

# A Review of WordPress Security

What is WordPress?

How secure is WordPress?

How does one deploy WordPress securely?

\$ whoami

Panda

panda@protectedbypanda.com

@fuzzing\_panda

cybermedsummit.org

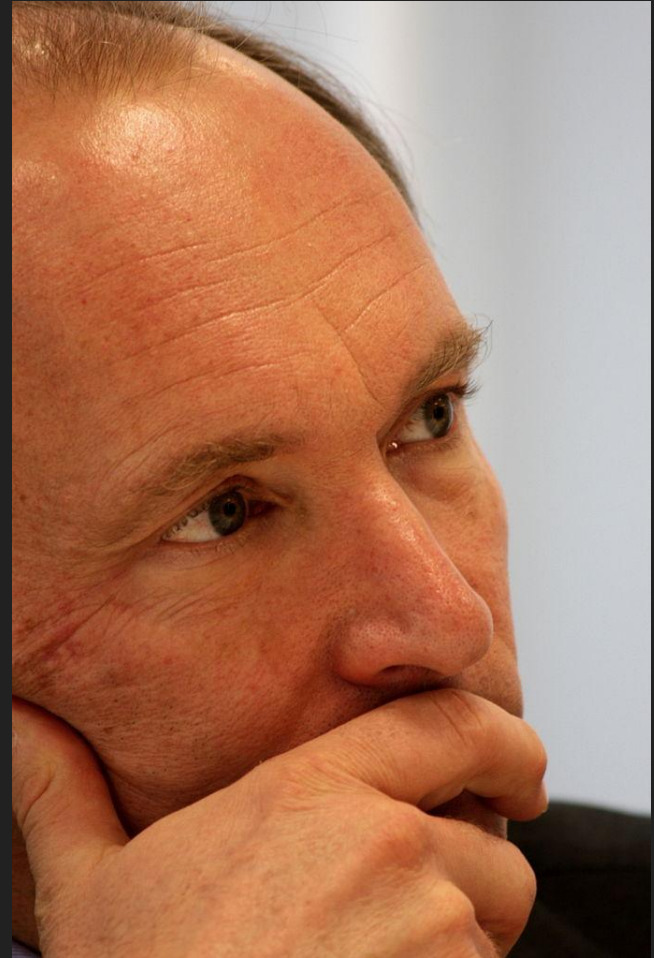
RaiseMe @ShellConLa



# Once upon a time...

1990 to be exact,  
British physicist Tim Berners-Lee invented  
the World Wide Web.

<https://home.cern/science/computing/birth-web>



# Web publishing grew and grew.

Unfortunately, many ran into the same problems.

1. Styling documents was not possible.
2. The document structure was not separate from the document layout (think newspapers).

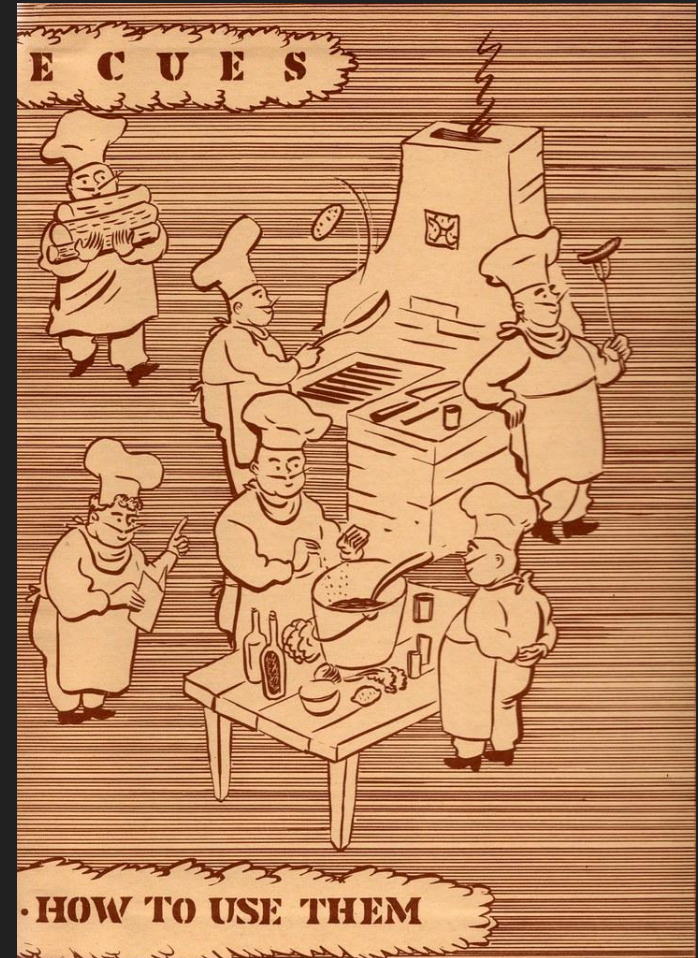
<https://www.contentstack.com/blog/all-about-headless/content-management-systems-history-and-headless-cms/>



