Improving the security of your WordPress site

AWESOME
TECH TRAINING

Housekeeping

- All the attendee mics are muted – you can hear us but we cannot hear you
- This session is being recorded – we will send you a link to the recording and a downloadable copy of the slides after the event
- If you have any questions please use the Q&A function to ask them – we'll cover the questions at the end if we have time otherwise we will follow up with you individually

Who we are

Agenda

- Introduction to Awesome Tech Training
- Background and the importance of security
- How WordPress gets hacked / compromised
- Steps you can take to secure your WP site
- What to do if you’ve been hacked
- Next Steps

If anything isn't clear...

- Please ask a question!
- There is no such thing as a stupid question

About us

- Our focus is on helping small businesses take control of their own digital marketing presence
- We can help you with all aspects of your digital marketing and web development
- We can work with you to help you build a new website for your business OR to make better use of the site that you already have
- Digital marketing and WordPress advice and support
  - Book sessions by the hour / half day / day – contact us to talk about how we can help you
- Other webinars

Scope of the webinar

Security is a massive subject

- We'll cover one small part of that subject
- Focus on steps you can take to protect your WordPress site(s)
- Assume that your site is hosted at a "regular" hosting company – GoDaddy, 123-reg, etc
- Hosting your own site on a dedicated server or VPS has many additional challenges (not for today!)

Why security is important

Data security

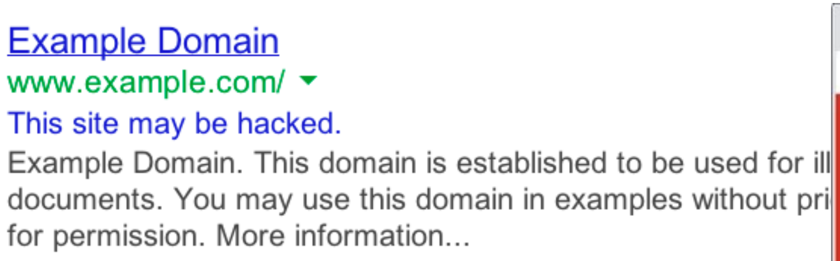
- If your site has any e-commerce or data capture then you might expose information about other visitors or users

- These leaks are serious under the GDPR regime

- You have a duty to keep any personal data on the site secure and safe

Hacked sites – visitor's perspective

- Google might warn or block access

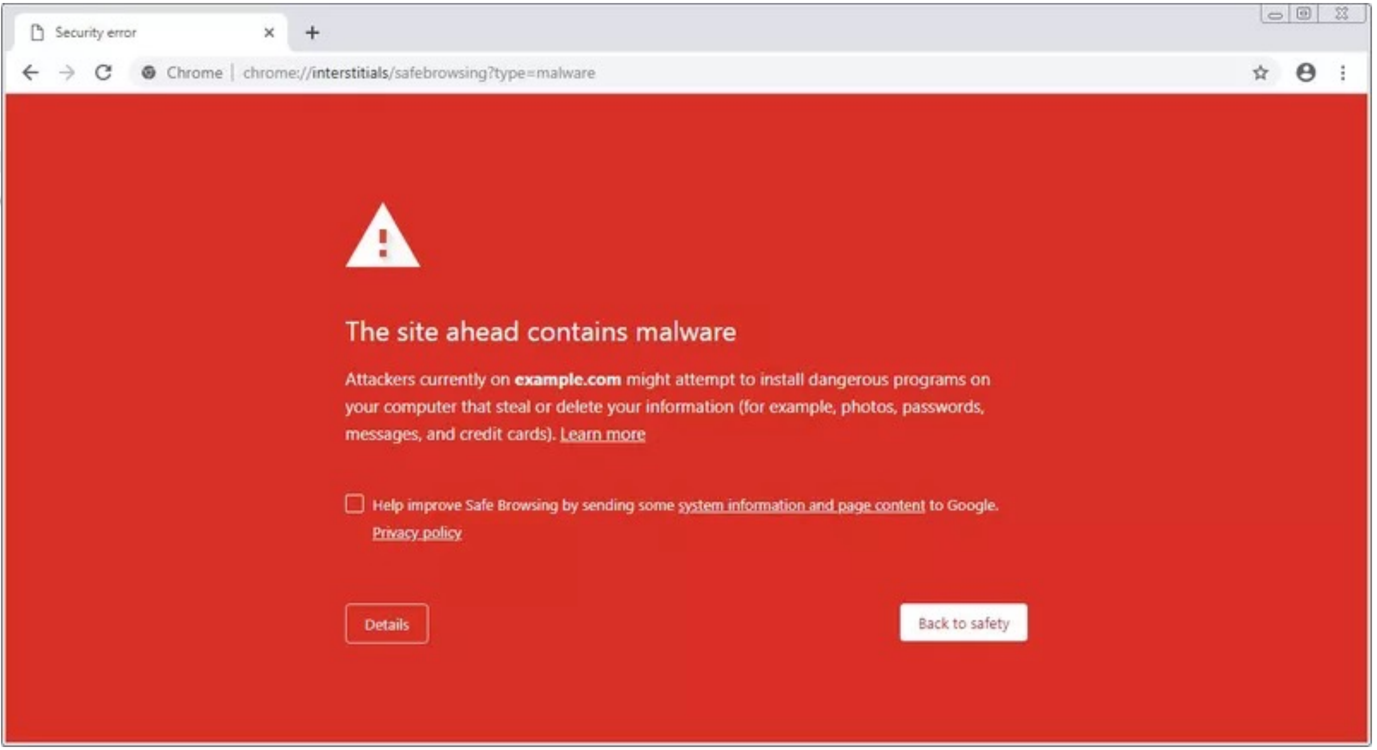


Example Domain

www.example.com/ ▾

This site may be hacked.

Example Domain. This domain is established to be used for ill documents. You may use this domain in examples without pri for permission. More information...



The site ahead contains malware

Attackers currently on **example.com** might attempt to install dangerous programs on your computer that steal or delete your information (for example, photos, passwords, messages, and credit cards). Learn more

□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

Hacked sites – visitor’s perspective

- Google might warn or block access
- At risk of downloading malware
- Might be redirected to a different site
- Content on the site might have changed

Hacked sites – owner’s perspective

- Hidden links can sometimes be impossible to spot until Google starts to recognize them. White text on white background

- Often hacked sites won’t be flagged to the owner until either someone informs them, or they discover in some other way (incognito mode, new browser, etc)

Hacked sites – owner's perspective

- Traffic from organic search will plummet if Google is telling users to avoid the site
- Loss of admin access if passwords are changed
- Sometimes new admin users are added and can change content on your site
- Site speed and performance may start to drop – affecting you and also maybe other sites if on shared hosting
- Hosting company may take your site offline

How WordPress gets compromised

Internal vs external threats

- Internal threats:
  - Anyone with a legitimate account who could cause damage or could access personal data
  - Unhappy or over-enthusiastic staff
  - Previous design companies
  - Ex-staff with access
- External threats:
  - Automated scripts: “bots”
  - Aggrieved individuals / organisations, competition
  - People wanting to capture your audience (redirects)
  - People wanting to exploit your SEO (by adding links to the content)

Myth: This won’t happen to my site

- Don’t imagine that this only happens to large sites, or sites where someone might have a disagreement or complaint
- Almost all these attacks are performed automatically by scripts
- Scripts can detect versions of WordPress, different plugins, probe for known vulnerabilities and can automatically deploy exploits

What are the bots doing?

- Check the logs*:

```
access.log:89.16.x.x - - [18/Apr/2023:02:25:15] "POST /wp-login.php HTTP/1.1" 200 12661 "-" "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.0)" "log=admin&pwd=password&wp-submit=Log+In"

access.log:89.16.x.x - - [18/Apr/2023:02:26:16] "POST /wp-login.php HTTP/1.1" 200 12661 "-" "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.0)" "log=admin&pwd=password1&wp-submit=Log+In"

access.log:89.16.x.x - - [18/Apr/2023:02:27:16] "POST /wp-login.php HTTP/1.1" 200 12661 "-" "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.0)" "log=admin&pwd=password123&wp-submit=Log+In”
```

*These logs have been generated for testing, they wouldn’t normally contain the login credentials

```
pass123
password
password1
password123
q1w2e3
q1w2e3r4
q1w2e3r4t5
qazwsx
qazxsw
qwe123
qwer1234
qwerty
qwerty123
qwertyuiop
root
secret
secret
success1
temppass
test
test1
test123
test1234
testing
testtest
webmaster
welcome
welcome1
zaq123
zaq12wsx
zxcvbnm
zzz
coronavirus
```

What are they doing?

- WordPress sites are made up of four main areas which can be exploited:
  - The admin back-end / dashboard
  - The core WordPress system
  - The plugins and themes that have been added
  - The database
- Bots will systematically test for weaknesses across your system to gain access

Your admin dashboard

- If a user gains access to your dashboard as an administrator then they can control every aspect of your WordPress site
- Bots will probe many different passwords to see if you’ve used anything that can be easily guessed
- WordPress can make this easier by showing what users have been set up
- Sometimes bots will try many thousands of passwords against each of your users

