

SECURING WOOCOMMERCE

WITHOUT SCARING
CUSTOMERS



Rahul Nagare

Co-Founder, Nestify.io & ScaleDynamix
WordPress user since 2009
Ramen aficionado

@nginxreload

facebook

Email:

Password:

☐ Remember me

Login

Forgot Password?

facebook

Facebook is a **social utility** that **connects you** with the people around you.

Use Facebook to...

Keep up with friends and family

Share photos and videos

Control privacy online

Reconnect with old classmates

Find your Friends on Facebook

Search by Name

or [Use the Friend Finder](#)

Sign up for Facebook

It's free and anyone can join.

Full Name:

Your Email:

New Password:

I am:

Select Sex: ▾

Birthday:

Month: ▾

Day: ▾

Year: ▾

Why do I need to provide this?


Sign Up

By clicking Sign Up, you are indicating that you have read and agree to the [Terms of Use](#) and [Privacy Policy](#).

Facebook © 2008 | [English](#) ▾

[About](#) [Find Friends](#) [Advertising](#) [Developers](#) [Terms](#) [Privacy](#) [Help](#)

Phishing

 Scale Dynamix

Slides: scaledynamix.com/WCPHX

Rahul Nagare | [@nginxreload](#)

Types of security

1. Invisible but effective
2. Intrusive and annoying







Create account

Your name

Email

Password

i Passwords must be at least 6 characters.

Re-enter password

Create your Amazon account

By creating an account, you agree to Amazon's
[Conditions of Use](#) and [Privacy Notice](#).

Already have an account? [Sign in](#) ▶

```
root@server: ~  
root@server:~# curl -I https://www.amazon.com  
HTTP/1.1 503 Service Unavailable  
Content-Type: text/html  
Content-Length: 2671  
Connection: keep-alive  
Server: Server  
Date: Mon, 11 Feb 2019 01:43:20 GMT  
Vary: Content-Type,Host,Cookie,Accept-Encoding,X-Amzn-CDN-Cache,User-Agent  
Last-Modified: Fri, 18 Jan 2019 21:39:11 GMT  
ETag: "a6f-57fc257719dc0"  
Accept-Ranges: bytes  
x-amz-rid: APS83VNBPJ2NSPVSJXS0  
X-Cache: Error from cloudfront  
Via: 1.1 e4b6271438d0996ea6650d16006bc05a.cloudfront.net (CloudFront)  
X-Amz-Cf-Id: yjhmhb0kSMAUqYJtRyjsBgr-F5KxhnGBT9a-xTW1eYGLYBvEaNf18Q==  
  
root@server:~#
```



```
root@server: ~  
root@server:~# curl -I https://www.ebay.com  
HTTP/1.1 302 Moved Temporarily  
X-Content-Type-Options: nosniff  
x-xss-protection: 1; mode=block  
x-frame-options: SAMEORIGIN  
Location: http://pages.ebay.com/messages/page_not_found.html  
Content-Length: 0  
rlogid: undefined  
Strict-Transport-Security: max-age=31536000  
Date: Mon, 11 Feb 2019 01:44:55 GMT  
Connection: keep-alive  
  
root@server:~#
```

Sign In

Sign In to Your Equifax account

User Name:

Password:

[Forgot User Name or Password?](#)

Sign In



Password Tip

Your Password was specified when you first established your account.

Show all saved passwords

Emoji Win+Period

Undo Ctrl+Z

Redo Ctrl+Shift+Z

Cut Ctrl+X

Copy Ctrl+C

Paste Ctrl+V

Paste as plain text Ctrl+Shift+V

Select all Ctrl+A

Spellcheck ▶

Writing Direction ▶

Inspect Ctrl+Shift+I

Get More Out of Your Product

New and Existing Customers
Sign In and Configure Your Product

Features of your Equifax product offer
insights and powerful protection.

Sign in and configure all your Equifax
product's features to get the most value and
protection.

©2019 Equifax, Inc., All rights reserved. [Online Privacy Policy](#)

Equifax and the Equifax marks used herein are registered trademarks.