# The years passed.

New technologies were developed, and dynamic content delivery came to fruition -- yay! The Web turned 2.0, the participatory and social web. Unfortunately, many ran into a problem: being able to have multiple content creators with varying permission levels.

<https://www.contentstack.com/blog/all-about-headless/content-management-systems-history-and-headless-cms/>



# In 2003 Matt and Mike created WordPress.

- Free and open source software (FOSS)
- Content management system (CMS)
- Plugin architecture
- Web templates that they dubbed "Themes"

Unfortunately, many ran into the same questions:

Is WordPress secure?

Is *my* WordPress secure?

Source

- <https://ma.tt/about/>
- <https://mikelittle.org/>
- <https://wordpress.org/about/>



# Security by Numbers

# Methodology

- Sample top sites around the world
- Common Vulnerabilities and Exposures (CVE) Program
- WPScan vulnerability statistics
- Exploits for WordPress



# WordPress Component = Vulnerability Categories

WordPress Plugins

WordPress Themes

WordPress Core

WordPress = WP

# Baseline: Sampling top sites from around the world

- How many sites? > 10 m = Alexa + Tranco
- How many sites use a content management system? > 6 m
- How many WordPress sites exist? > 4 m (40% all sites)
- How many WordPress versions exist? 497
- How many WordPress plugins exist? > 93 k
- How many WordPress plugins are installed on average? 22

## Sources

- [https://w3techs.com/blog/entry/40\\_percent\\_of\\_the\\_web\\_uses\\_wordpress](https://w3techs.com/blog/entry/40_percent_of_the_web_uses_wordpress)
- <https://w3techs.com/technologies/details/cm-wordpress>
- <https://wpscan.com/statistics>

# What are common types of plugins?

Search engine optimization (SEO)

Automation (e.g., blocking spam posts, tracking)

E-commerce

Editors

Security

<https://themeisle.com/blog/most-popular-wordpress-plugins/>

# Baseline: Sampling top sites from around the world

- How many sites? > 10 m = Alexa + Tranco
- How many sites use a content management system? > 6 m
- How many WordPress sites exist? > 4 m (40% all sites)
- How many WordPress versions exist? 497
- How many WordPress plugins exist? > 93 k
- How many WordPress plugins are installed on average? 22
- How many WordPress themes exist? > 22 k

## Sources

- [https://w3techs.com/blog/entry/40\\_percent\\_of\\_the\\_web\\_uses\\_wordpress](https://w3techs.com/blog/entry/40_percent_of_the_web_uses_wordpress)
- <https://w3techs.com/technologies/details/cm-wordpress>
- <https://wpscan.com/statistics>