The core WordPress system

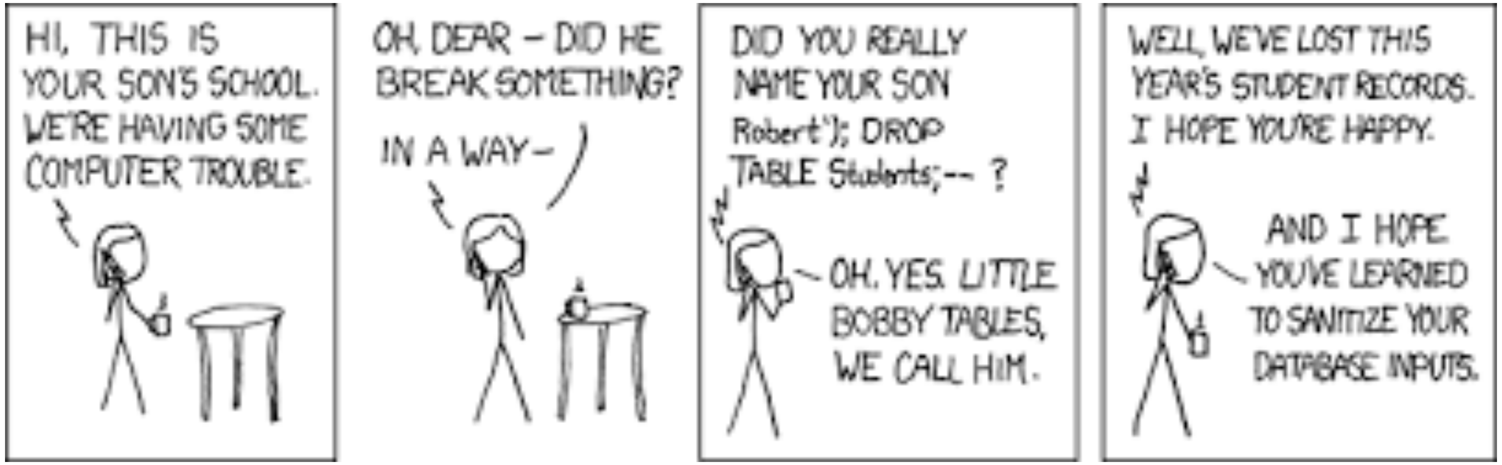
- Older versions of WordPress have known vulnerabilities
- Newer versions of WP have vulnerabilities, it’s just that they might not be known yet
- These are regularly fixed and new released close many security holes
- However, known vulnerabilities mean that attackers can also try to use those to access your site

Themes and plugins

- Like core WordPress, older versions of themes and plugins can often have vulnerabilities
- New versions are released, some less popular plugins might be slower to release fixes
- Some themes and plugins are “abandonware” and may never get a fix
- As new vulnerabilities are found, scripts are updated to exploit them

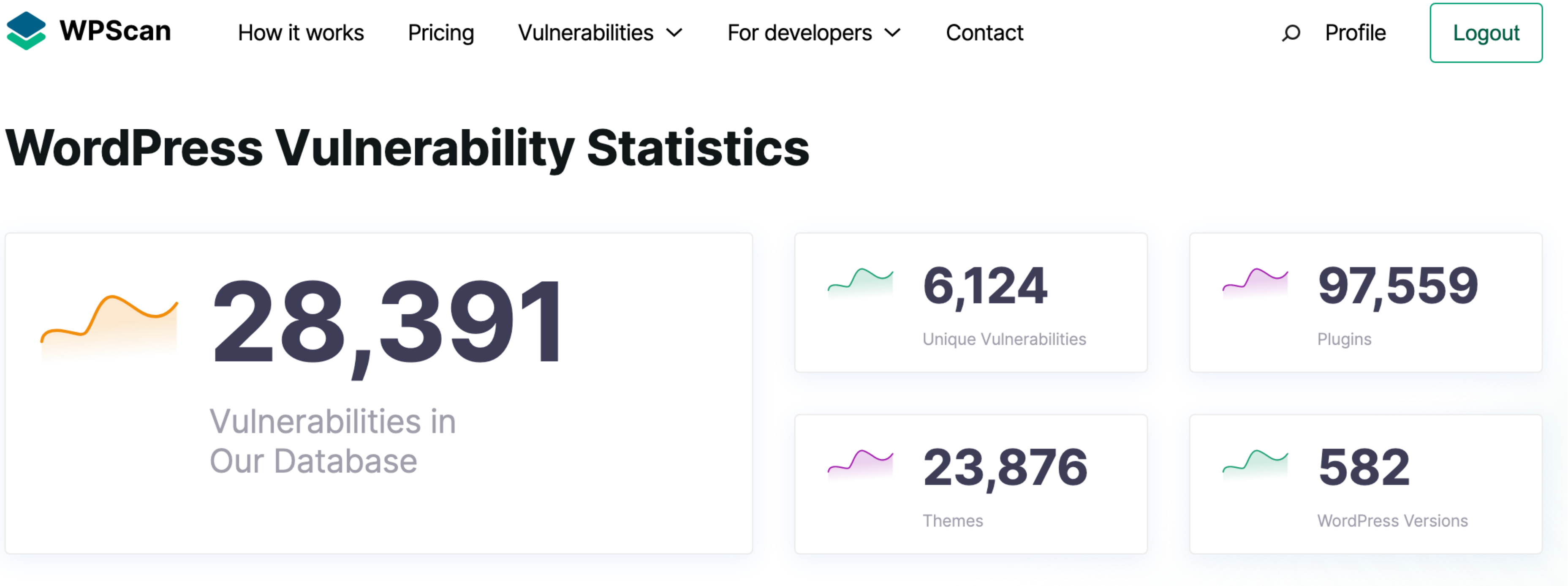
Database

- WordPress stores information in a database – often a MySQL database
- If some code is written badly then it can leave the database open to “SQL Injection” exploits


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

From https://xkcd.com/327/

There are plenty of vulnerabilities



WordPress Vulnerability Statistics

28,391 Vulnerabilities in Our Database

6,124 Unique Vulnerabilities

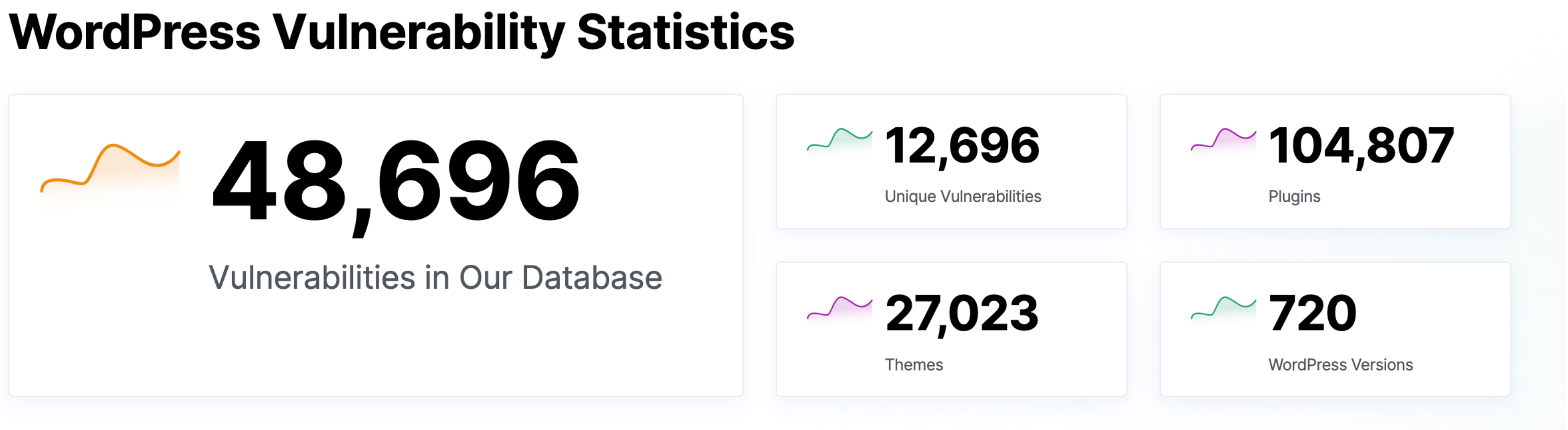
97,559 Plugins

23,876 Themes

582 WordPress Versions

From: https://wpscan.com/statistics 3/4/22

There are plenty more vulnerabilities over time



WordPress Vulnerability Statistics

48,696
Vulnerabilities in Our Database

12,696
Unique Vulnerabilities

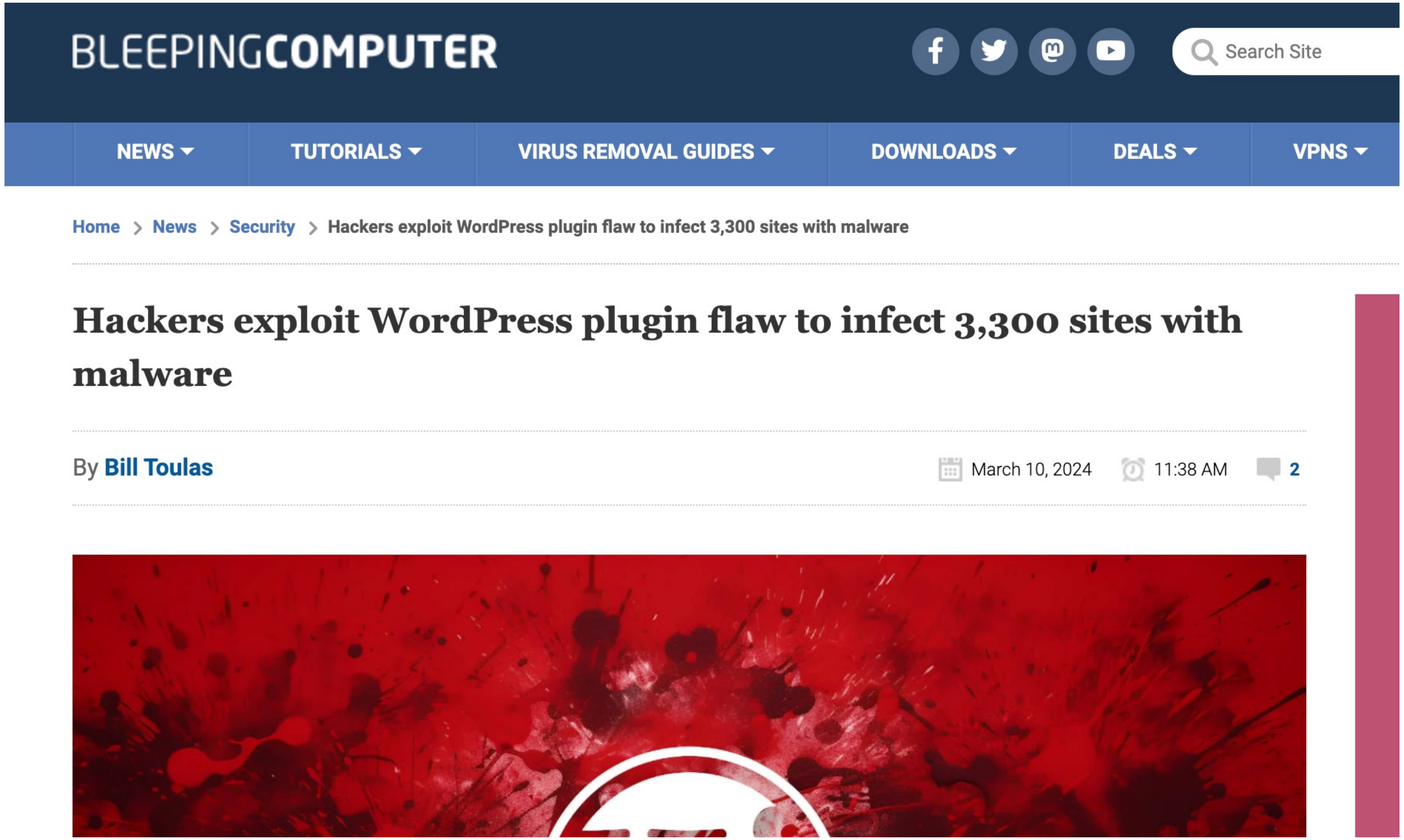
104,807
Plugins

27,023
Themes

720
WordPress Versions

From: https://wpscan.com/statistics 11/03/24

There's always something…



BLEEPINGCOMPUTER

Home > News > Security > Hackers exploit WordPress plugin flaw to infect 3,300 sites with malware

Hackers exploit WordPress plugin flaw to infect 3,300 sites with malware

By Bill Toulas

March 10, 2024 11:38 AM 2

Steps you can take to secure your WordPress site

All is not lost!

