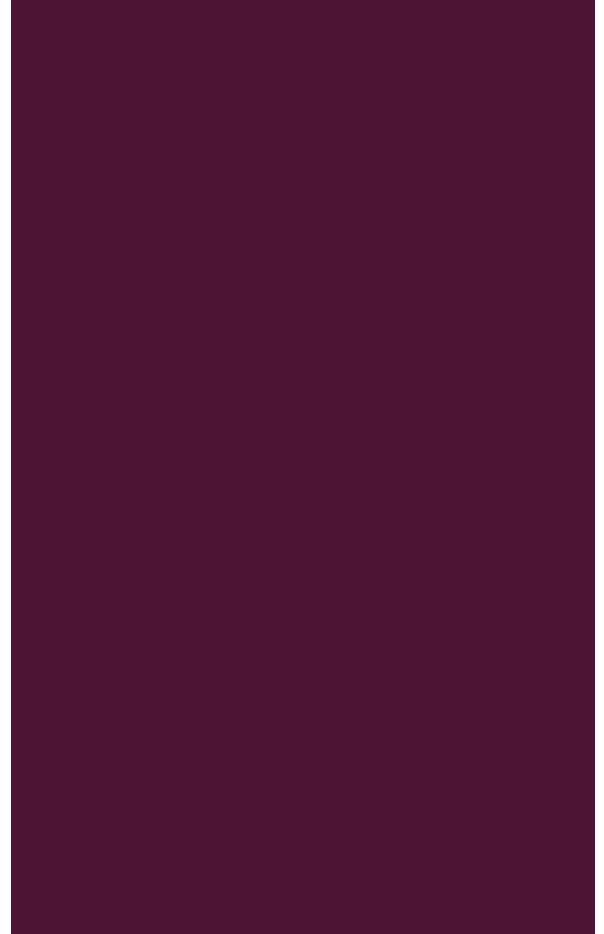


# Securing WordPress in the Age of 0-Day Vulnerabilities





# Rahul Nagare

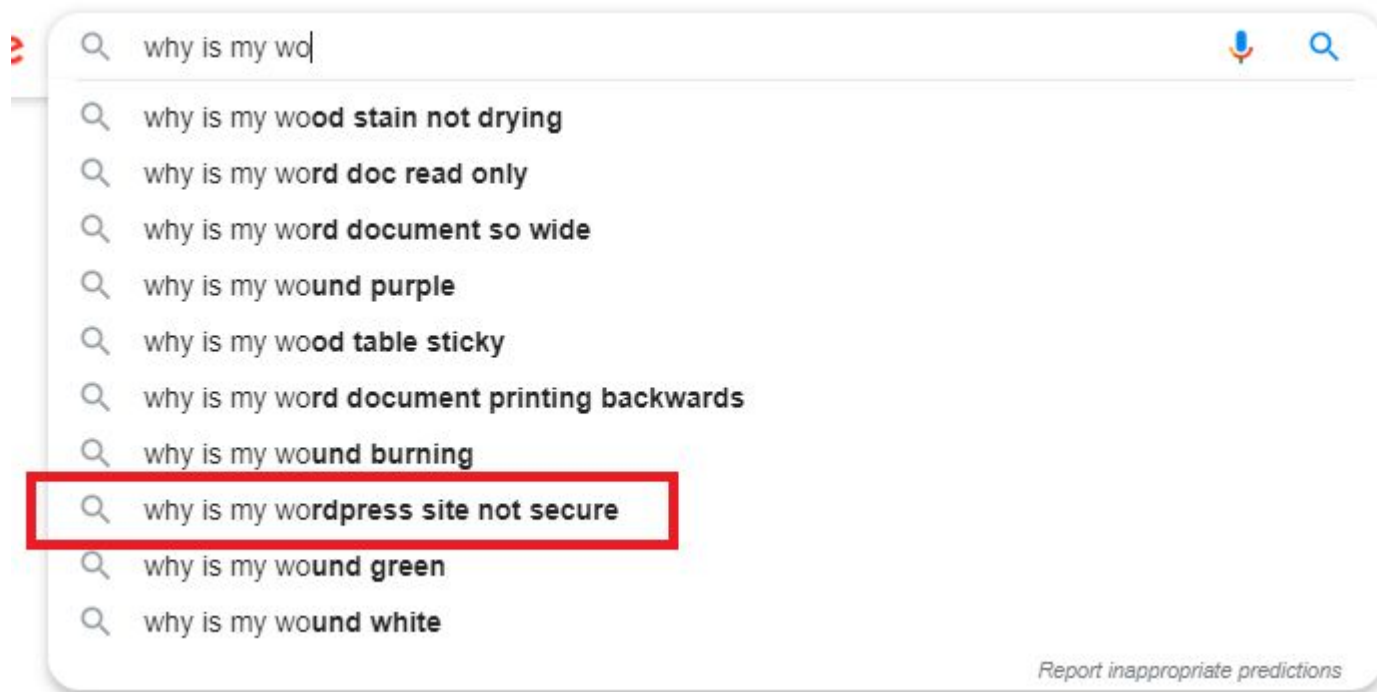
Co-Founder, Nestify & Scale Dynamix

WordPress user since 2009

Dog Person

@nginxreload

