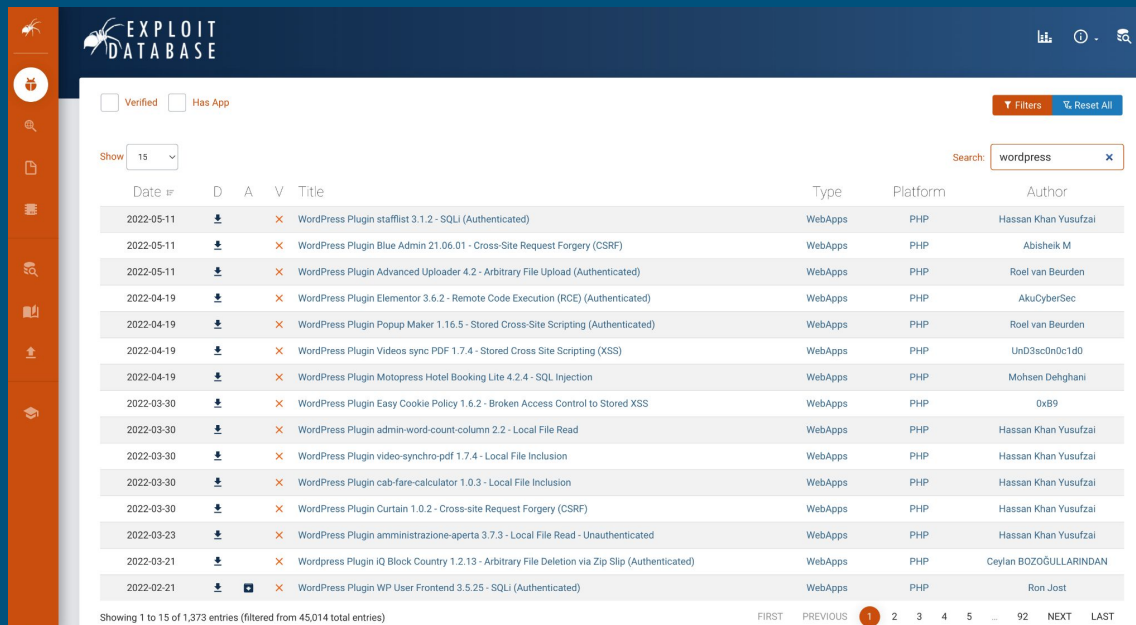


★★★★★ (5,254 ratings)

Version: 3.3.2

## 2. Plugins & Themes

- Not available on Exploit Database (<https://www.exploit-db.com/>)



The screenshot shows the Exploit Database interface. The search bar contains 'wordpress'. The table lists 15 entries, each with a date, a download icon, a verified status (orange X), a title, a type, a platform, and an author. The entries are sorted by date, with the most recent at the top. The table is filtered to show 15 of 1,373 entries.

Date	#	D	A	V	Title	Type	Platform	Author
2022-05-11				×	WordPress Plugin stafflist 3.1.2 - SQLi (Authenticated)	WebApps	PHP	Hassan Khan Yusufzai
2022-05-11				×	WordPress Plugin Blue Admin 21.06.01 - Cross-Site Request Forgery (CSRF)	WebApps	PHP	Abisheik M
2022-05-11				×	WordPress Plugin Advanced Uploader 4.2 - Arbitrary File Upload (Authenticated)	WebApps	PHP	Roel van Beurden
2022-04-19				×	WordPress Plugin Elementor 3.6.2 - Remote Code Execution (RCE) (Authenticated)	WebApps	PHP	AkuCyberSec
2022-04-19				×	WordPress Plugin Popup Maker 1.16.5 - Stored Cross-Site Scripting (Authenticated)	WebApps	PHP	Roel van Beurden
2022-04-19				×	WordPress Plugin Videos sync PDF 1.7.4 - Stored Cross Site Scripting (XSS)	WebApps	PHP	UnD3ac0n0c1d0
2022-04-19				×	WordPress Plugin Motopress Hotel Booking Lite 4.2.4 - SQL Injection	WebApps	PHP	Mohsen Dehghani
2022-03-30				×	WordPress Plugin Easy Cookie Policy 1.6.2 - Broken Access Control to Stored XSS	WebApps	PHP	0xb9
2022-03-30				×	WordPress Plugin admin-word-count-column 2.2 - Local File Read	WebApps	PHP	Hassan Khan Yusufzai
2022-03-30				×	WordPress Plugin video-synchro-pdf 1.7.4 - Local File Inclusion	WebApps	PHP	Hassan Khan Yusufzai
2022-03-30				×	WordPress Plugin cab-fare-calculator 1.0.3 - Local File Inclusion	WebApps	PHP	Hassan Khan Yusufzai
2022-03-30				×	WordPress Plugin Curtain 1.0.2 - Cross-site Request Forgery (CSRF)	WebApps	PHP	Hassan Khan Yusufzai
2022-03-23				×	WordPress Plugin amministrazione-aperta 3.7.3 - Local File Read - Unauthenticated	WebApps	PHP	Hassan Khan Yusufzai
2022-03-21				×	WordPress Plugin IQ Block Country 1.2.13 - Arbitrary File Deletion via Zip Slip (Authenticated)	WebApps	PHP	Ceylan BOZOĞULLARINDAN
2022-02-21				×	WordPress Plugin WP User Frontend 3.5.25 - SQLi (Authenticated)	WebApps	PHP	Ron Jost

Showing 1 to 15 of 1,373 entries (filtered from 45,014 total entries)

FIRST PREVIOUS 1 2 3 4 5 ... 92 NEXT LAST

# 3. Prevent From Brute Force Attack



## Limit Login Attempts Reloaded

[Install Now](#)[More Details](#)

Block excessive login attempts and protect your site against brute force attacks. Simple, yet powerful tools to improve site performance.