- There are many simple ways to lock down and protect your WordPress site

- Many of the steps that we’ll look at can be managed by plugins and automated

- Other steps are simply good practice

All is not lost!

- We’ll look at the following:
  - Improvements to account based authentication and the logging in process
  - Regular maintenance
  - WordFence plugin
  - Web application firewalls

Securing your accounts

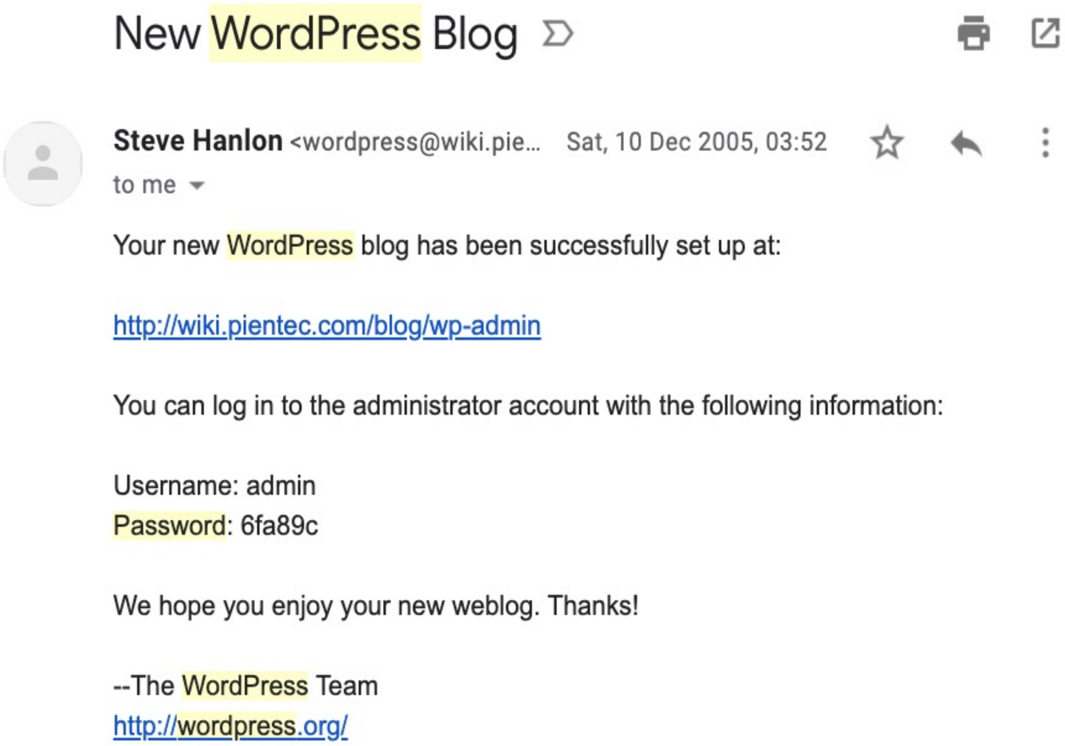
- Your first line of defence is the username and password that you use for your accounts.

- If you do nothing else then consider making your accounts and login process more secure

- These are some of the easiest things you can do

Accounts: Passwords

- Password management has moved on since the early days of WordPress.
- Setting up WordPress, creating accounts and resetting passwords will now make it difficult to set easy passwords
- You definitely won't get an email with a password in these days – if you do, it's almost certainly malicious!



New WordPress Blog

Steve Hanlon <wordpress@wiki.pie... Sat, 10 Dec 2005, 03:52

to me

Your new WordPress blog has been successfully set up at:

http://wiki.pientec.com/blog/wp-admin

You can log in to the administrator account with the following information:

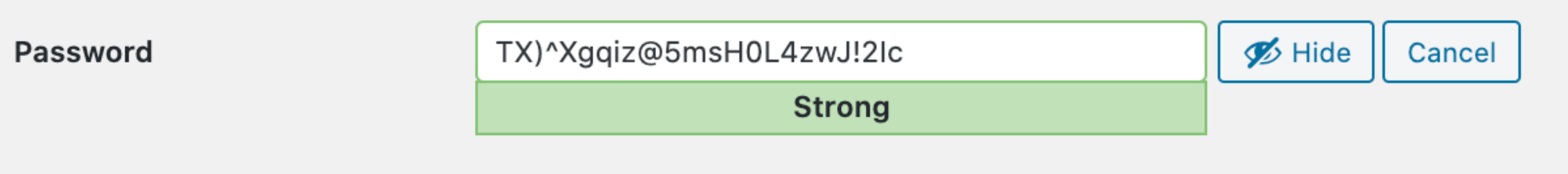
Username: admin
Password: 6fa89c

We hope you enjoy your new weblog. Thanks!

--The WordPress Team
http://wordpress.org/

Accounts: Complex passwords

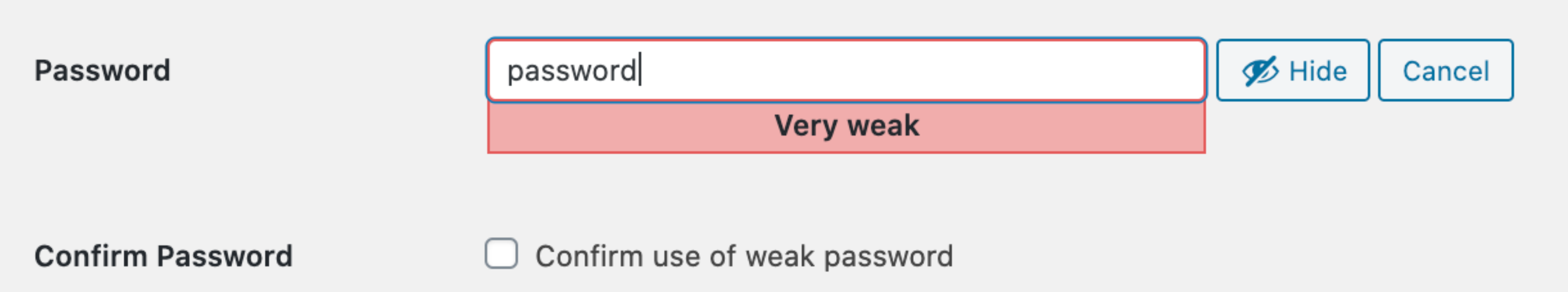
- WordPress will suggest long complex passwords
- Unless there's a VERY GOOD REASON then use them



Password: TX)^Xgqiz@5msH0L4zwJ!2lc

Strong

- You can always choose a bad, insecure password, but you must confirm it



Password: password

Very weak

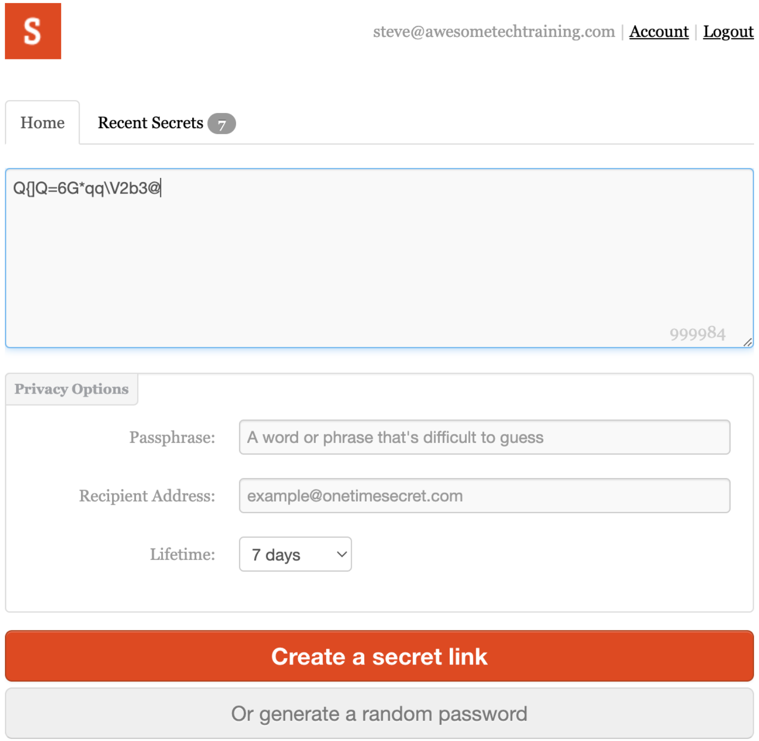
Confirm Password: ☐ Confirm use of weak password

Accounts: use a password manager

- There are many simple, safe password managers
- Choose one that you trust and is easy for the way you work
- If you are Apple based, then keychain is good
- Google has a similar password manager built into Chrome and Android
- Or choose a third party: Bitwarden and 1Password are both good – LastPass has had problems of late
- Use a different password for every site