[Privacy of Rights](#) | [Ad Choices](#)



Products and services mentioned herein are the property of their respective owners.

```
root@server: ~  
root@server:~# curl -I https://www.equifax.com/personal/  
HTTP/1.1 200 OK  
Date: Mon, 11 Feb 2019 01:53:07 GMT  
Content-Length: 101155  
Content-Type: text/html; charset=UTF-8  
ETag: "0"  
X-Content-Type-Options: nosniff  
X-Frame-Options: SAMEORIGIN  
X-XSS-Protection: 1  
Liferay-Portal: Liferay Digital Experience Platform  
Set-Cookie: JSESSIONID=60C8BE60ABFCD8538A3C57928134DD95; Path=/; Secure; HttpOnly  
Set-Cookie: COOKIE_SUPPORT=true; Expires=Tue, 11-Feb-2020 01:53:07 GMT; Path=/; Secure; HttpOnly  
Set-Cookie: GUEST_LANGUAGE_ID=en_US; Domain=.equifax.com; Expires=Tue, 11-Feb-2020 01:53:07 GMT; Path=/; Secure; HttpOnly  
Set-Cookie: ApplicationGatewayAffinity=e82b65a6f1da1a860b72d678f4f3e4218635930ef3b5ef9ddbfe0cc0a9099597; Path=/; Domain=www.equifax.com  
Set-Cookie: TS01b82cf0=01e7cb8be3ae82c55f6d94c6fb4b610f74849c0ac9c52e71ef51db48b2c3c23ee1b7e8a30679eee7c8367c00b18b31c032d00f47b98e5dd341909d568ce4051f538f88d6993369e9ea09385155505247c406694c86c4179866be8c07a092fc39abb5e35ecdce783a407b5a6d5798db8c9778c1d495; Path=/; Domain=.equifax.com; Secure; HTTPOnly  
root@server:~#
```

Difference between WordPress and WooCommerce security

1. What happens when a WordPress site gets hacked?
2. What happens when a WooCommerce site gets hacked?

Doesn't my host take care of this?

Host will usually:

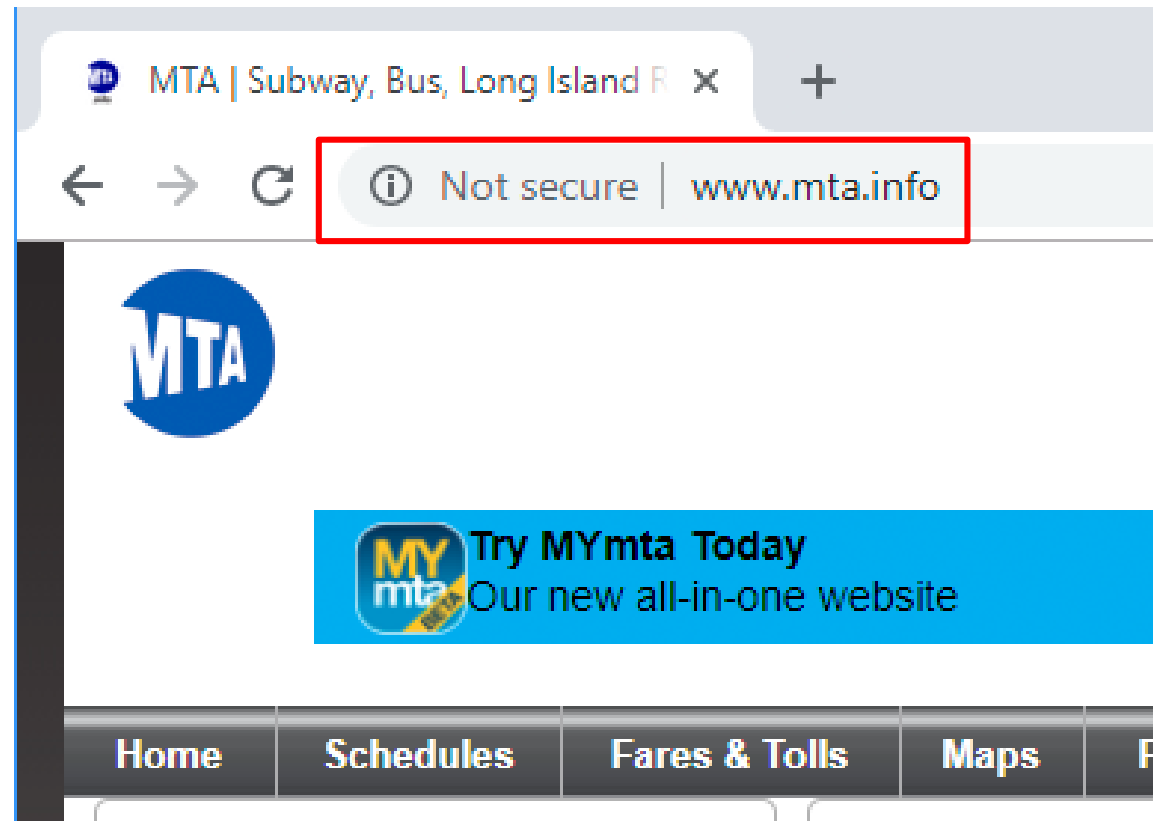
- ✓ Update WordPress core, maybe plugins
- ✓ Protect from brute force and DDoS attacks
- ✓ Maybe block malware

