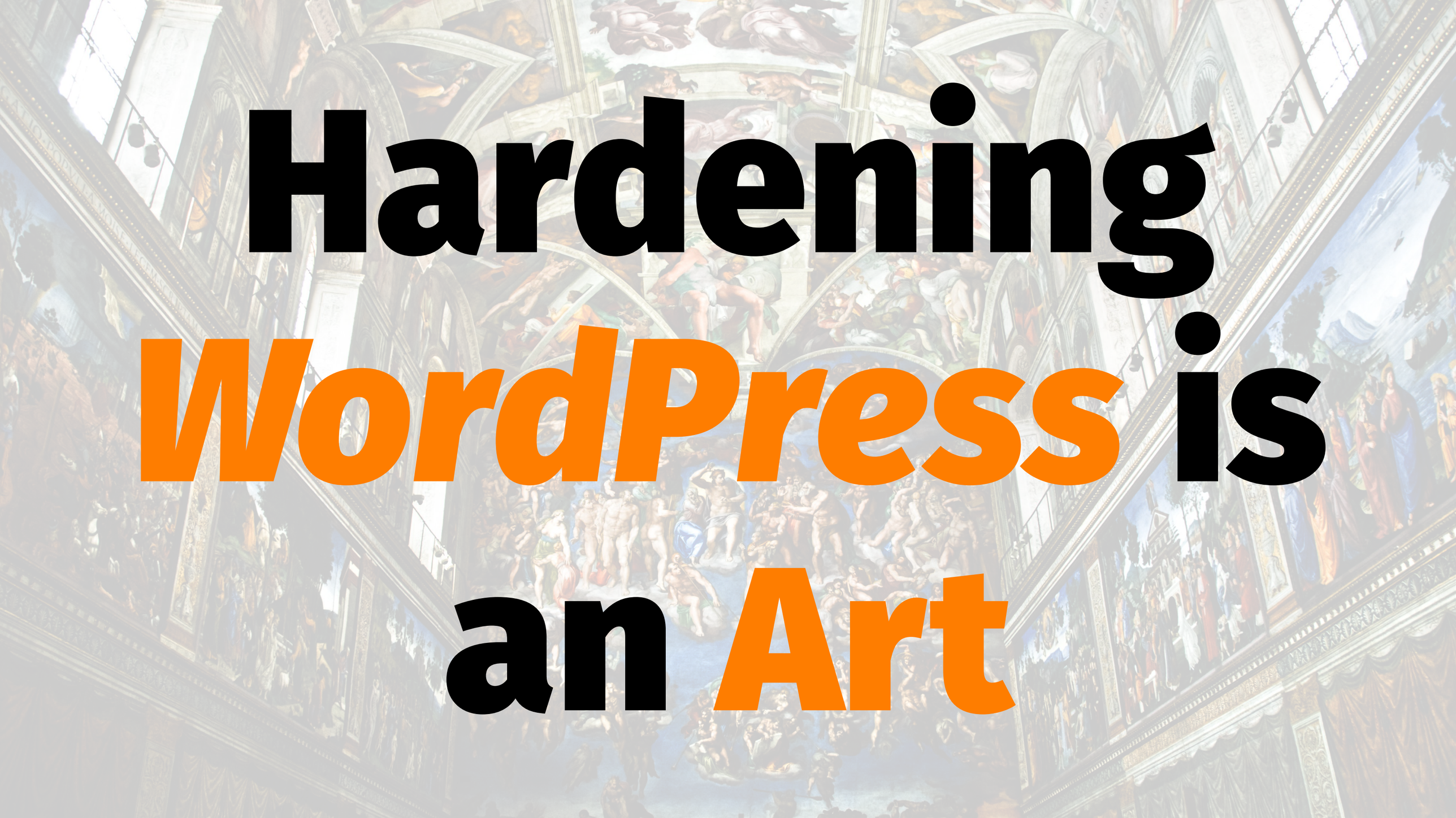
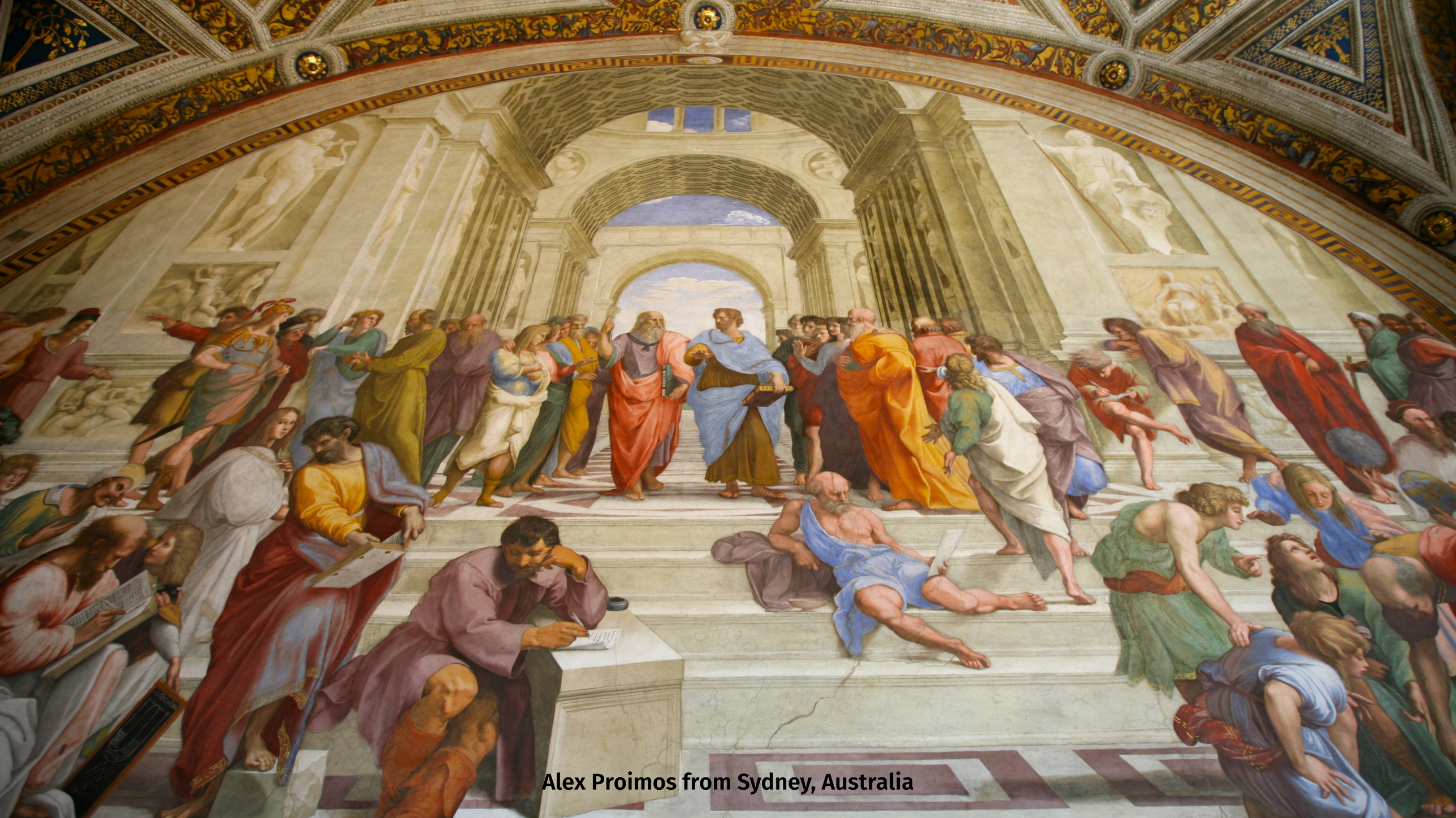