Password sharing

- If you must share a password use a service like https://onetimesecret.com
- It’s a simple service that lets you share a unique one-time link privately



steve@awesometechtraining.com | Account | Logout

Home | Recent Secrets 7

Q{]Q=6G*qq\V2b3@

999984

Privacy Options

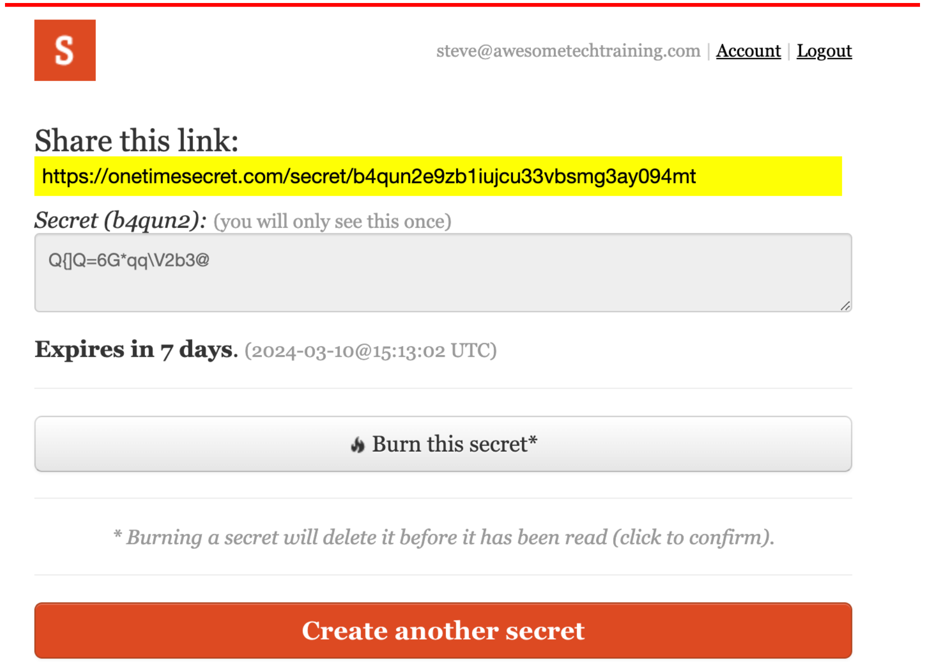
Passphrase: A word or phrase that's difficult to guess

Recipient Address: example@onetimesecret.com

Lifetime: 7 days

Create a secret link

Or generate a random password



steve@awesometechtraining.com | Account | Logout

Share this link:

https://onetimesecret.com/secret/b4qun2e9zb1iujcu33vbsmg3ay094mt

Secret (b4qun2): (you will only see this once)

Q{]Q=6G*qq\V2b3@

Expires in 7 days. (2024-03-10@15:13:02 UTC)

Burn this secret*

** Burning a secret will delete it before it has been read (click to confirm).*

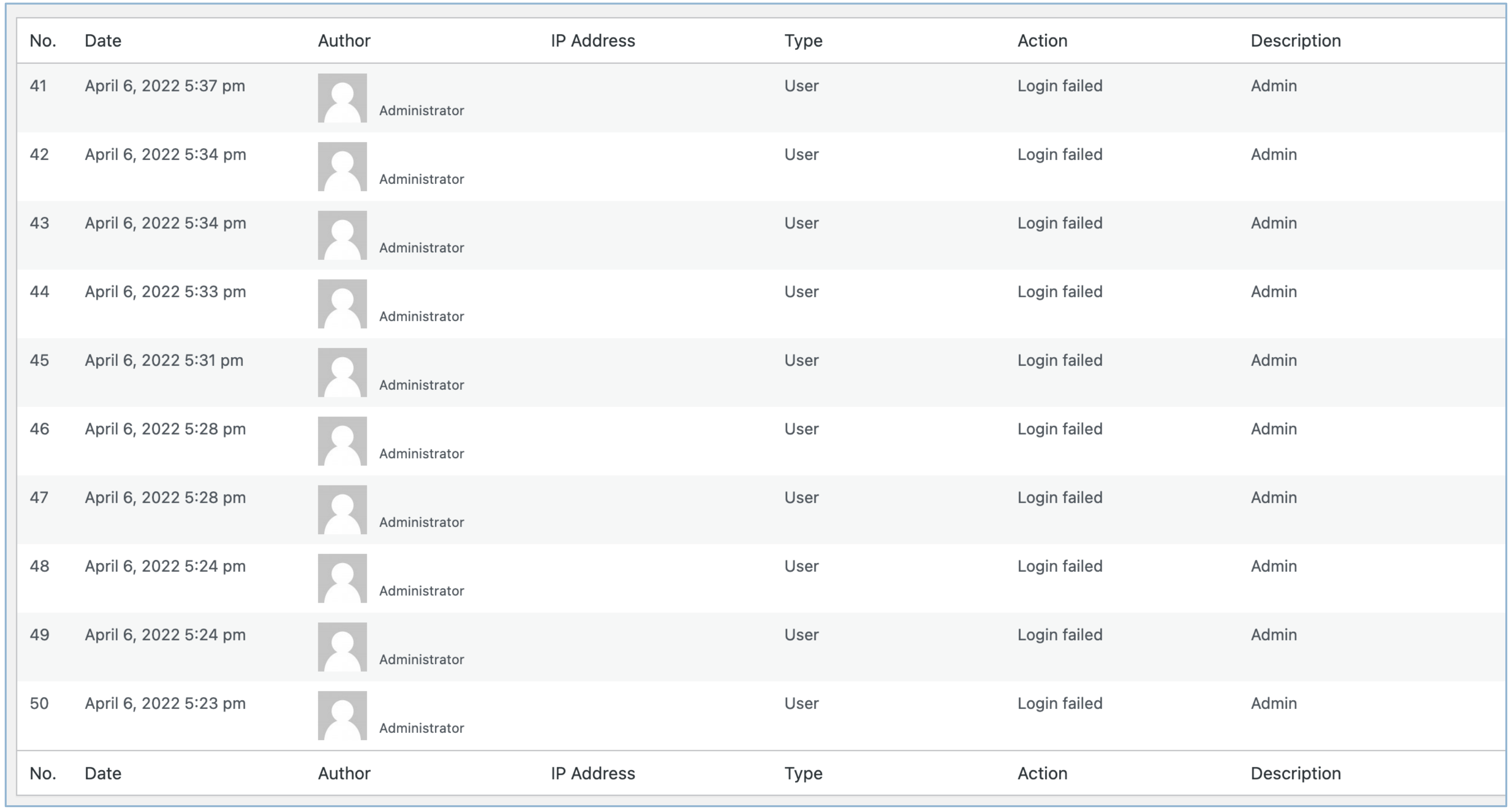
Create another secret

Accounts: Don’t call your admin “admin”!

- When you set up your WordPress installation, choose a unique username for the first admin user
- This makes it harder for the bots to break into an admin account
- Try not to choose obvious administrator usernames. Avoid:
  - administrator
  - manager
  - root
  - etc.

```
access.log:89.16.x.x - - [18/Apr/2023:02:25:15] "POST /wp-login.php HTTP/1.1" 200 12661 "-"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)" "log=admin&pwd=password&wp-submit=Log+In"
access.log:89.16.x.x - - [18/Apr/2023:02:26:16] "POST /wp-login.php HTTP/1.1" 200 12661 "-"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)" "log=admin&pwd=password1&wp-submit=Log+In"
access.log:89.16.x.x - - [18/Apr/2023:02:27:16] "POST /wp-login.php HTTP/1.1" 200 12661 "-"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)" "log=admin&pwd=password123&wp-submit=Log+In”
```

Accounts: Don’t call your admin “admin”!



No.	Date	Author	IP Address	Type	Action	Description
41	April 6, 2022 5:37 pm	Administrator		User	Login failed	Admin
42	April 6, 2022 5:34 pm	Administrator		User	Login failed	Admin
43	April 6, 2022 5:34 pm	Administrator		User	Login failed	Admin
44	April 6, 2022 5:33 pm	Administrator		User	Login failed	Admin
45	April 6, 2022 5:31 pm	Administrator		User	Login failed	Admin
46	April 6, 2022 5:28 pm	Administrator		User	Login failed	Admin
47	April 6, 2022 5:28 pm	Administrator		User	Login failed	Admin
48	April 6, 2022 5:24 pm	Administrator		User	Login failed	Admin
49	April 6, 2022 5:24 pm	Administrator		User	Login failed	Admin
50	April 6, 2022 5:23 pm	Administrator		User	Login failed	Admin
No.	Date	Author	IP Address	Type	Action	Description

Using user activity log plugin https://en-gb.wordpress.org/plugins/user-activity-log/

Accounts: Block user enumeration

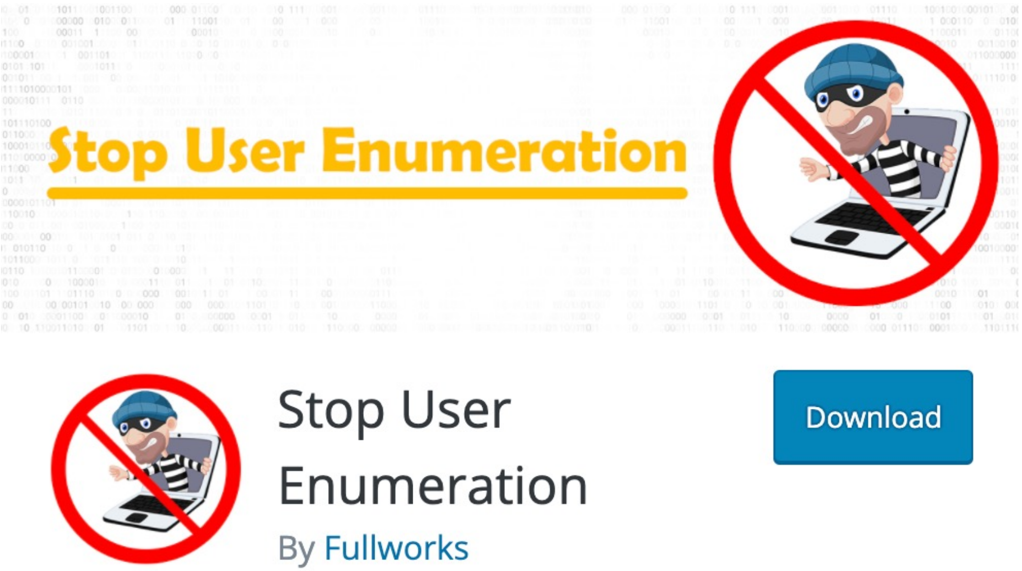
- If you give a bot a list of users then it can try hacking into each account. Your security is only as strong as its weakest link
- Unfortunately, WordPress makes it easy for bots to discover usernames
- User enumeration means that queries like:
  `https://example.com/?p=123`
  will redirect to something containing the username:
  `https://example.com/author/steve`