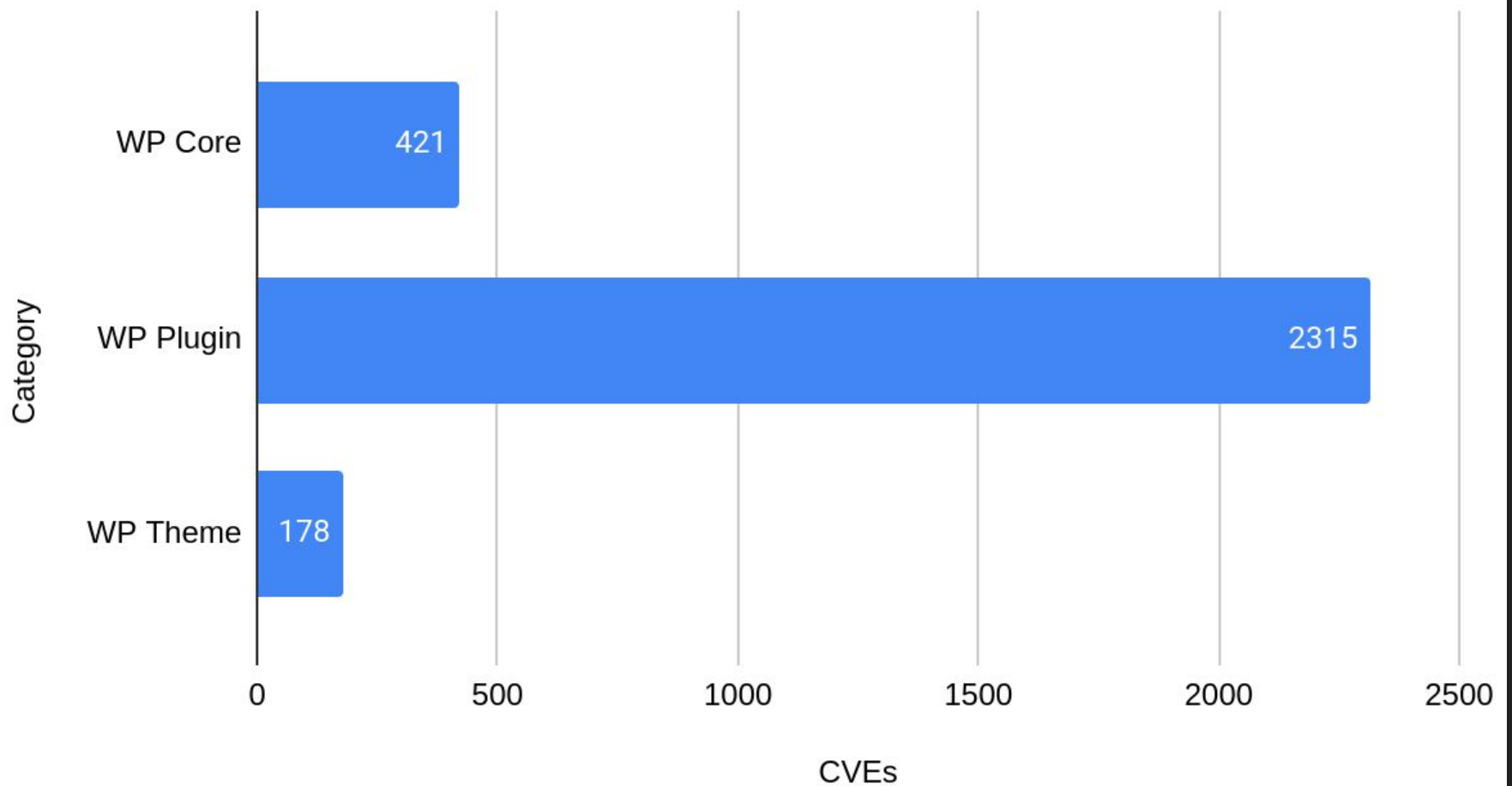
# Common Vulnerabilities and Exposures (CVE) Program

- CVE Program catalogs *publicly* disclosed cybersecurity vulnerabilities.
- Keyword = "wordpress" or "wp"
- 2,875 unique CVEs

## Source

- <https://cve.mitre.org/about/index.html>
- <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wordpress>
- <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wp>

## Count of CVEs by Categories



<https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wordpress>

<https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wp>

# Limitations of CVE Perspective

- Some vulnerabilities are the *sum* of multiple CVEs.
- Some vulnerabilities do *not* have CVE ID.