Hardening
WordPress is
an Art

Who am I

Chathu Vishwajith

Auth0 Ambassador
Co-Founder of a startup



Alex Proimos from Sydney, Australia

Is WordPress is *secure?*

→ **52%** are from WordPress plugins

→ **37%** are from core WordPress

→ **11%** are from WordPress themes

Recent incidents

Recent Incidents

→ Display Widgets

→ WooCommerce Product Vendors

→ WordPress Security Update 4.8.2 – **Update Immediately!**

Types of vulnerabilities

→ SQL Injection (SQLI)

→ Cross-site Scripting (XSS)

→ Cross-Site Request Forgery (CSRF)

→ Brute Force

→ Denial of Service (DoS)

→ Distributed Denial of Service (DDoS)

→ Full Path Disclosure (FPD)

→ User Enumeration

→ Remote Code Execution (RCE)

→ Remote File Inclusion (RFI)

→ Directory Traversal

So what is the Art

Continuous improvements

Find a secured *hosting*

Don’t *forget* to update!

Don’t *forget* to update!

→ Keep your WordPress up-to-date

→ Update your plugins and themes

→ Change passwords periodically

→ Keep yourself updated

Use *your own*, not *defaults!*

Use your own, not *defaults!*

→ Do not use ***'admin'*** as your username

→ Change `WP_CONFIG`'s keys and salt values to **randomly generated** values

→ Change **table prefix**

Stop directory *indexing*

Index of /wp-content/plugins

Name	Last modified	Size	Description
Parent Directory		-	
fancy-box/	20-May-2013 15:44	-	
formbuilder/	03-Jan-2013 08:08	-	
jetpack/	20-May-2013 15:44	-	

Prevent User *emumaration*

Disable XML-RPC *if not using*

Limit login *failed* *attempts*

Backup *regularly*

Remove unused *plugins/themes*

Turn on Comments *approval*

Use HTTPS!