Accounts: Block user enumeration

- There are a few plugins that will stop this from happening

- We use “Stop User Enumeration”

- Just install and activate and it’ll start work straight away



Stop User Enumeration

By Fullworks

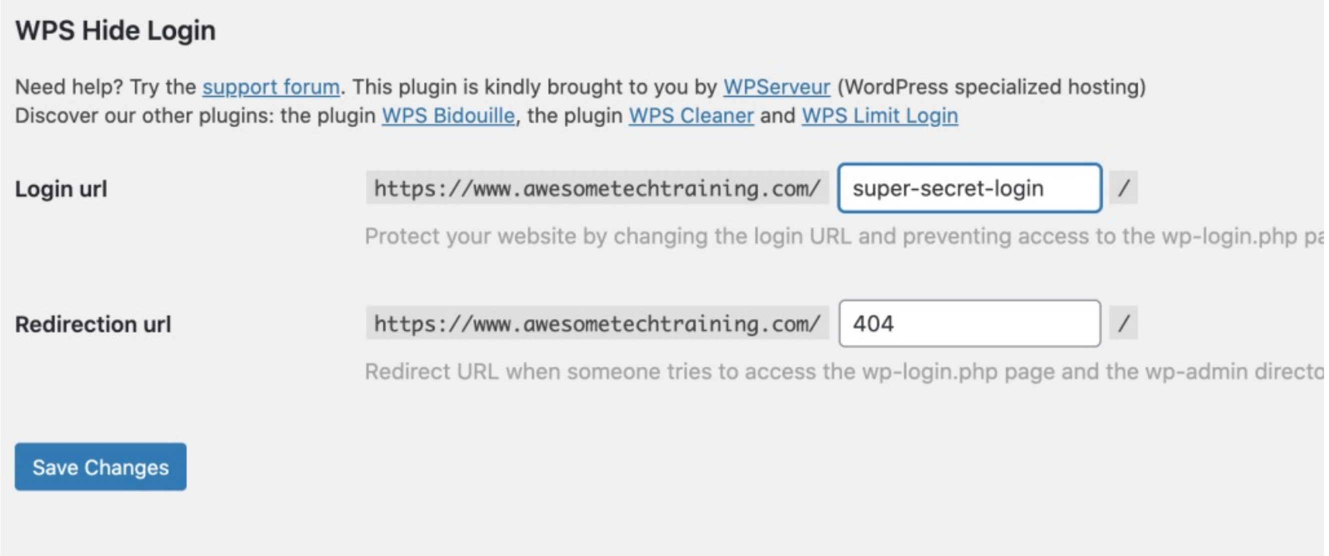
Accounts: Change the login URL

- Another way to deflect bots is to change where you log in
- If you check your web logs you’ll see many POSTs to wp-login.php, these are bots trying to gain access or test passwords
- Move the login to somewhere different and the bot won’t be able to work and will move on to another site
- REMEMBER – make a note of the new login URL. You’re stuck if you can’t remember it!

```
access.log:89.16.x.x - - [18/Apr/2023:02:25:15] "POST /wp-login.php HTTP/1.1" 200 12661 "-"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)" "log=admin&pwd=password&wp-submit=Log+In"
access.log:89.16.x.x - - [18/Apr/2023:02:26:16] "POST /wp-login.php HTTP/1.1" 200 12661 "-"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)" "log=admin&pwd=password1&wp-submit=Log+In"
access.log:89.16.x.x - - [18/Apr/2023:02:27:16] "POST /wp-login.php HTTP/1.1" 200 12661 "-"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)" "log=admin&pwd=password123&wp-submit=Log+In”
```

Accounts: Change the login URL

- There are a few plugins that will can change the login URL
- We use “WPS Hide Login”
- Very easy to configure:



WPS Hide Login

Need help? Try the support forum. This plugin is kindly brought to you by WPServeur (WordPress specialized hosting)
Discover our other plugins: the plugin WPS Bidouille, the plugin WPS Cleaner and WPS Limit Login

Login url https://www.awesometechtraining.com/ super-secret-login /

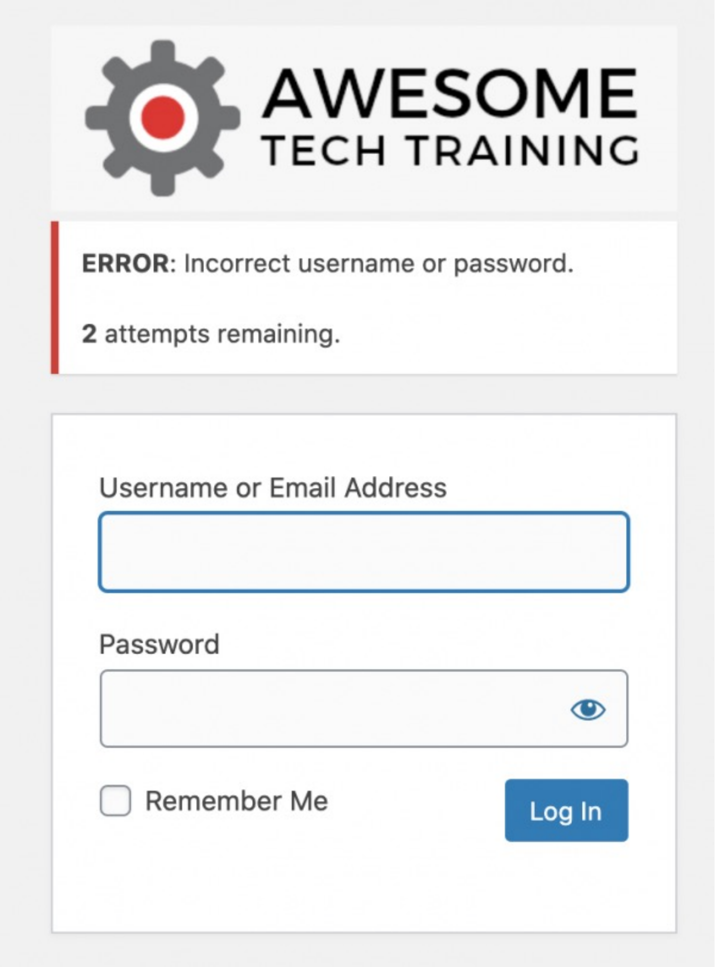
Protect your website by changing the login URL and preventing access to the wp-login.php pa

Redirection url https://www.awesometechtraining.com/ 404 /

Redirect URL when someone tries to access the wp-login.php page and the wp-admin directo

Accounts: Limit logins

- Don’t let bots, or people, try many login attempts
- We recommend the “Limit login attempts reloaded” plugin
- Another simple plugin
- This blog post has more information about these three plugins to help you protect your login page

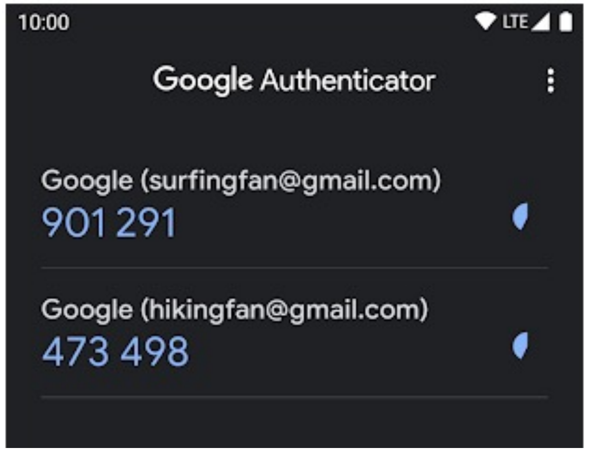


ERROR: Incorrect username or password.

2 attempts remaining.

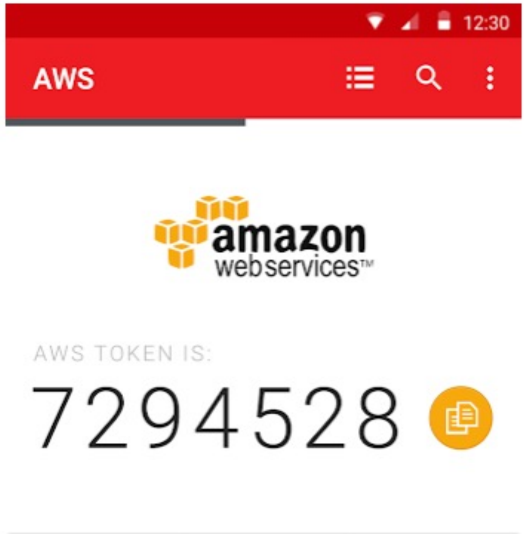
Accounts: Two factor authentication (2FA)

- You may have used two factor authentication for other sites or online banking
- You use a combination of your password and a unique code that is generated in an app or emailed to you to log in
- Apps:
  - Google Authenticator
    app store, play store
  - Authy
    app store, play store



Google (surfingfan@gmail.com)
901 291

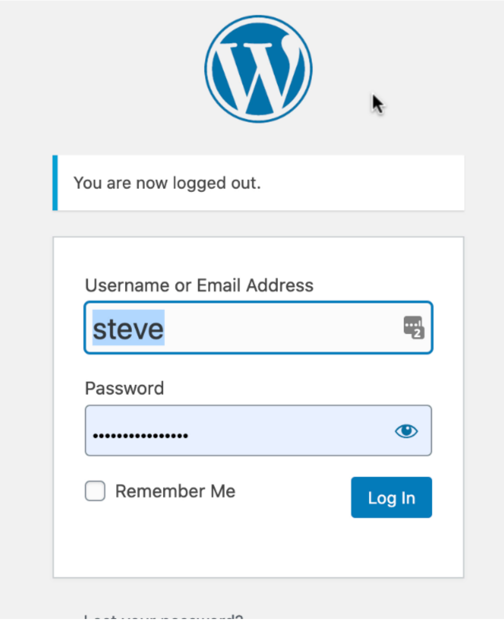
Google (hikingfan@gmail.com)
473 498



AWS TOKEN IS:
7294528

Accounts: Two factor authentication (2FA)

- We use the WP 2FA plugin
- This is a more complex configuration but is worth it for the extra security
- We have a blog post explaining how to set up two factor authentication

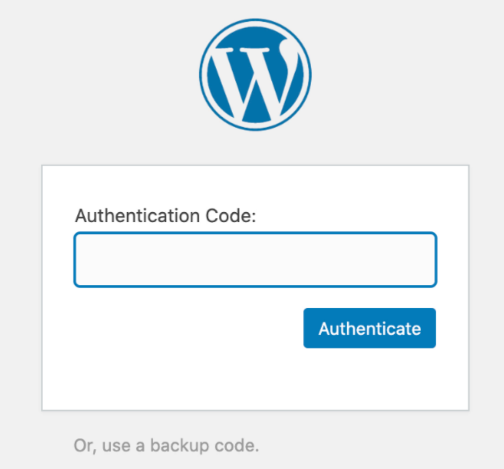


You are now logged out.