Host can not:

- ✗ Protect against poorly coded plugins or themes
- ✗ Protect against Weak password / Stolen laptop / Stolen phone
- ✗ Protect against human error

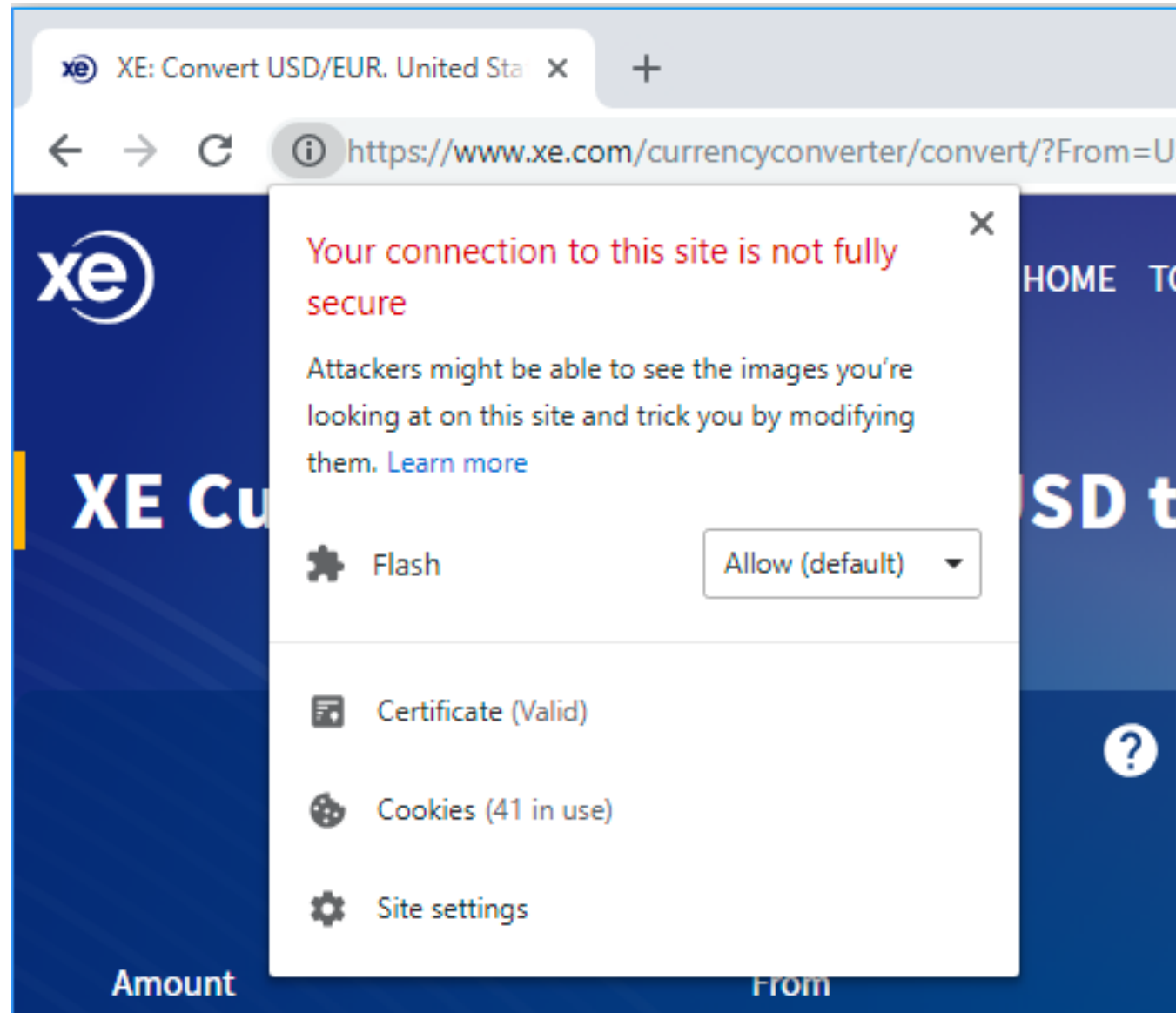
Which security issues affect conversions?