# WordPress: an attractive target for hackers

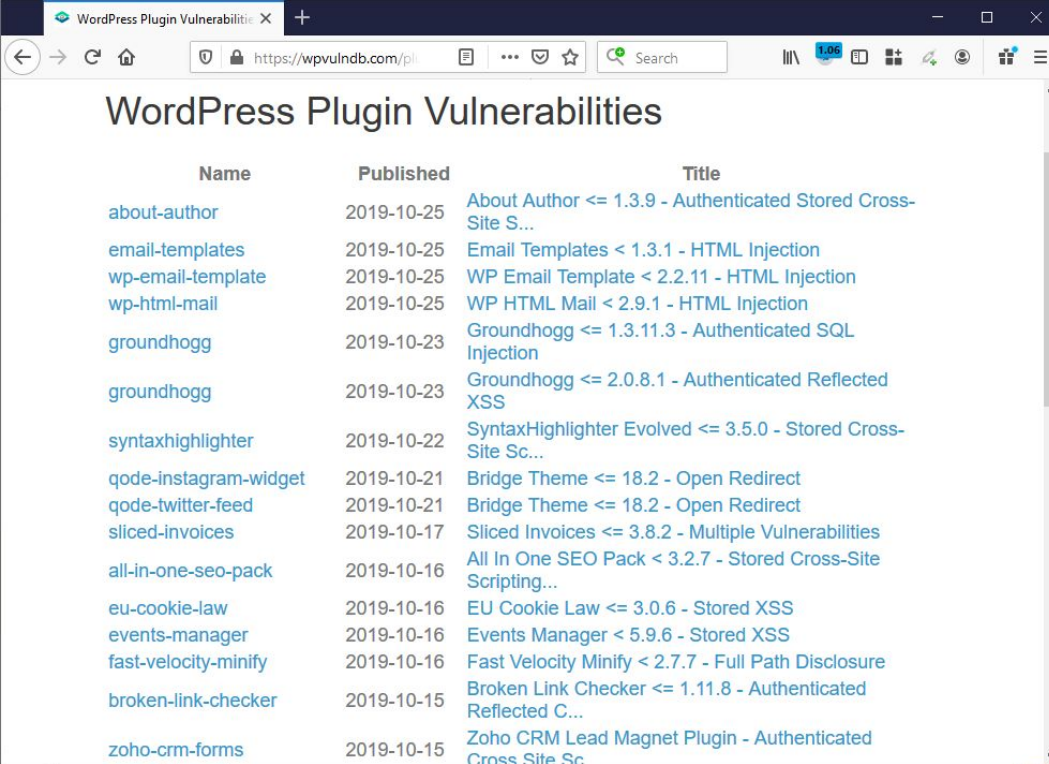


---

# 0-Day Vulnerabilities

- Recently discovered security issues in core, themes, or plugins
- Used by hackers (typically) in an automated manner
- Can also be introduced when installing updates
- Not just limited to free plugins