Username or Email Address: steve

Password: ••••••••••••••••

☐ Remember Me



Authentication Code:

Or, use a backup code.

Accounts: Who has access?

- Thinking about your internal security – who has access to what on your site?
- Consider the following:
  - Do users have the right role? Admin, Editor, Author, Contributor
  - Have some users left the organisation?
  - Do designers or other third party users still have access?
- Actions:
  - Delete old users
  - Grant appropriate permissions

Regular maintenance

- Regular maintenance doesn’t have to be a lot of work
- There are plugins that can automate the steps that you should be considering
- Don’t install and forget, the regular work should just be to cast an eye over everything and make sure they’re doing their job
- We’ll look at:
  - Remove unused themes and plugins
  - Use the latest versions of WordPress, plugins and themes
  - Regular backups

Maintenance: Remove unused code

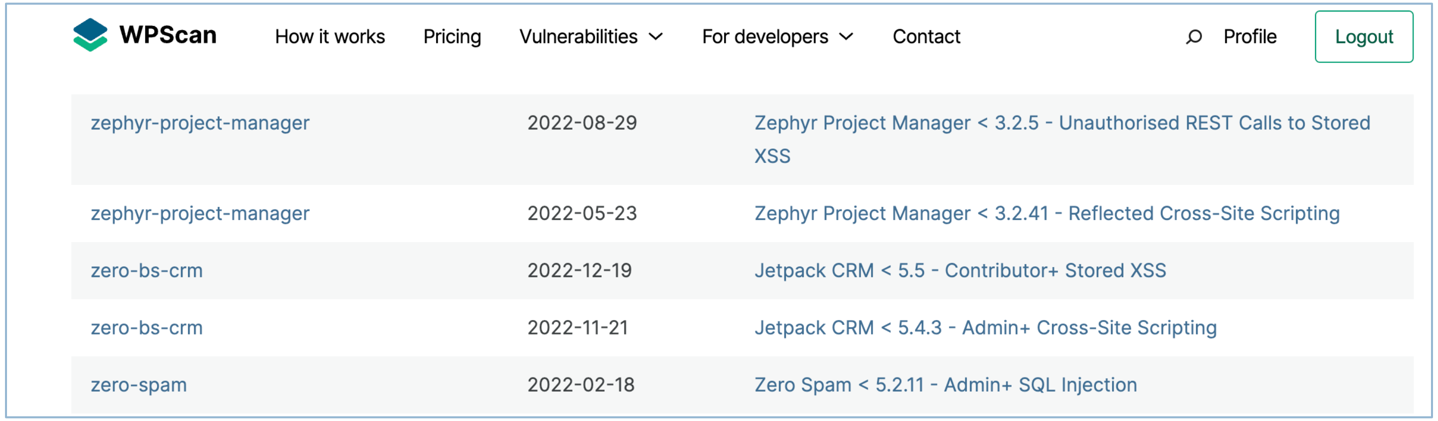
- Often admins will try out plugins, themes and constantly try new methods
- This can leave deactivated plugins and themes in your site

- Deactivated plugins and unused themes can be a security risk:
  - Less likely to be updated when there are security fixes
  - Vulnerable code could still be executed depending on the type of exploit

- Actions:
  - Review what plugins and themes are not being used
  - Remove all themes and plugins which are unlikely to be used in the near future

Maintenance: Keep everything updated

- Old code can contain many vulnerabilities
- The core WordPress code is regularly updated with many small releases and a regular large update every four months

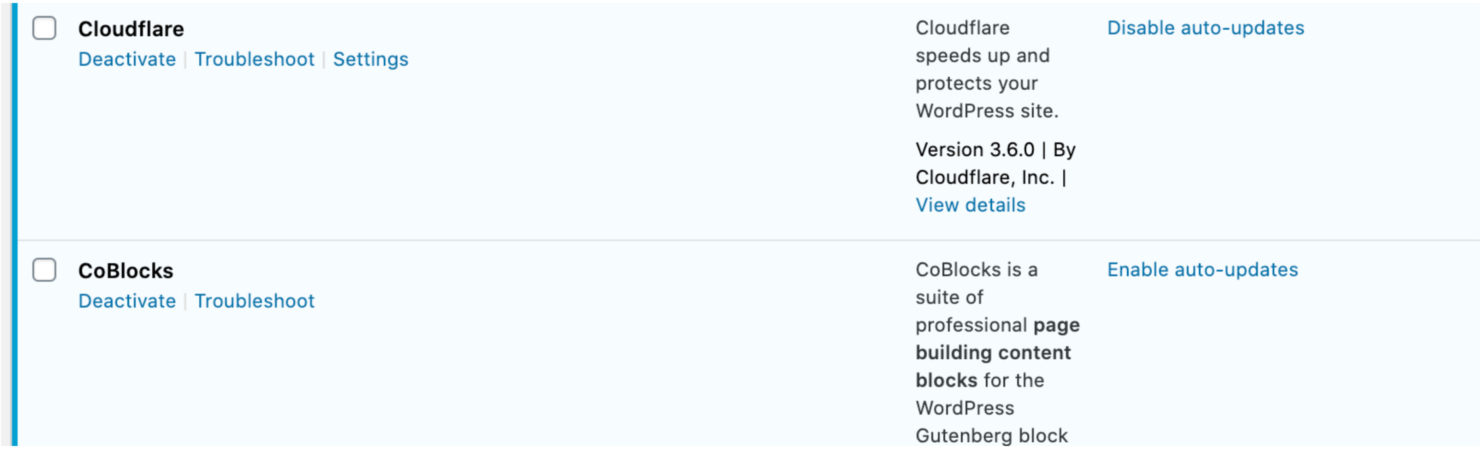


zephyr-project-manager	2022-08-29	Zephyr Project Manager < 3.2.5 - Unauthorised REST Calls to Stored XSS
zephyr-project-manager	2022-05-23	Zephyr Project Manager < 3.2.41 - Reflected Cross-Site Scripting
zero-bs-crm	2022-12-19	Jetpack CRM < 5.5 - Contributor+ Stored XSS
zero-bs-crm	2022-11-21	Jetpack CRM < 5.4.3 - Admin+ Cross-Site Scripting
zero-spam	2022-02-18	Zero Spam < 5.2.11 - Admin+ SQL Injection

- Many plugins and themes are regularly updated to introduce new features and fix security problems
- To protect your site and your data, you need to keep running the latest versions of the plugins

Maintenance: Keep everything updated

- Core WordPress Introduced an auto-update a few years ago
- Plugins and themes will now auto-update
- By default plugins don’t auto update, but one click will enable it
- Choose carefully which plugins should auto-update



□ **Cloudflare**
Deactivate | Troubleshoot | Settings

Cloudflare speeds up and protects your WordPress site.

Version 3.6.0 | By Cloudflare, Inc. | View details

Disable auto-updates

□ **CoBlocks**
Deactivate | Troubleshoot

CoBlocks is a suite of professional **page building content blocks** for the WordPress Gutenberg block

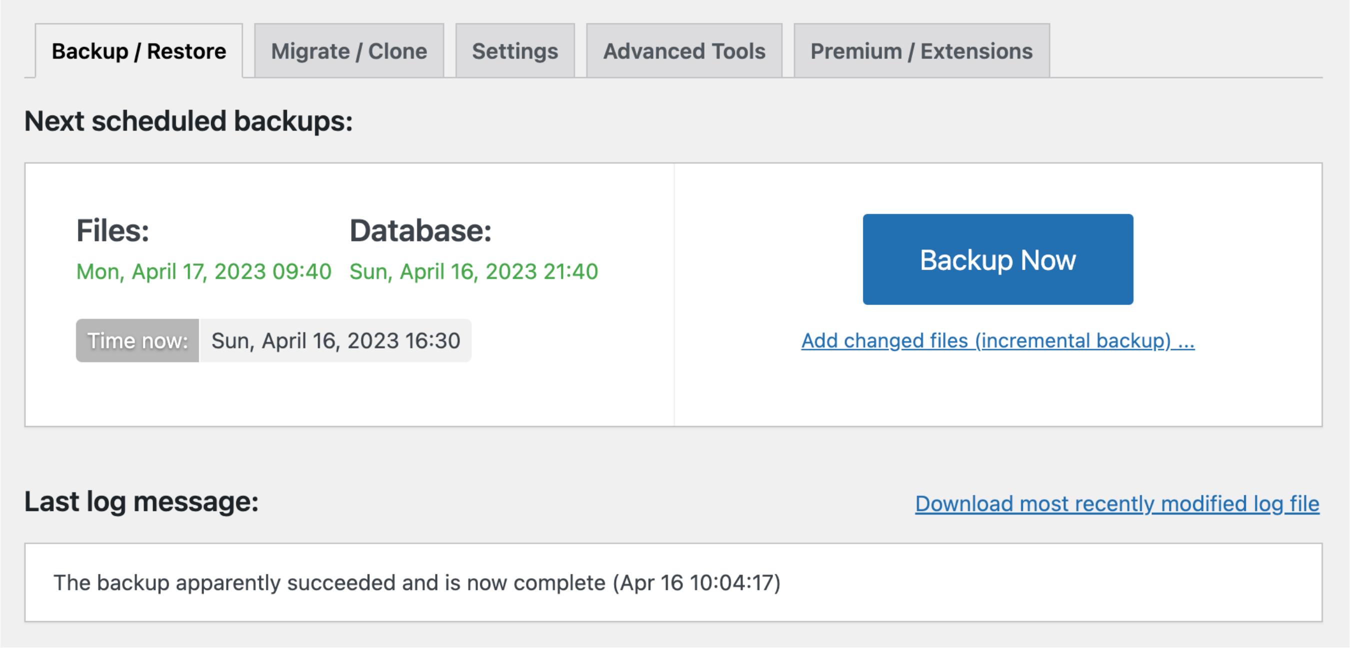
Enable auto-updates

Backups

- Why are backups so important for security?
  - They provide a safety net for when updating / changing your site
  - If your site gets hacked, you can revert to an earlier, clean version

