Scale Dynamix

SECURING WOOCOMMERCE

WITHOUT SCARING CUSTOMERS

Rahul Nagare

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

@nginxreload

Phishing

Types of security

1. Invisible but effective

2. Intrusive and annoying

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?
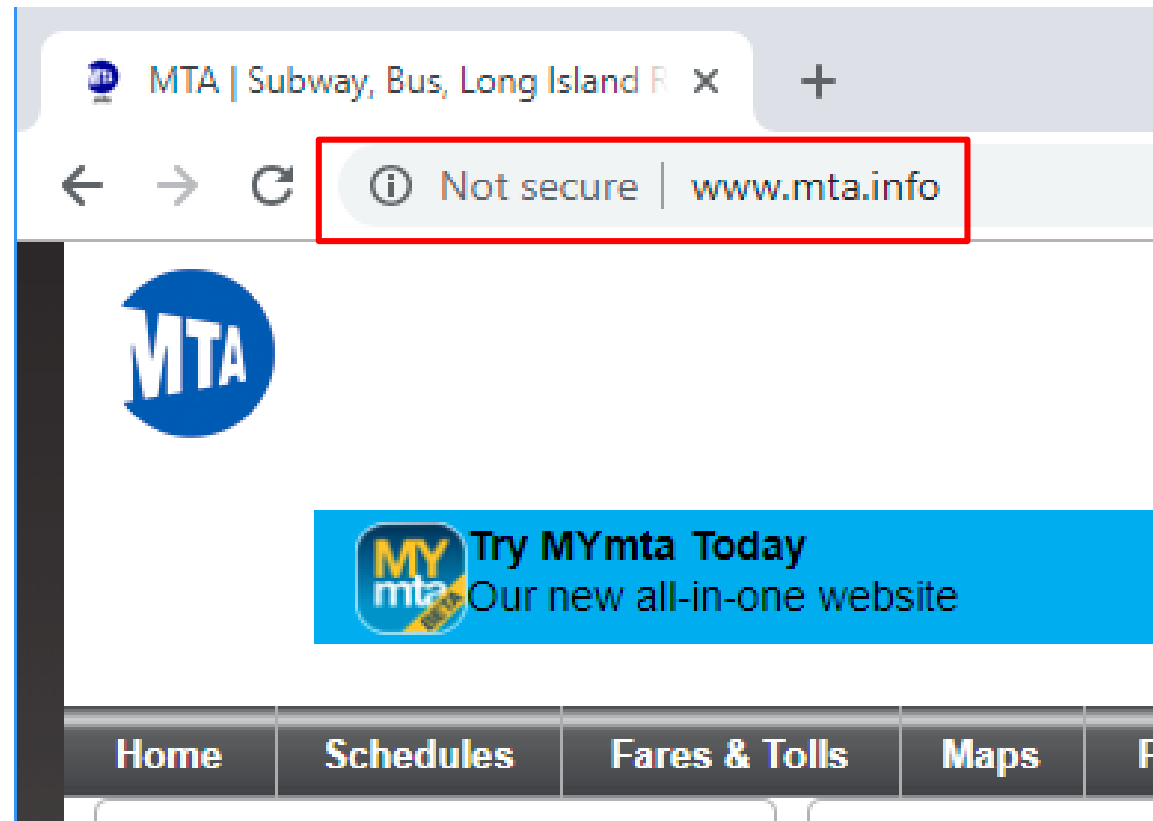
- Lack of SSL