# WPScan

- "Free"
- Not open source but on GitHub
- Language: Ruby
- Vulnerabilities > 22 k
- Unique vulnerabilities > 4 k

## Source

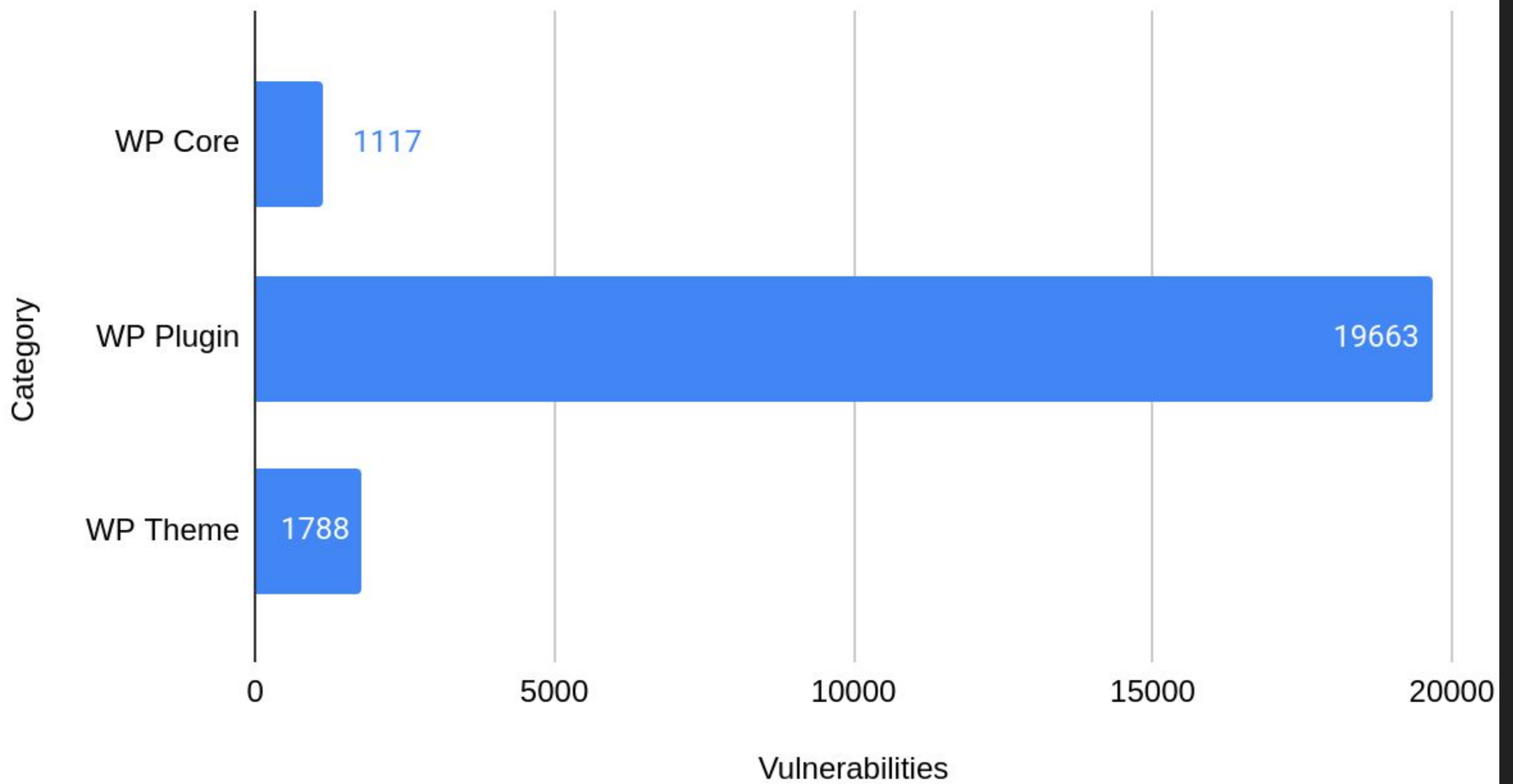
- <https://github.com/wpscanteam/wpscan>
- <https://github.com/wpscanteam/wpscan/wiki/WPScan-User-Documentation>
- <https://wpscan.com/statistics>