Backups

- WordPress backups generally consist of two main parts: files and database
- Many ways to back up your site, lots of plugins
- We tend to use the UpdraftPlus plugin



Next scheduled backups:

Files: Mon, April 17, 2023 09:40

Database: Sun, April 16, 2023 21:40

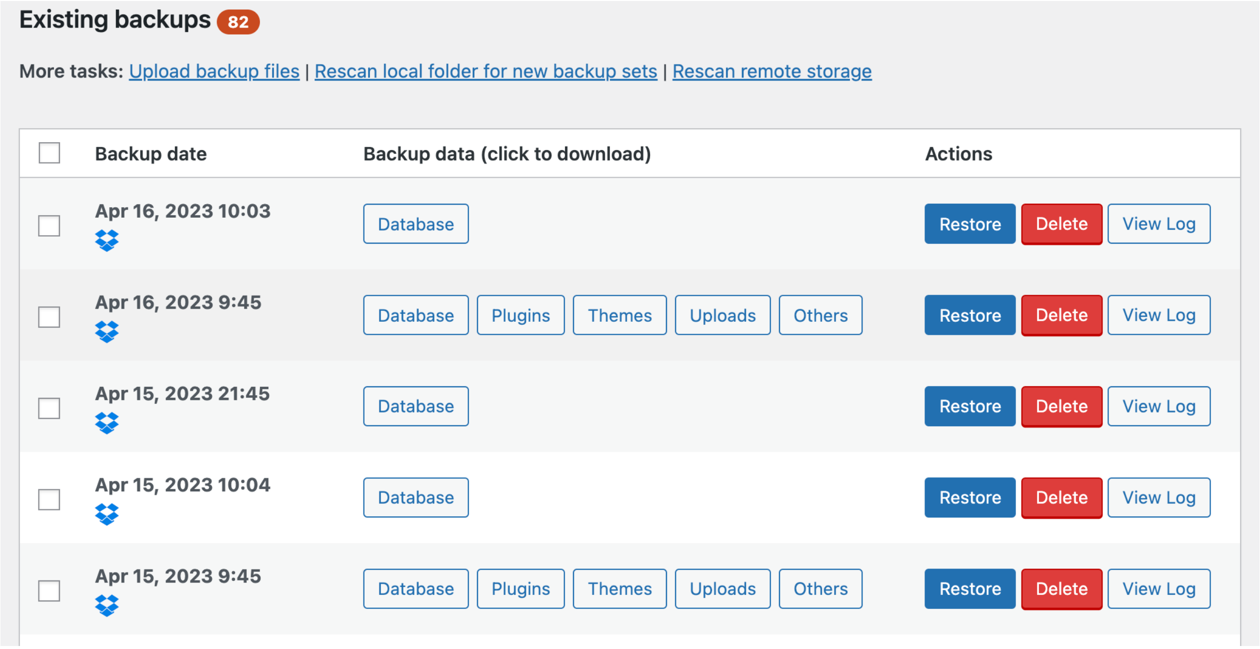
Time now: Sun, April 16, 2023 16:30

Last log message:

The backup apparently succeeded and is now complete (Apr 16 10:04:17)

Backups

- UpdraftPlus backups are easily automated
- Backups can be copied to cloud storage such as Dropbox
- Restoring is straightforward
- We have a video showing how to do this



Existing backups 82

More tasks: Upload backup files | Rescan local folder for new backup sets | Rescan remote storage

□	Backup date	Backup data (click to download)	Actions
□	Apr 16, 2023 10:03	Database	Restore Delete View Log
□	Apr 16, 2023 9:45	Database Plugins Themes Uploads Others	Restore Delete View Log
□	Apr 15, 2023 21:45	Database	Restore Delete View Log
□	Apr 15, 2023 10:04	Database	Restore Delete View Log
□	Apr 15, 2023 9:45	Database Plugins Themes Uploads Others	Restore Delete View Log

Change the database prefix

- When WordPress is first installed, the table names usually have a prefix of “wp_”

- This makes them easy for bots to find and manipulate

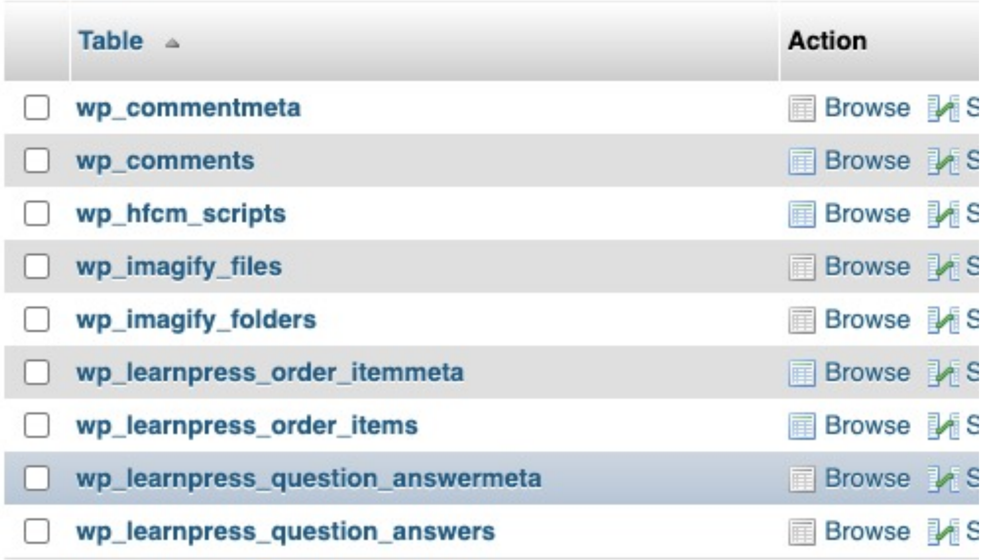
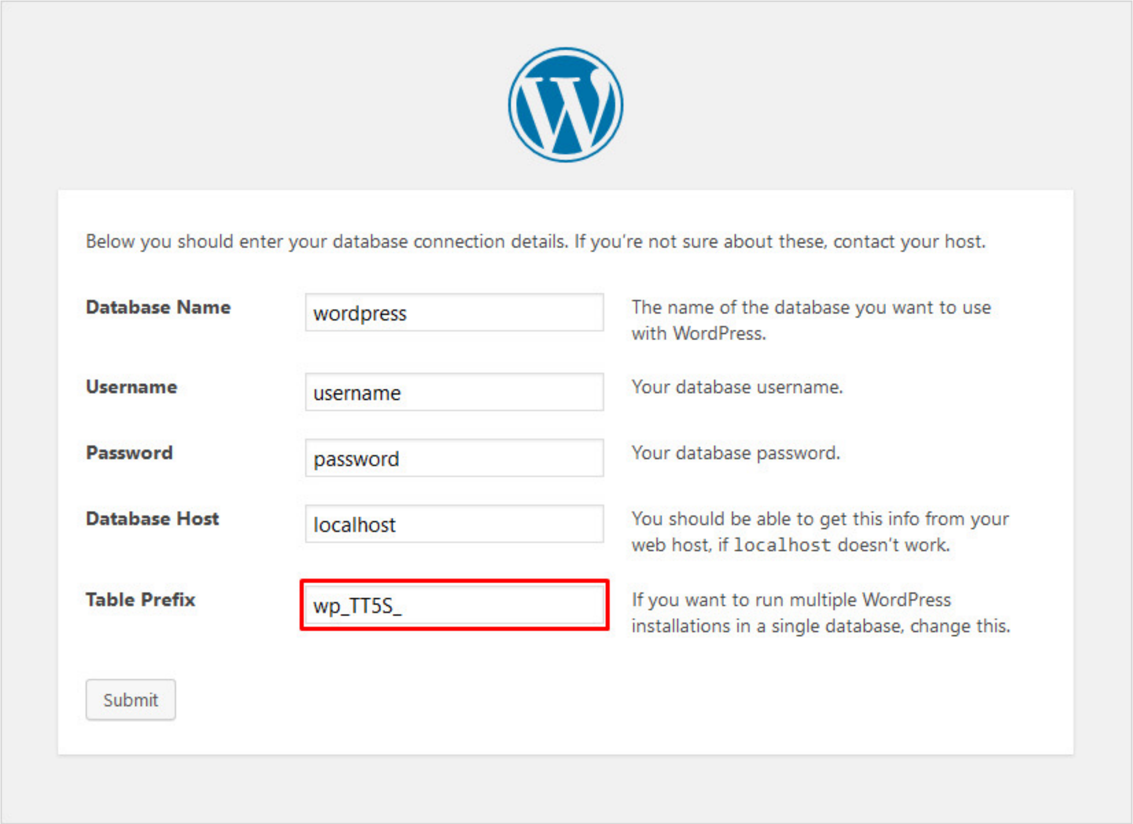


	Table ▲	Action
☐	wp_commentmeta	Browse S
☐	wp_comments	Browse S
☐	wp_hfcm_scripts	Browse S
☐	wp_imagify_files	Browse S
☐	wp_imagify_folders	Browse S
☐	wp_learnpress_order_itemmeta	Browse S
☐	wp_learnpress_order_items	Browse S
☐	wp_learnpress_question_answermeta	Browse S
☐	wp_learnpress_question_answers	Browse S