Which security issues affect conversions?
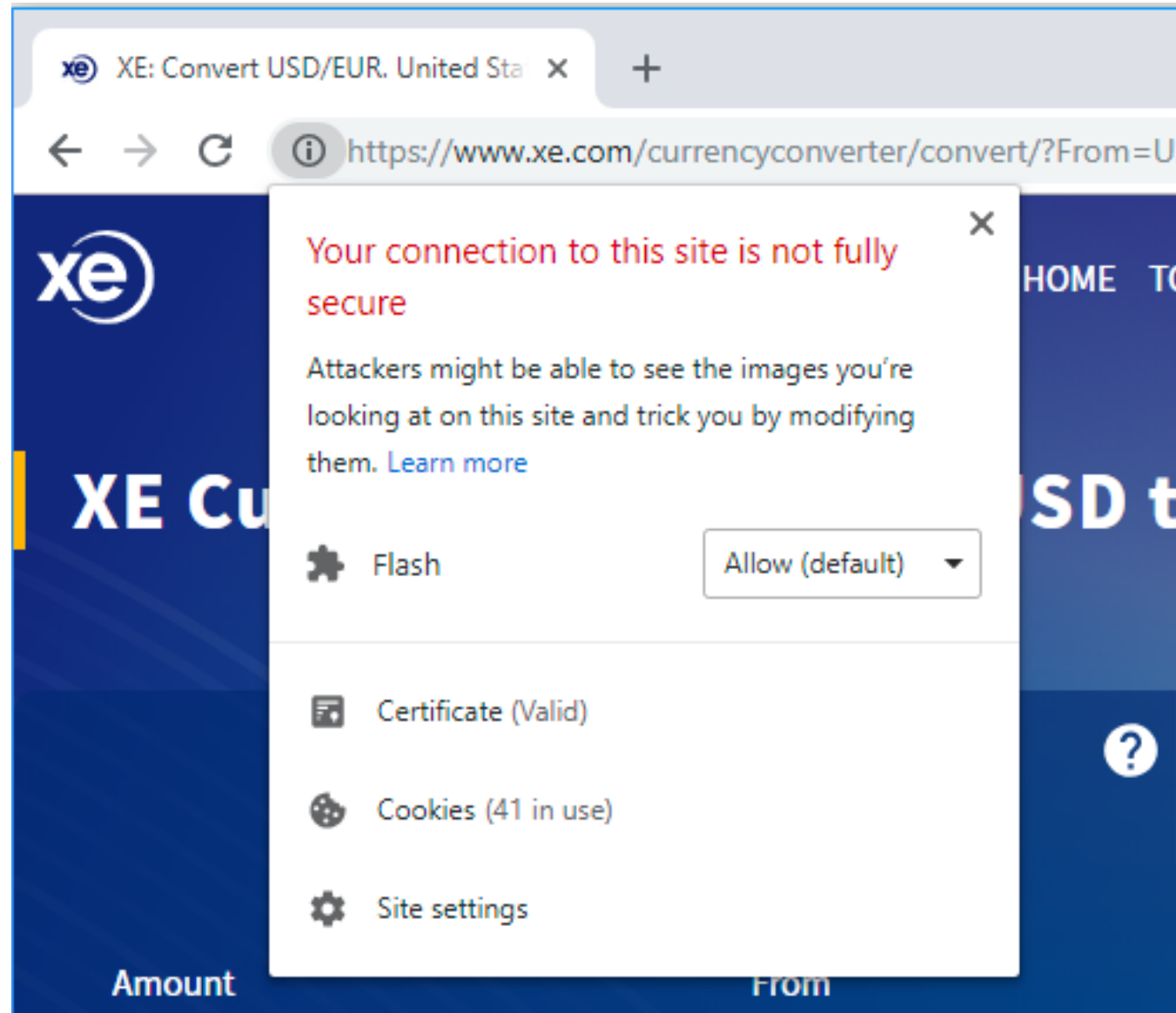
- Lack of SSL
- Mixed content warnings

Which security issues affect conversions?

