Beginner WordPress Security
Tips to Help Secure Your WordPress Site

WordCamp Oklahoma City, 2016
#WCOKC
Gerroald Barron
gerroald@ithemes.com - @gerroald
https://profiles.wordpress.org/gerroald
Why Would Someone Want to Hack My Site?
There are currently over 1 Billion websites on the web.

WordPress powers about 25% of them.

https://sucuri.net/website-security/website-hacked-report
You’re likely not the target, WordPress is.
In most instances, the compromises analyzed had little, if anything, to do with the core of the CMS application itself, but more with improper deployment, configuration, and overall maintenance by the webmasters and their hosts.

**Infected Websites Platform Distribution Q1 - 2016**

- **WordPress**: 78%, 8900
- **Joomla!**: 14%, 1600
- **Undefined**: 6%, 700
- **Magento**: 5%, 600
- **Drupal**: 2%, 200
- **vBulletin**: 0.02%, 20
- **ModX**: 0.01%, 12
It’s not about if you get attacked, but rather how to prevent it from being successful.
If you know your passwords, they’re likely too weak.
Two-Factor Authentication

Two-Factor Authentication is not a mere nuisance, it’s Real Security.
Changing the Salts

Salted Keys further protect your login credentials stored in your cookies.

https://api.wordpress.org/secret-key/1.1/salt/
Secure File Permissions

How secure is your site if anyone can view or write to your server files? It’s not. Secure file permissions are a must.

Never Use 777!
Using sFTP Encryption vs FTP

The sFTP and FTP protocols both transfer data; that’s where their similarities end.
FTP stands for File Transfer Protocol

FTP transfers data between two remote connections in plain text.

sFTP stands for SSH File Transfer Protocol

sFTP ensures that data is securely transferred privately with use of the SSH2 protocol.
SSL (Secure Sockets Layer)

What is it? Why should I use it?
SSL creates an encrypted connection between your web server and your visitors' web browser.
HTTP stands for Hyper Text Protocol

When using HTTP to transfer information, it’s relatively easy for a knowledgable person to intercept and view it.

HTTPS stands for Hyper Text Protocol Secure

When using HTTPS, if anyone is able to intercept it, they still won’t be able to decipher it because it’s encrypted.

SSL

Secure Socket Layers is the security used during the transfer while using HTTPS.

https://letsencrypt.org/
In most instances, the compromises analyzed had little, if anything, to do with the core of the CMS application itself, but more with improper deployment, configuration, and overall maintenance by the webmasters and their hosts.

**Infected Websites Platform Distribution Q1 - 2016**

- **WordPress**: 78%, 8900
- **Joomla!**: 14%, 1600
- **Undefined**: 6%, 700
- **Magento**: 5%, 600
- **Drupal**: 2%, 200
- **vBulletin**: .02%, 20
- **ModX**: .01%, 12

Horizontal bar chart showing the distribution of infected websites by platform.
Maintenance

Keep WordPress Core up to date.

Keep your plugins and themes up to date.

Regularly update your passwords.

Remove plugins, themes and users that aren't being used.

**ALWAYS** have a recent backup.
Summary

Use a strong password with the help of a password manager

Two-Factor for ALL THE THINGS

Regularly change your Salts

Use secure file permissions

Use sFTP when ever possible

Use SSL on all of your sites

Please keep your site and everything on it up to date