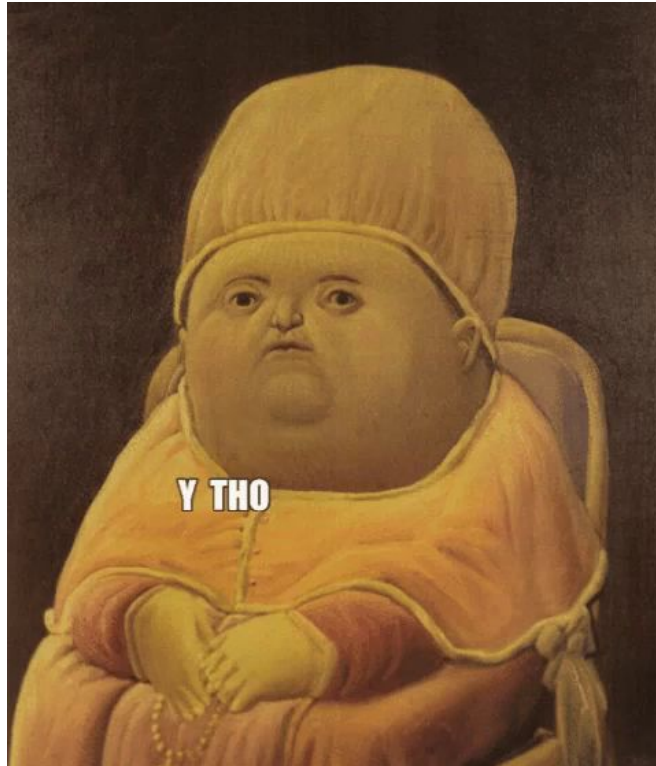
# wpvulndb.com/plugins



Name	Published	Title
<a href="#">about-author</a>	2019-10-25	About Author <= 1.3.9 - Authenticated Stored Cross-Site S...
<a href="#">email-templates</a>	2019-10-25	Email Templates < 1.3.1 - HTML Injection
<a href="#">wp-email-template</a>	2019-10-25	WP Email Template < 2.2.11 - HTML Injection
<a href="#">wp-html-mail</a>	2019-10-25	WP HTML Mail < 2.9.1 - HTML Injection
<a href="#">groundhogg</a>	2019-10-23	Groundhogg <= 1.3.11.3 - Authenticated SQL Injection
<a href="#">groundhogg</a>	2019-10-23	Groundhogg <= 2.0.8.1 - Authenticated Reflected XSS
<a href="#">syntaxhighlighter</a>	2019-10-22	SyntaxHighlighter Evolved <= 3.5.0 - Stored Cross-Site Sc...
<a href="#">qode-instagram-widget</a>	2019-10-21	Bridge Theme <= 18.2 - Open Redirect
<a href="#">qode-twitter-feed</a>	2019-10-21	Bridge Theme <= 18.2 - Open Redirect
<a href="#">sliced-invoices</a>	2019-10-17	Sliced Invoices <= 3.8.2 - Multiple Vulnerabilities
<a href="#">all-in-one-seo-pack</a>	2019-10-16	All In One SEO Pack < 3.2.7 - Stored Cross-Site Scripting...
<a href="#">eu-cookie-law</a>	2019-10-16	EU Cookie Law <= 3.0.6 - Stored XSS
<a href="#">events-manager</a>	2019-10-16	Events Manager < 5.9.6 - Stored XSS
<a href="#">fast-velocity-minify</a>	2019-10-16	Fast Velocity Minify < 2.7.7 - Full Path Disclosure
<a href="#">broken-link-checker</a>	2019-10-15	Broken Link Checker <= 1.11.8 - Authenticated Reflected C...
<a href="#">zoho-crm-forms</a>	2019-10-15	Zoho CRM Lead Magnet Plugin - Authenticated Cross Site Sc...

---

# 0-Day Vulnerabilities



---

# 0-Day Vulnerability Usage

- To redirect visitors to spam sites
- To inject links in your content for SEO purpose
- To create an army of sites that attack a specific target

---

# How is a 0-Day Vulnerability Used?

1. Prepare a list of WordPress sites
2. Try exploit on a site
3. Go to the next site in the list
4. Repeat 2 & 3 until rich or bored
5. Automate for faster results



# Protection Against Spam Redirects

1. Hardcode siteurl and home values in wp-config.php

```
define( 'WP_HOME', 'https://mysite.com' );  
  
define( 'WP_SITEURL', 'https://mysite.com' );
```

2. Make wp-config.php readonly

# Protection Against Automated Plugin Option Updates

Only permit access to wp-admin from trusted IP addresses

Include this in /wp-admin/.htaccess file:

```
<Limit GET POST PUT>
order deny,allow
deny from all
SetEnvIf Request_URI "admin-ajax.php" allow
allow from xx.xx.xx.xx
allow from yy.yy.yy.yy
Satisfy any
</Limit>
```

# Protection Against Code Injections

Block all POST requests that don't have a valid referrer value

Include this in your primary .htaccess file:

```
RewriteCond %{REQUEST_METHOD} POST
RewriteCond %{HTTP_REFERER} !^https://(www\.)?mysite.com/.*$ [NC]
RewriteRule .* - [F]
```

# Protection Against XSS and Already Injected Code

Use content security policy to only load pre-approved scripts

Include this in your primary .htaccess file:

```
<IfModule mod_headers.c>
    Header set Content-Security-Policy "default-src 'self';
script-src 'self' www.google-analytics.com maps.google.com"
    Header set X-Content-Type-Options nosniff
    Header set X-Frame-Options DENY
</IfModule>
```

---

# Results

- Redirect visitors to spam sites - BLOCKED
- Inject links / code in your content - BLOCKED
- Attack other sites using XSS - BLOCKED



Thank You!

Slides: [scaledynamix.com/WCUS](https://scaledynamix.com/WCUS)

Questions? [twitter.com/nginxreload](https://twitter.com/nginxreload)