Atleast *wp-admin* area and *wp-login.php*

Make sure Debugging is *off!*

Apache, PHP, NGINX, SSL

Vulnerabilities

WPScan Vulnerability Database

Cataloging **8053** WordPress Core, Plugin and Theme vulnerabilities

Free Email Alerts | Submit a Vulnerability | Try our API

WordPress Vulnerability Database

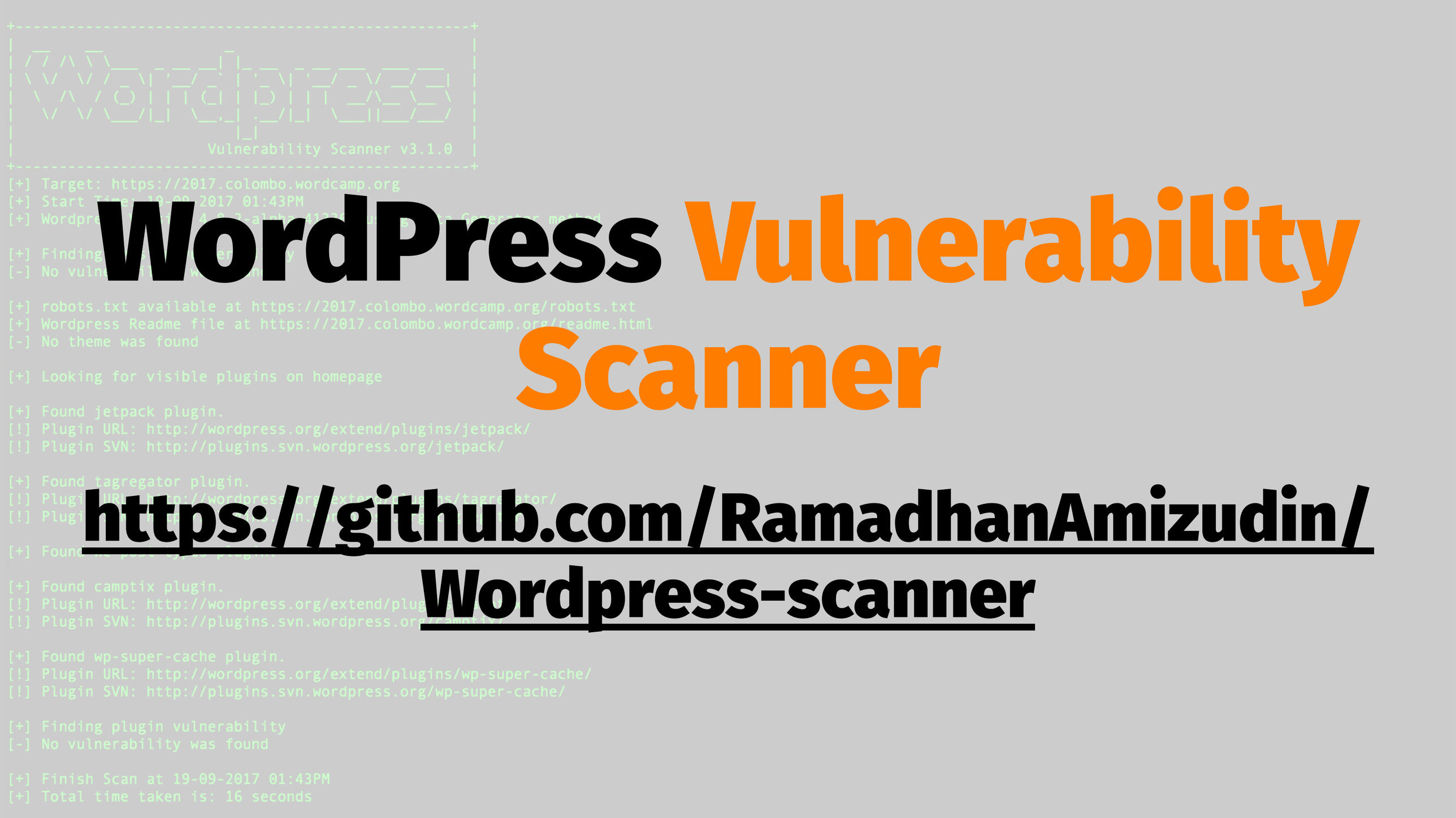
https://wpvulndb.com

Latest WordPress Vulnerabilities

2017-05-17 WordPress 2.7.0-4.7.4 - Insufficient Redirect Validation
2017-05-17 WordPress 2.5.0-4.7.4 - Post Meta Data Validation
2017-05-17 WordPress 3.4.0-4.7.4 - XML-RPC Post Data Handling
2017-05-17 WordPress 2.5.0-4.7.4 - Filesystem Credentials Dialog CSRF
2017-05-17 WordPress 3.3-4.7.4 - Large File Upload Error XSS
2017-05-17 WordPress 3.4.0-4.7.4 - Customizer XSS & CSRF
2017-05-05 WordPress 2.3-4.7.5 - Host Header Injection in Password Reset

Latest Plugin Vulnerabilities

2017-09-11 Display Widgets 2.6.0-2.6.3.1 - Backdoored
2017-09-06 Participants Database <= 1.7.5.9 - Cross-Site Scripting
2017-08-29 BackupGuard <= 1.1.46 - Authenticated Cross-Site Scripting (XSS)
2017-08-31 WooCommerce Product Vendors Plugin <= 2.0.27 - Unauthenticated Reflected XSS
2017-08-25 Photo Gallery by WD <= 1.3.50 - Authenticated SQL Injection
2017-08-25 Embed Images in Comments <= 0.5 - Unauthenticated Stored XSS



WordPress Vulnerability Scanner

https://github.com/RamadhanAmizudin/Wordpress-scanner

```
+-------------------------------------------------------+
|  __    __                _                            |
| / / /\ \ \___  _ __ __| |_ __  _ __ ___  ___ ___      |