- Lack of SSL

- Mixed content warnings

- Security plugins that slow down your site

- Aggressive captchas

Rahul Nagare | @nginxreload

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

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

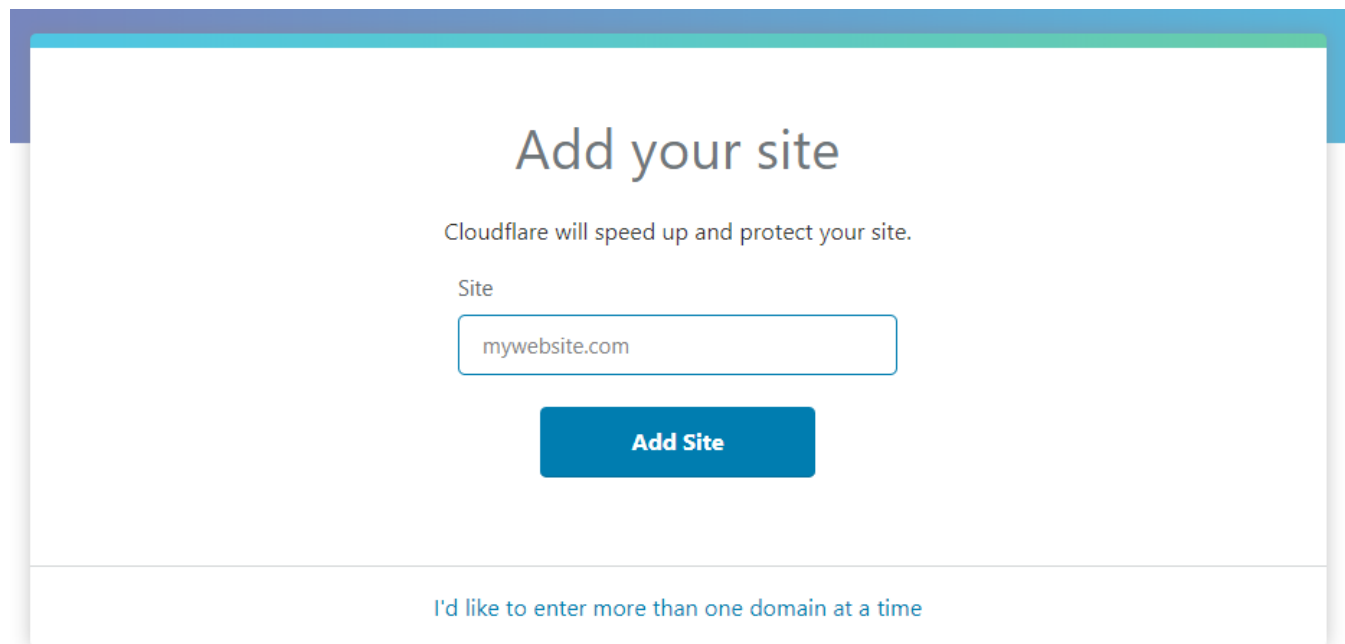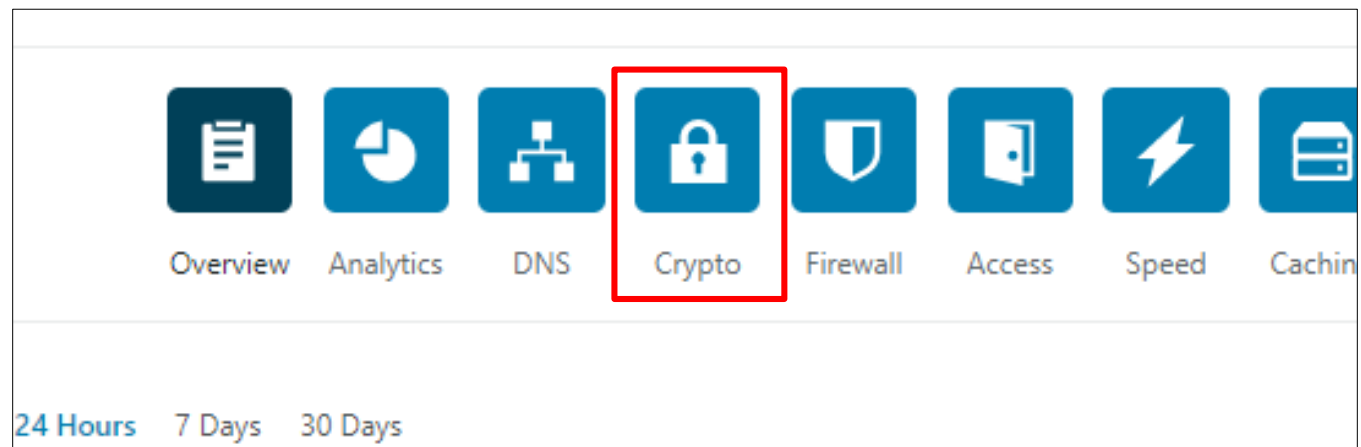# Blocking hackers before they reach your server