**WPScan**



## Count of Vulnerabilities by Category



# Risk: How dangerous is a vulnerability?

- Risk = Likelihood \* Impact
- Likelihood = threat agent \* vulnerability
- Threat agent = skill, motivation, opportunity, and size
- Vulnerability = ease of discovery, ease of exploitation, awareness, and intrusion detection

## Source

- [https://owasp.org/www-community/OWASP\\_Risk\\_Rating\\_Methodology](https://owasp.org/www-community/OWASP_Risk_Rating_Methodology)

# EXPLOIT DB

Free

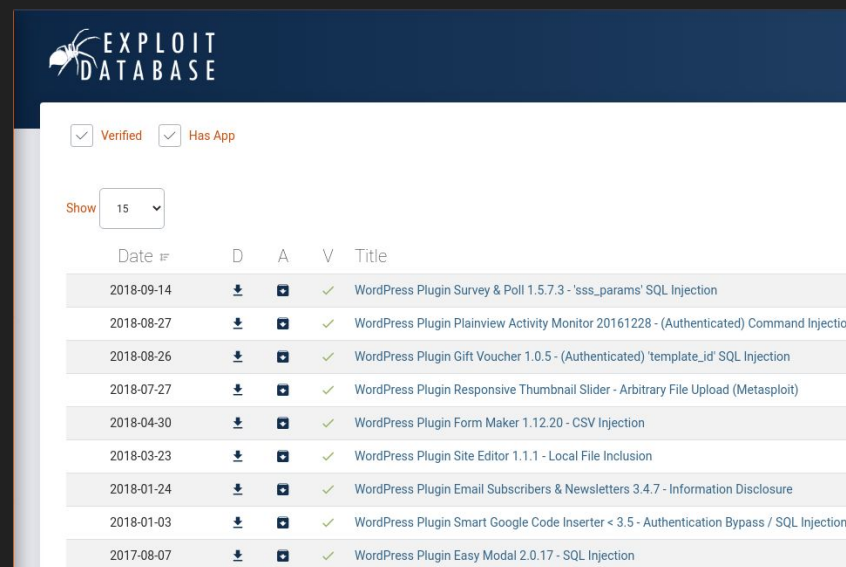
Maintainers: Offensive Security + Community

Keyword = "wordpress"

1,251 exploits

734 validated exploits

270 validated exploits with a vulnerable application



The screenshot shows the Exploit Database interface with search filters for 'Verified' and 'Has App'. A table lists 15 results, each with a date, download icon, app icon, validation status, and title.

Date	D	A	V	Title
2018-09-14	↓	📺	✓	WordPress Plugin Survey & Poll 1.5.7.3 - 'sss_params' SQL Injection
2018-08-27	↓	📺	✓	WordPress Plugin Plainview Activity Monitor 20161228 - (Authenticated) Command Injection
2018-08-26	↓	📺	✓	WordPress Plugin Gift Voucher 1.0.5 - (Authenticated) 'template_id' SQL Injection
2018-07-27	↓	📺	✓	WordPress Plugin Responsive Thumbnail Slider - Arbitrary File Upload (Metasploit)
2018-04-30	↓	📺	✓	WordPress Plugin Form Maker 1.12.20 - CSV Injection
2018-03-23	↓	📺	✓	WordPress Plugin Site Editor 1.1.1 - Local File Inclusion
2018-01-24	↓	📺	✓	WordPress Plugin Email Subscribers & Newsletters 3.4.7 - Information Disclosure
2018-01-03	↓	📺	✓	WordPress Plugin Smart Google Code Inserter < 3.5 - Authentication Bypass / SQL Injection
2017-08-07	↓	📺	✓	WordPress Plugin Easy Modal 2.0.17 - SQL Injection