- Lack of SSL



Which security issues affect conversions?

- Lack of SSL
- Mixed content warnings



Which security issues affect conversions?

- Lack of SSL
- Mixed content warnings
- Security plugins that slow down your site
- Aggressive captchas

Please prove that you are human.



Type the two words:

reCAPTCHA™
stop spam.
read books.

Word Verification



Type the two words:

reCAPTCHA™
stop spam.
read books.

Type the 2 words and press Continue

Continue

Which security issues affect conversions?

- Lack of SSL
- Mixed content warnings
- Security plugins that slow down your site
- Aggressive captchas
- Trigger happy firewalls
- Complex password policies

Sorry, but your password must contain an uppercase letter, a number, a hieroglyph, a feather from a hawk and the blood of a unicorn.

someecards
user card



Which security issues affect conversions?

- Lack of SSL
- Mixed content warnings
- Security plugins that slow down your site
- Aggressive captchas
- Trigger happy firewalls
- Complex password policies
- Emails that end up in spam

Securing WooCommerce

- Use a good hosting provider

Is my host any good?

Good Host will not:


- ❌ Ask last 4 characters of your password
- ❌ Show other users' data in your SFTP account
- ❌ Allow downloading .sql / .git / .tar.gz files without authentication

Securing WooCommerce

- Use a good hosting provider
- Use SSL. Use Really-simple-ssl plugin if there are mixed-content warnings
- Use strong passwords everywhere
- Use 2 Factor Authentication where available
- Offer 2 Factor Authentication to your customers using Auth0 / Google authenticator plugin
- Use invisible captcha (Use invisible-recaptcha or advanced-nocaptcha plugin)
- Use SMTP service like Sendgrid / Mailgun / Sparkpost / Mailjet

Securing WooCommerce Code

- Check if you are using any outdated plugins

 **WORDPRESS.ORG**

Search WordPress.org

Showcase Themes **Plugins** Mobile Support Get Involved About Blog Hosting


Get WordPress

Plugins

My Favorites Beta Testing Developers

Search plugins

This plugin hasn't been tested with the latest 3 major releases of WordPress. It may no longer be maintained or supported and may have compatibility issues when used with more recent versions of WordPress.



uWSGI Object Cache

By [Andrew Bevitt](#)

Download

Details

Reviews

Installation

Support

Development

Description

uWSGI Object Cache for WordPress.

WARNING: This requires a manual install.

GitHub repository: <https://github.com/andrewbevitt/uwsgi-object-cache>

Contributors & Developers

Version: 1.1

Last updated: 4 years ago

Active installations: Fewer than 10

WordPress Version: 3.5 or higher

Tested up to: 4.2.22

Tag: cache

Securing WooCommerce Code

- Check if you are using any outdated plugins
- Check functions.php for keywords like `eval()`, `exec()`, `base64_decode()`, `file_get_contents()`, `curl_exec()`
- Use wp-cli
 - `wp core verify-checksums`

wp core verify-checksums

```
# Verify checksums
$ wp core verify-checksums
Success: WordPress installation verifies against checksums.

$ wp core verify-checksums
Warning: File doesn't verify against checksum: wp-includes/version.php
Warning: File doesn't verify against checksum: readme.html
Warning: File doesn't verify against checksum: wp-config-sample.php
Error: WordPress installation doesn't verify against checksums.
```