1. Cloudflare

2. Amazon WAF

3. Sucuri WAF

Rahul Nagare | @nginxreload

cloudflare.com

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 ▶

Minimum TLS Version: 1.2

Firewall Tab > Block known bots

Disaster recovery planning

1. Backups

Good Backup Strategy

1. Frequency

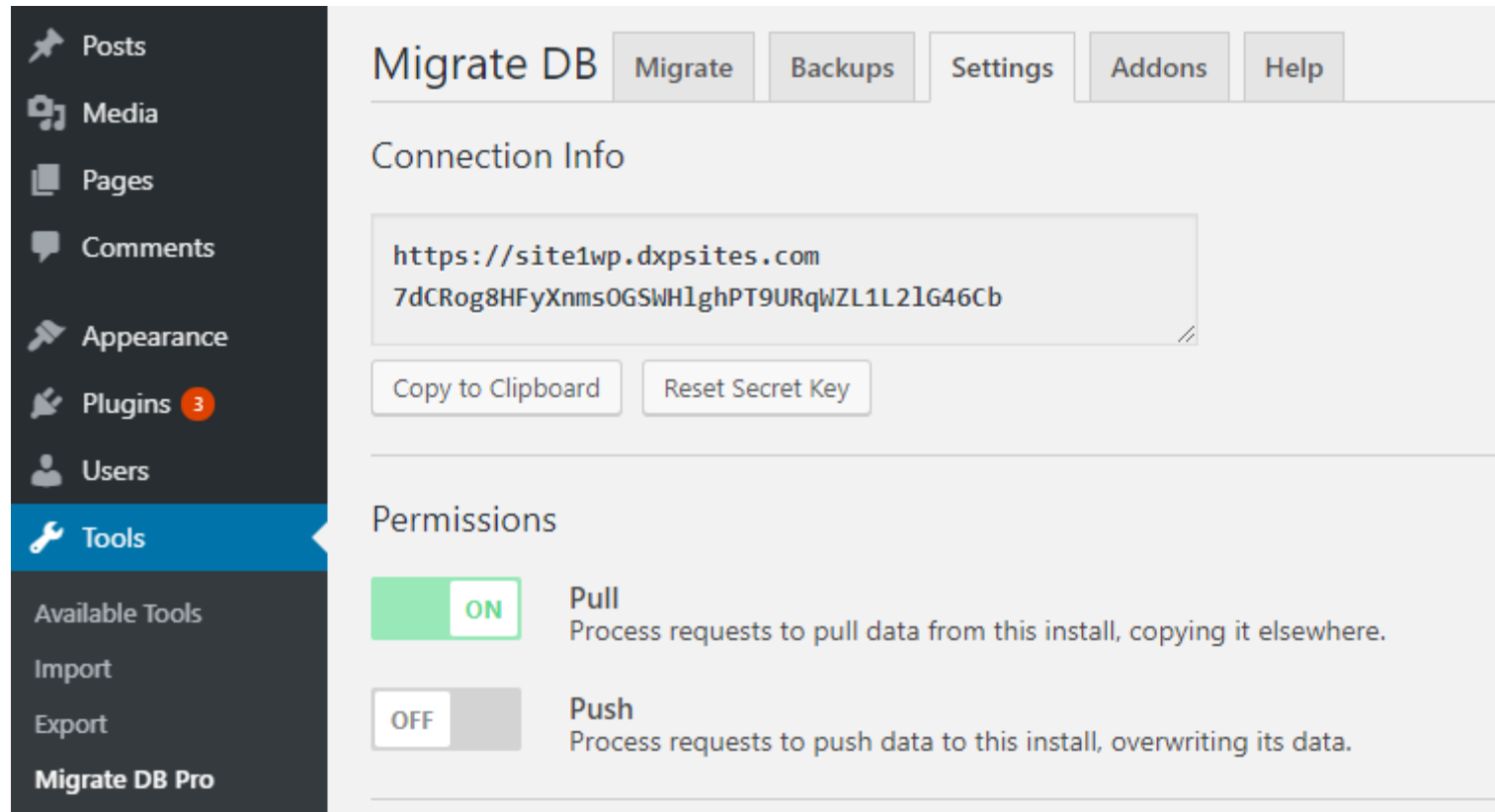2. Destination

3. Verification

Disaster recovery planning

1. Backups

2. Printed copy of 2 factor authentication recovery codes

3. Warm Standby

Creating a warm standby

1. Signup with another host using same domain name, restore latest site backup

2. Install and configure wp-migrate-db pro with wp-cli addon

wp-migrate-db pro

Creating a warm standby

1. Signup with another host using same domain name, restore latest site backup

2. Install and configure wp-migrate-db pro with wp-cli addon

3. Setup this cron job on new hosting account:

    `wp migratedb pull https://mysite.com [secret] --media=compare`

    `--preserve-active-plugins`

Rahul Nagare | @nginxreload

Using warm standby

1. Update DNS to point to new host

2. Done

Resources

- haveibeenpwned.com (Have I been Pwned)

- wpvulndb.com

- blog.sucuri.net

- scaledynamix.com/blog

Thank You!

Questions?