By *Limit Login Attempts Reloaded*



2+ Million Active Installations

Last Updated: 2 weeks ago

✓ **Compatible** with your version of WordPress



## Two Factor Authentication (2FA , MFA, OTP SMS and Email)

[Install Now](#)[More Details](#)

multi factor authentication  
- Two Factor (2FA/OTP) Two Factor Authentication (2 Factor/2FA/Two factor/TFA) supports many Two...

By *miniOrange*



800+ Active Installations

Last Updated: 3 weeks ago

✓ **Compatible** with your version of WordPress

# 4. Disable user registration if not necessary

General Settings

Site Title

Tagline   
In a few words, explain what this site is about.


WordPress Address (URL)

Site Address (URL)

Administration Email Address   
This address is used for admin purposes. If you change this, an email will be sent to your new address to confirm it. The new address will not become active until confirmed.

Membership ☐ Anyone can register

New User Default Role

Site Language 

Timezone   
Choose either a city in the same timezone as you or a UTC (Coordinated Universal Time) time offset.  
Universal time is 2022-06-10 02:34:28 . Local time is 2022-06-10 09:34:28 .




Date Format ☒ June 10, 2022 ☐ 2022-06-10 ☐ 06/10/2022 ☐ 10/06/2022

# 5. Always clean up spam comments

## Comments

All (26) | Mine (1) | Pending (0) | Approved (26) | **Spam (268)** | Trash (0)

Bulk actions ▼ Apply All comment types ▼ Filter Empty Spam

<input type="checkbox"/>	Author	Comment
<input type="checkbox"/>	 <b>DavidKab</b> профиль%20дорс x kuzneczovmaksim@rambler.ru 79.139.164.128	<a href="https://www.profildoors-doors.ru/">профиль дорс</a> https://www.profildoors-doors.ru/
<input type="checkbox"/>	 <b>AlbertKap</b> albi@my-mail.site 89.22.233.6	Обязательно попробуйте [url=https://3d-pechat-perm.ru/]печать на 3д принтере в Перми[url] – приятная цена, быстро и качественно! [url=http://www.google.im/url?q=http://3d-pechat-perm.ru]http://maps.google.td/url?q=http://3d-pechat-perm.ru[url]
<input type="checkbox"/>	 <b>JamesEvoky</b> galeria-zdjec.com x seesugeme197874@rambler.ru 216.131.114.199	[url=https://galeria-zdjec.com/smierc-i-miser-hieronim-bosch/]Portret Henryka VIII – Hansa Holbeina[url] – Dante i Virgil w piekle – Adolph Bouguero, Boze Narodzenie – Petrus Christus

# 6. Backup

- Backup both your data and system-configuration automatically
- Keep the backup in the safe place
- Test disaster recovery



**UpdraftPlus**  
WordPress  
Backup Plugin

Backup and restoration made easy. Complete backups; manual or scheduled (backup to Dropbox, S3, Google Drive, Rackspace, FTP, SFTP, email + others).

*By UpdraftPlus.Com,  
DavidAnderson*

[Install Now](#)  
[More Details](#)

★★★★★ (6,185)

3+ Million Active Installations

Last Updated: 1 month ago

✓ **Compatible** with your version of WordPress

# 7. Use the latest version of PHP

- Current supported PHP version is 7.4

Branch	Initial Release		Active Support Until		Security Support Until	
<a href="#">7.4</a>	28 Nov 2019	<i>2 years, 6 months ago</i>	28 Nov 2021	<i>6 months ago</i>	28 Nov 2022	<i>in 5 months</i>
<a href="#">8.0</a>	26 Nov 2020	<i>1 year, 6 months ago</i>	26 Nov 2022	<i>in 5 months</i>	26 Nov 2023	<i>in 1 year, 5 months</i>
<a href="#">8.1</a>	25 Nov 2021	<i>6 months ago</i>	25 Nov 2023	<i>in 1 year, 5 months</i>	25 Nov 2024	<i>in 2 years, 5 months</i>



## 8. Choose secured usernames

---

- Avoid dictionary words

`root, admin, user, password, ...`



# 9. Table Prefix

---



Below you should enter your database connection details. If you're not sure about these, contact your host.

Database Name	<input type="text" value="wordpress"/>	The name of the database you want to use with WordPress.
Username	<input type="text" value="username"/>	Your database username.
Password	<input type="text" value="password"/>	Your database password.
Database Host	<input type="text" value="localhost"/>	You should be able to get this info from your web host, if localhost doesn't work.
Table Prefix	<input type="text" value="wp_"/>	If you want to run multiple WordPress installations in a single database, change this.

## 10. Disable Theme Editor

---

```
define( 'DISALLOW_FILE_EDIT', true );
```

# Your Tips?

---

# More Tips

---

- <https://wordpress.org/support/article/hardening-wordpress/>
- <https://www.cisa.gov/uscert/ncas/tips/ST18-006>