<https://www.exploit-db.com/>



```
msf6 > search wordpress wp type: exploit
```

```
Matching Modules
```

```
=====
```

#	Name
0	exploit/multi/php/wp_duplicator_code_inject
1	exploit/multi/http/wp_db_backup_rce
2	exploit/multi/http/wp_ait_csv_rce
3	exploit/unix/webapp/wp_admin_shell_upload
4	exploit/unix/webapp/wp_asset_manager_upload_exec
5	auxiliary/scanner/http/wp_contus_video_gallery_sqli

Metasploit Framework: 43 exploits

## Description

-----

Snap Creek Duplicator WordPress plugin code injection

WP Database Backup RCE

WordPress AIT CSV Import Export Unauthenticated Remote Code Execution

WordPress Admin Shell Upload

WordPress Asset-Manager PHP File Upload Vulnerability

Metasploit Framework:

> 30 critical vulnerabilities with exploits

# WordPress in the 2020 Wild

Timeframe: 2020

Targets: 11 k

Unique WP vulns: 210

Vulnerability Type	Percent of Vulnerabilities
Information Disclosure	71.1%
Varied	16.9%
Remote Code Execution (RCE)	4.9%
Cross-site Scripting (XSS)	3.2%
Directory Traversal	2.2%
XML injection	1.1%
SQL Injection (SQLi)	0.4%

How does one deploy  
WordPress securely?



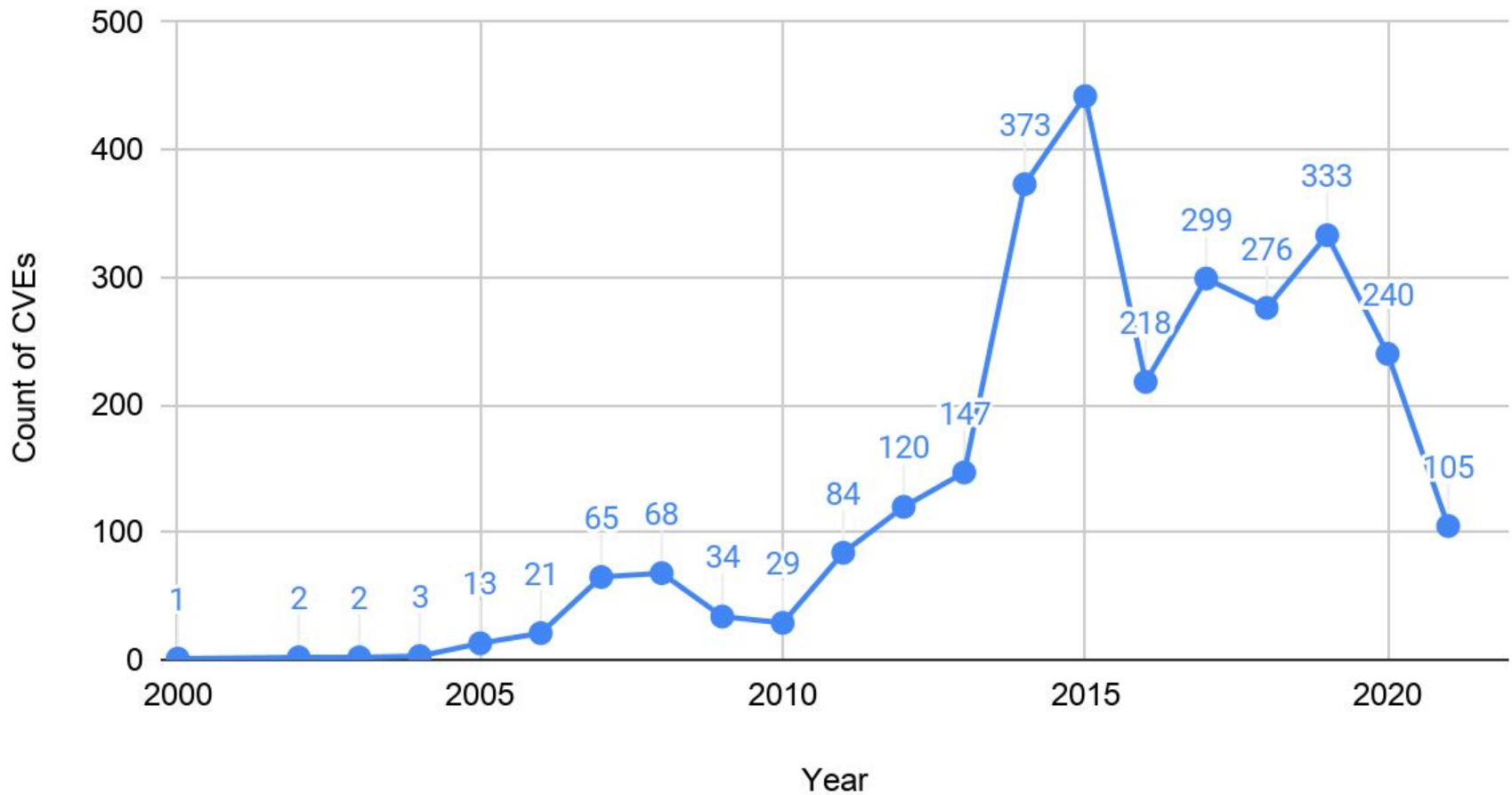
# How does one deploy WordPress securely?