Securing WooCommerce Code

- Check if you are using any outdated plugins
- Check functions.php for keywords like `eval()`, `exec()`, `base64_decode`, `file_get_contents()`, `curl_exec()`
- Use wp-cli
 - `wp core verify-checksums`
 - `wp package install markri/wp-sec`
`wp wp-sec check`

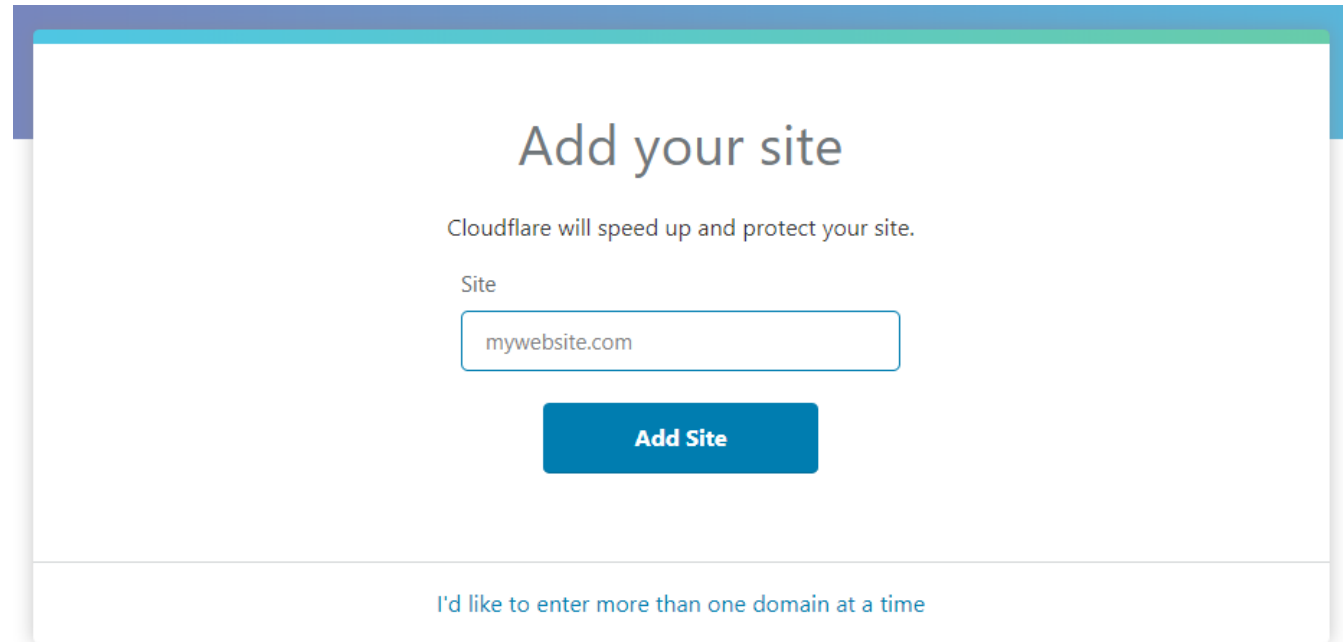
Blocking hackers before they reach your server