| \ \/  \/ / _ \| '__/ _` | '_ \| '__/ _ \/ __/ __|     |
|  \  /\  / (_) | | | (_| | |_) | | |  __/\__ \__ \     |
|   \/  \/ \___/|_|  \__,_| .__/|_|  \___||___/___/     |
|                         |_|                           |
|                    Vulnerability Scanner v3.1.0       |
+-------------------------------------------------------+
[+] Target: https://2017.colombo.wordcamp.org
[+] Start Time: 19-09-2017 01:43PM
[+] Wordpress Version 4.8.2-alpha-41336, using Meta Generator method

[+] Finding version vulnerability
[-] No vulnerability was found

[+] robots.txt available at https://2017.colombo.wordcamp.org/robots.txt
[+] Wordpress Readme file at https://2017.colombo.wordcamp.org/readme.html
[-] No theme was found

[+] Looking for visible plugins on homepage

[+] Found jetpack plugin.
[!] Plugin URL: http://wordpress.org/extend/plugins/jetpack/
[!] Plugin SVN: http://plugins.svn.wordpress.org/jetpack/

[+] Found tagregator plugin.
[!] Plugin URL: http://wordpress.org/extend/plugins/tagregator/
[!] Plugin SVN: http://plugins.svn.wordpress.org/tagregator/

[+] Found wc-post-types plugin.

[+] Found camptix plugin.
[!] Plugin URL: http://wordpress.org/extend/plugins/camptix/
[!] Plugin SVN: http://plugins.svn.wordpress.org/camptix/

[+] Found wp-super-cache plugin.
[!] Plugin URL: http://wordpress.org/extend/plugins/wp-super-cache/
[!] Plugin SVN: http://plugins.svn.wordpress.org/wp-super-cache/

[+] Finding plugin vulnerability
[-] No vulnerability was found

[+] Finish Scan at 19-09-2017 01:43PM
[+] Total time taken is: 16 seconds
```

Summery

→ Don’t forget to update.