- Patch -- 39% of incidents were secondary to out of date deployments

## Source

- <https://blog.sucuri.net/2018/04/hacked-website-trend-report-2017.html>
- [https://owasp.org/www-project-top-ten/2017/Top\\_10](https://owasp.org/www-project-top-ten/2017/Top_10)
- <https://www.hostinger.com/tutorials/how-to-secure-wordpress>

## Count of CVEs vs. Year



<https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wordpress>

<https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wp>

# How to deploy WordPress securely?

1. Patch -- 39% of incidents 2017 were secondary to out of date deployments
2. Configure -- Security misconfigurations #6 OWASP Top 10 2017
3. Use multifunctional and well supported plugins
4. Use well supported themes
5. Remove unused or unsupported plugins and themes
6. Consider the efficacy of a hosting provider
7. Validate periodically

## Source

- <https://blog.sucuri.net/2018/04/hacked-website-trend-report-2017.html>
- [https://owasp.org/www-project-top-ten/2017/Top\\_10](https://owasp.org/www-project-top-ten/2017/Top_10)
- <https://www.hostinger.com/tutorials/how-to-secure-wordpress>

# This review does *not* consider...

- Technical stack
- Severity of vulnerabilities
- Assumes that all vulnerabilities have a fix

# Closing the Loop

- WordPress is a FOSS CMS.
- Plugins are the top attack vectors for WP deployments.
- Securing WP requires
  - Patch & Configure
  - Chose plugins and themes judiciously
  - Remove unused or unsupported plugins and themes
  - Consider the efficacy of a hosting provider
  - Validate periodically
- Limitation of review
- Additional reading
  - <https://wordpress.org/about/security/>
  - <https://wordpress.org/support/article/hardening-wordpress/>

Go raibh maith agaibh go léir.

Panda

[panda@protectedbypanda.com](mailto:panda@protectedbypanda.com)

[@fuzzing\\_panda](#)

[cybermedsummit.org](http://cybermedsummit.org)

RaiseMe [@ShellConLa](#)