1. Cloudflare

2. Amazon WAF

3. Sucuri WAF

cloudflare.com



Add your site

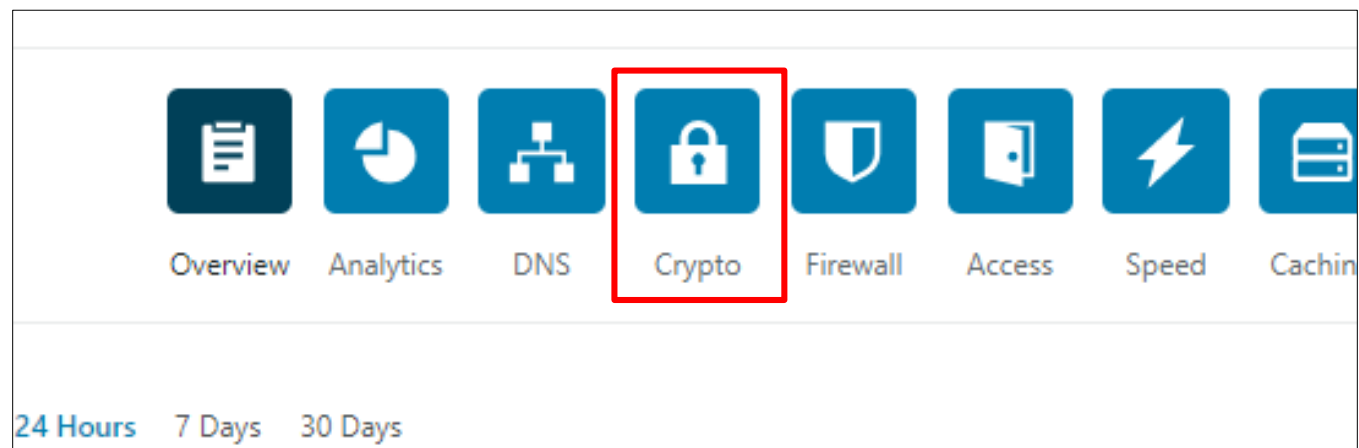
Cloudflare will speed up and protect your site.

Site

Add Site

[I'd like to enter more than one domain at a time](#)

Crypto Tab



SSL Mode: Full

SSL

Encrypt communication to and from your website [using SSL](#).

It may take up to 24 hours after the site becomes active on Cloudflare for new certificates to issue.

Universal SSL Status ● Active Certificate

This setting was last changed a few seconds ago

Full ▼

[API](#) ▶

[Help](#) ▶

Enable HSTS

HTTP Strict Transport Security (HSTS)

Enforce web security policy for your website.

Enable HSTS

[API ▶](#)

[Help ▶](#)



Your connection is not private

Attackers might be trying to steal your information from **192.168.100.40** (for example, passwords, messages, or credit cards).

[Hide advanced](#)

Reload

192.168.100.40 normally uses encryption to protect your information. When Chrome tried to connect to 192.168.100.40 this time, the website sent back unusual and incorrect credentials. Either an attacker is trying to pretend to be 192.168.100.40, or a Wi-Fi sign-in screen has interrupted the connection. Your information is still secure because Chrome stopped the connection before any data was exchanged.

You cannot visit 192.168.100.40 right now because the website uses HSTS. Network errors and attacks are usually temporary, so this page will probably work later.

NET::ERR_CERT_AUTHORITY_INVALID

Minimum TLS Version: 1.2

Minimum TLS Version

Only allow HTTPS connections from visitors that support the selected TLS protocol version or newer.

TLS 1.2 ▼

[API](#) ▶

[Help](#) ▶

Firewall Tab > Block known bots

Create Firewall Rule

Rule name

Give your rule a descriptive name

Known Bots

When incoming requests match...

Field

Operator

Value

Known Bots ×

equals

On

And

Or

Expression Preview

Edit expression

(cf.client.bot)

Then...