→ Use your own rather defaults.

→ Stop directory traversal.

→ Disable XML-RPC if you are not using it.

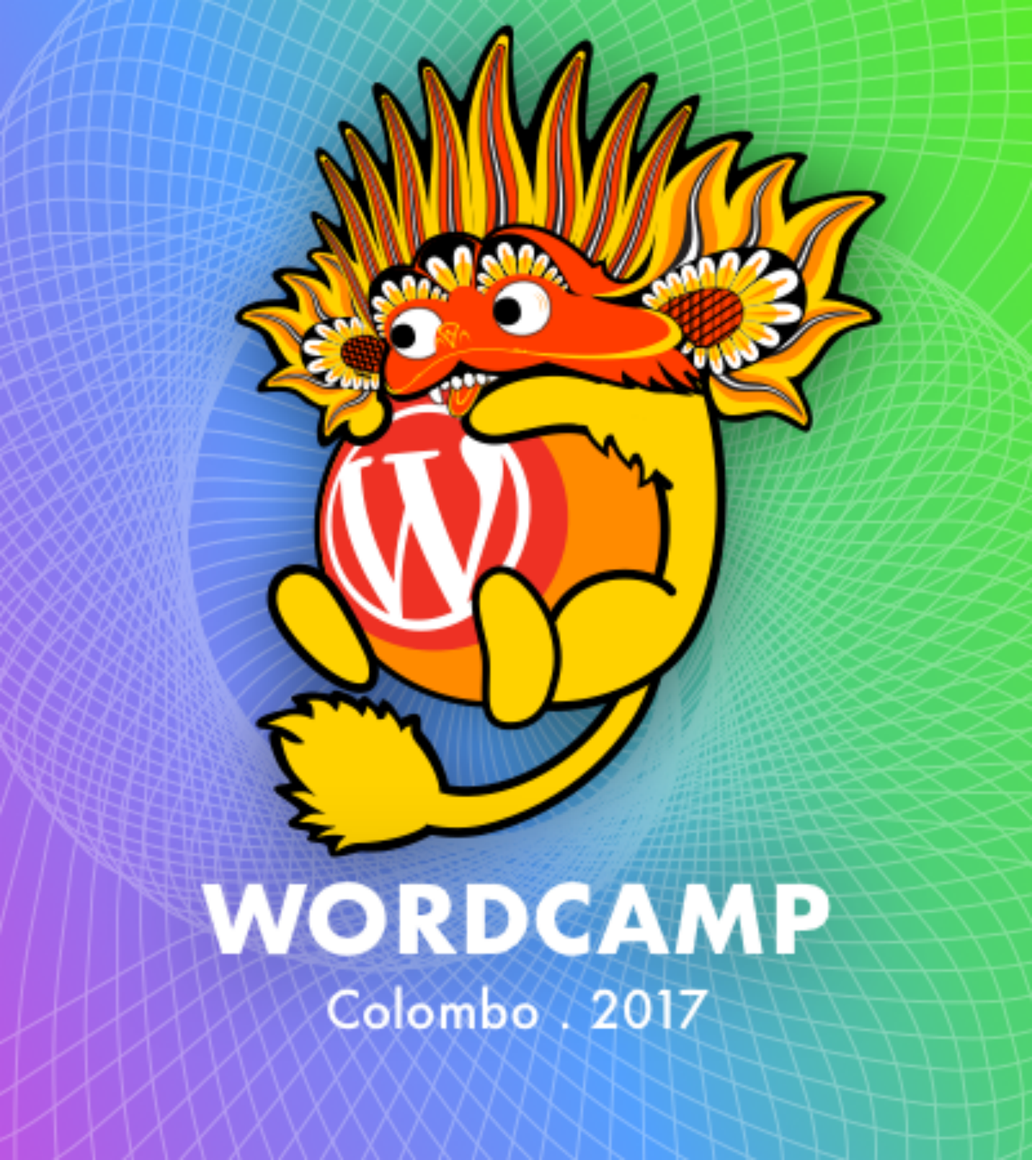
→ Limit login attempts.

→ Backup regularly

→ Remove unused plugins/themes

→ Keep yourself updated

From Sri Lanka 🇱🇰



Thank you 👍