Change the database prefix

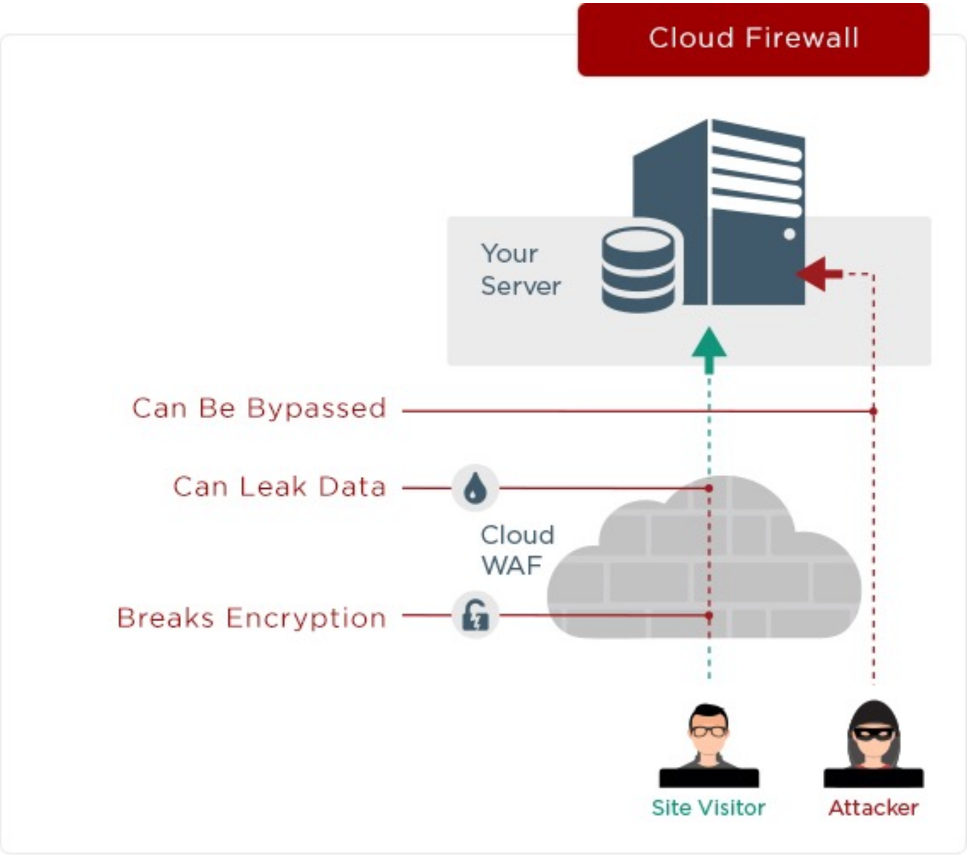
- If you’re building a new website from scratch with WordPress then consider changing the prefix when you are asked in the setup

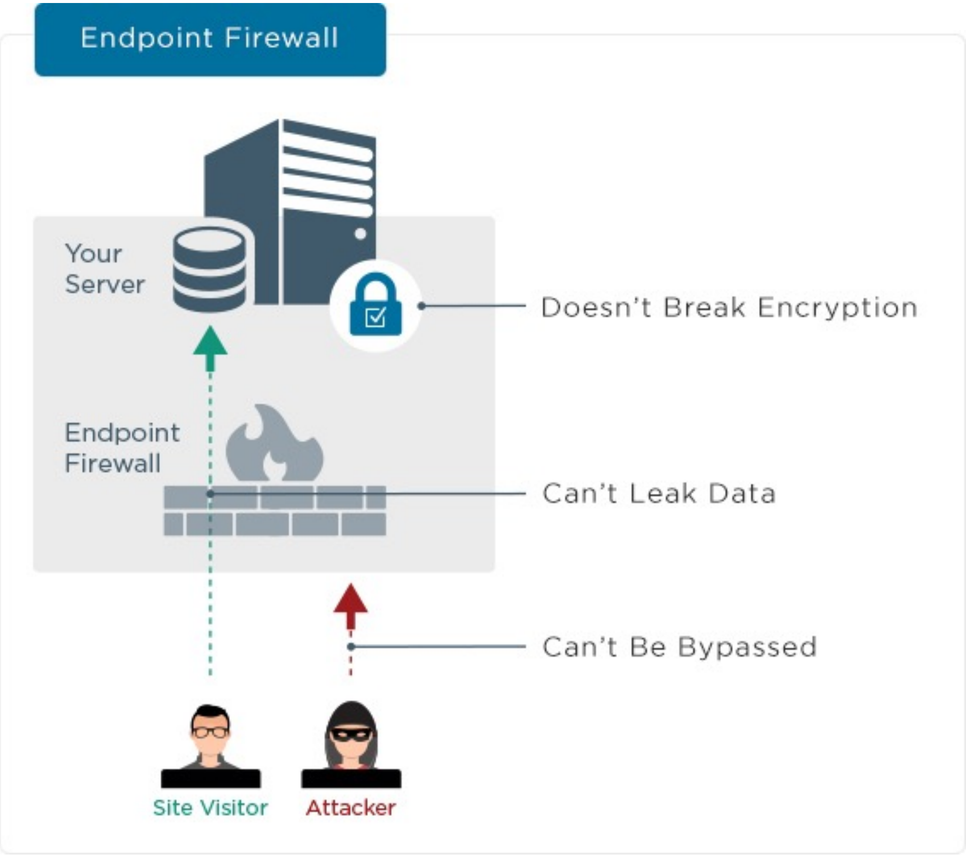


Below you should enter your database connection details. If you’re not sure about these, contact your host.

Database Name	wordpress	The name of the database you want to use with WordPress.
Username	username	Your database username.
Password	password	Your database password.
Database Host	localhost	You should be able to get this info from your web host, if `localhost` doesn’t work.
Table Prefix	wp_TT5S_	If you want to run multiple WordPress installations in a single database, change this.

WordFence – security plugin





From https://www.wordfence.com/

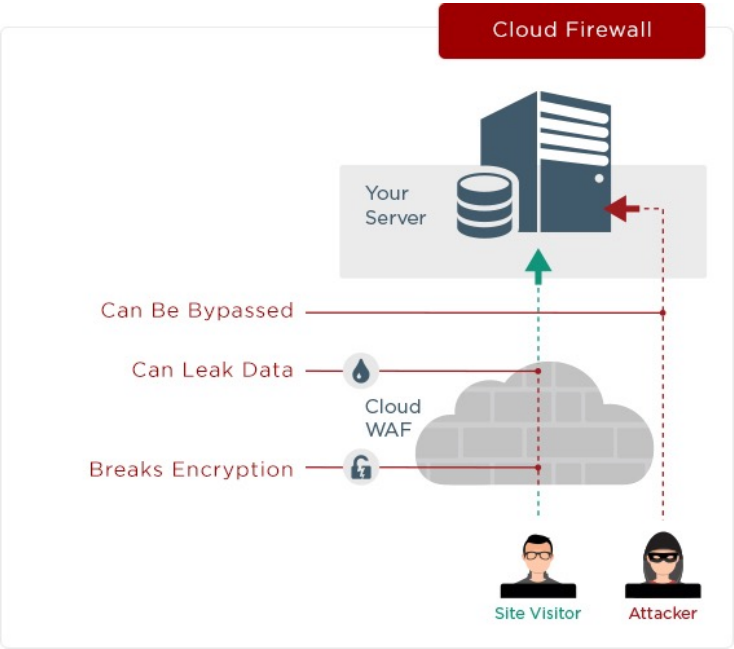
WordFence features

- WAF – web application firewall
- Checks core WordPress files for changes
- Block IP ranges and countries
- Blocks attacks like SQL injection or other well known vulnerabilities
- Email alerts when attacks are detected

- Note – some hosting companies will not let you install WordFence (eg. WPEngine) because of the performance hit

Cloud CDNs / firewalls

- Content Delivery Networks such as CloudFlare can hide and protect your site
- You need to use rules on your hosting to restrict access (usually a .htaccess file)
- It can completely hide how your site is hosted



Cloud CDNs / firewalls

- Cloud based firewalls can recognise malicious attacks and stop them before they reach your server
- Many understand WordPress and can be configured to protect against attack
- They also improve the speed of your site
- They can protect from a denial of service attacks (DDoS)

What to do if you get hacked

How do you know you’ve been hacked?

- Some of the tell-tale signs:
  - Your site redirects to a different web page
  - New text appears on your site, usually links
  - The site might start going slower or things stop working
  - You can’t log in
  - Google shows a warning
  - People complain about spam emails from your site
  - Your site slows down

What to do?

- Give yourself time – enable a “maintenance mode” plugin – try the WP Maintenance Mode plugin
- If you have a clean backup then restore that
- Update all plugins, themes and core WordPress
- Reinstall any plugins that are already at newest version (uninstall and reinstall, or FTP or use the wp command line)
- Use an FTP program or your hosting file browser to replace your .htaccess file
- If Google warning, then inform Google via Search Console that your site is clean again

What if you can’t log in?

- If you have a backup, then restore it – your old credentials will work after the restore
- Check if the problem is a PHP error (you’ll usually get a PHP error message)
- Try resetting the password using the “forgot my password” link

For the more technical:

- If you can log into your hosting on the command line, try using the “wp” command if installed:

```
wp user update <username> --user_pass=<new_password>
```

- If you can access the database using something like phpMyAdmin, then reset the password. The command is:

```
UPDATE wp_users
SET user_pass = MD5('new_password’)
WHERE user_login = 'your_admin_username';
```

Next steps

- Review your site
- Focus on big, quick wins:
  - Secure your accounts
  - Review users
  - Make sure you have regular backups (yourself, or via your hosting)
  - Check your code and plugins are up to date
- We can help consultancy and training – contact us

How we can help

- WordPress training options
  - Free WordPress resources
  - One-to-one tailored WordPress training for you / your team
  - Getting started with WordPress – we hold regular webinars introducing WordPress
  - Half hour free ‘surgery’ session to discuss your business
  - Ongoing help with WordPress maintenance / support / site development
- Free resources
  - Written checklist
  - SEO guide
  - Video library
- Other webinars
- 20% off other webinars for webinar attendees – quote code webinar20 at checkout

Other training and consulting

- Help configuring your Google Analytics account – contact us for more info
- Digital marketing audit – contact us for more info
- Website development – contact us for more info
- Website health-check or full technical review – contact us for more info
- Ongoing marketing support, advice and technical resource – contact us for more info

Questions

If you found this webinar useful we would love it if you would write us a review!

Scan this QR code to leave us a Google review

info@awesometechtraining.com

www.awesometechtraining.com