Choose an action

Block

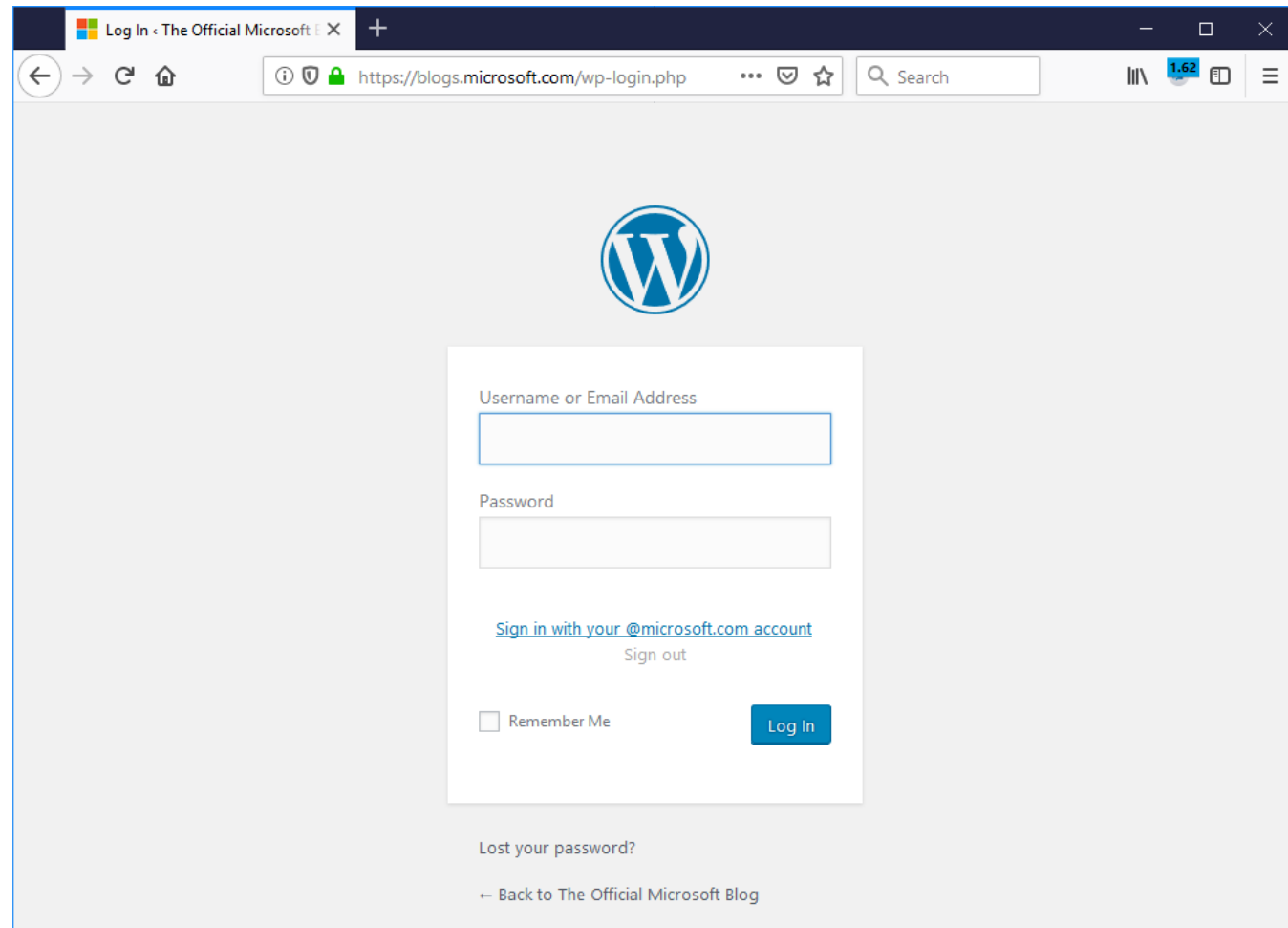
Cancel

Save as Draft

Save and Deploy

Things that are not very effective for security

1. Using robots.txt to block bots
2. Using plugins to hide wp-login page



Things that are not very effective for security

1. Using robots.txt to block bots
2. Using plugins to hide wp-login page
3. Using firewalls that block users after failed logins

Disaster recovery planning

I. Backups

Good Backup Strategy

1. Frequency
2. Destination
3. Verification

Disaster recovery planning

1. Backups
2. Printed copy of 2 factor authentication recovery codes
3. Better password hashing for WordPress

WordPress default password management

1. Uses MD5 algorithm
2. Converts 'password' to '5f4dcc3b5aa765d61d8327deb882cf99'
3. Can't convert '5f4dcc3b5aa765d61d8327deb882cf99' to 'password'
4. Sites like md5online.org turn '5f4dcc3b5aa765d61d8327deb882cf99' to 'password'

Improving WordPress password management

1. Use bcrypt algorithm to hash passwords
2. Bcrypt takes 0.1 seconds to generate hash per login attempt
3. Password guesses in one second

MD5: 1 Billion

Bcrypt: 100

Improving WordPress password management

1. Visit <https://github.com/roots/wp-password-bcrypt>
2. Download wp-password-bcrypt.php
3. Copy it to wp-content/mu-plugins

Resources

- haveibeenpwned.com (Have I been Pwned)
- wpvulndb.com
- blog.sucuri.net
- scaledynamix.com/blog
- wpmrr.com/podcast

Thank You!

Questions?