

WordPress Security Basics

Ryan Plas - @wordplas

Defense In Depth

Defense In Depth

The idea behind the defense in depth approach is to defend a system against any particular attack using several independent methods.¹

There is no single approach to security - have many layers.

1: [https://en.wikipedia.org/wiki/Defenseindepth_\(computing\)](https://en.wikipedia.org/wiki/Defenseindepth_(computing))

Defense In Depth

Layers:

1. Code
2. Authentication
3. Hosting

code

Code

What this section isn't: How to write secure code

What this section is: How to make sure the code of your site is secure

Code

Keep your site updated

- Auto updates for minor versions since 3.7
- Update to major versions as soon as possible

Code

Keep your plugins and themes updated


- The longer you wait, the more likely there's a vulnerability.
- [WPScan Vulnerability Database](#)

Code

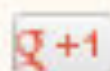
Only use plugins and themes from reputable sources

- Trusted brands/companies
- Don't avoid paying money
- Don't look for free versions of premium plugins/themes
- The Plugin/Theme repo is your friend



 **Add to My WatchList**

Share:



Q&A

Board



Download Now

(4.61MB)



ADL Uncompressor

Open Compressed
Files in 1 Click

Rating: ★★★★★

"...Recommended Download"



Download



 Add to My WatchList

Share:       Q&A

Board



Download Now

(4.61MB)

If the site looks like this...run!



ADL Uncompressor

Open Compressed
Files in 1 Click

Rating: ★★★★★

"...Recommended Download"

Download



Authentication

Authentication

Use a strong password

- Question...what is a strong password?

Authentication

Use one of preferably both of the following:

- Password manager
- Two-factor authentication

Authentication

Password Manager:

- Program that can create and securely store passwords
- Allows you to use longer/more complex passwords without having to memorize or write them down

Authentication

Two-factor Authentication:

- Something you know - password, pin
- Something you have - phone, YubiKey

Authentication

Passwords:

Use a password manager and/or two-factor authentication

- LastPass, 1Password, Dashlane - **Personal**
- Duo, Google Authenticator, etc. - **Plugin**

If you can't do that, use a long but easy to remember password.

- correct horse battery staple
- [date]-[place]-[thing]: 1976-Switzerland-dragon

Principle of Least Privilege

Authentication

Principle of least privilege:

- Any user should only be able to access exactly what they need to and nothing else.
- Don't make everyone an admin
- Restrict user roles to only what is required
- Use a plugin if necessary

Authentication

Bonus: Don't use admin as a username

Hosting

Hosting

What to look for in a good hosting provider:

- SSL
- Firewall
- Datacenter
- Customer Support



NETWORK SERVICES

Never let a sudden torrent of traffic knock your servers down again. Distribute traffic with a load balancer and protect DDoS attacks with DDoS prevention services.

- **DDoS Attack Prevention**
- **Load Balancers**

[Read More](#)



STORAGE & BACKUP SERVICES

We offer many versatile backup options and a number of flexible storage options.

- **Guardian Off-Site Backups**
- **Storage Area Network (SAN)**
- **Cloud Block Storage**
- **Cloud Object Storage**
- **Log Storage**

[Read More](#)



FIREWALL & VPN

Use a Firewall to protect your servers from Malicious traffic & take security to the next level with a VPN to keep your connection secure.

- **Cloud Firewall**
- **Cisco Firewalls**
- **VPN**

[Read More](#)



SECURITY SERVICES

Solid security is essential when it comes to web hosting. Whether you're securing your site with an SSL, filtering for spam, or more - we've got you covered.

- **ServerSecure**
- **Firewalls**
- **SSL Certificates**
- **PCI Compliance Scanning**
- **Nessus Vulnerability Scanning**
- **Cloudflare®**
- **Protection and Cleanup Services**

[Read More](#)

25,000+ Servers Powering 30,000+ Customers

- ✔ Privately Owned and Operated Core Data Centers
- ✔ Redundant networks, cooling and power
- ✔ Tier-1 Premium Bandwidth
- ✔ On-Site Security
- ✔ Geographic Redundancy Available
- ✔ Team of experts dedicated to monitoring network performance and security - 24/7/365

With the Most Helpful Humans in Hosting, You're Never Alone

Web Hosting without the worry. Rely on our 24/7/365 Human Support.



Phone & Chat Support

Help Within Minutes



100% Network Uptime

Guarantee



100% Power Uptime

Guarantee



30-Minute Help Desk

Initial Response Time
Guarantee



30-Minute Hardware

Replacement Guarantee

Rapid-fire Tips

Disable File Editing

In **wp-config.php**:

```
## Disable Editing in Dashboard  
define( 'DISALLOW_FILE_EDIT', true );
```

Limit Login Attempts

- Make brute forcing passwords take **much longer**
- Potentially **block malicious attempts**
- Lots of plugins that do this
 - JetPack, Limit Login Attempts

Backup Your Site

- Helps in the event of a security incident
- Able to **roll back** to an unaffected backup
- Lots of plugins/services that do this
 - Backup Buddy, BackWPU

"Complete" Solutions

- No solution is "**complete**" (Defense in Depth)
- But...these have a lot of the features we talked about
 - **iThemes Security** - plugin
 - **JetPack** - plugin
 - **Wordfence** - plugin
 - **Securi** - hosting/security platform

wpscan

- Command-line utility to **scan a WP install** for vulnerabilities
- <https://github.com/wpscanteam/wpscan>
- ***ONLY USE ON SITES YOU OWN***

Overview

- **Defense in Depth**
 - Many **layers** of security
- Code
 - **Update** your site/plugins/themes
 - Use **reputable** plugins/themes
- Authentication
 - **Password Manager/Two-factor Authentication**
 - **Principle of Least Privilege**
- Hosting
 - Look for **emphasis on security** (SSL, Firewall, Datacenter etc.)

Questions?

Ryan Plas

@wordplas

github.com/ryanplasma