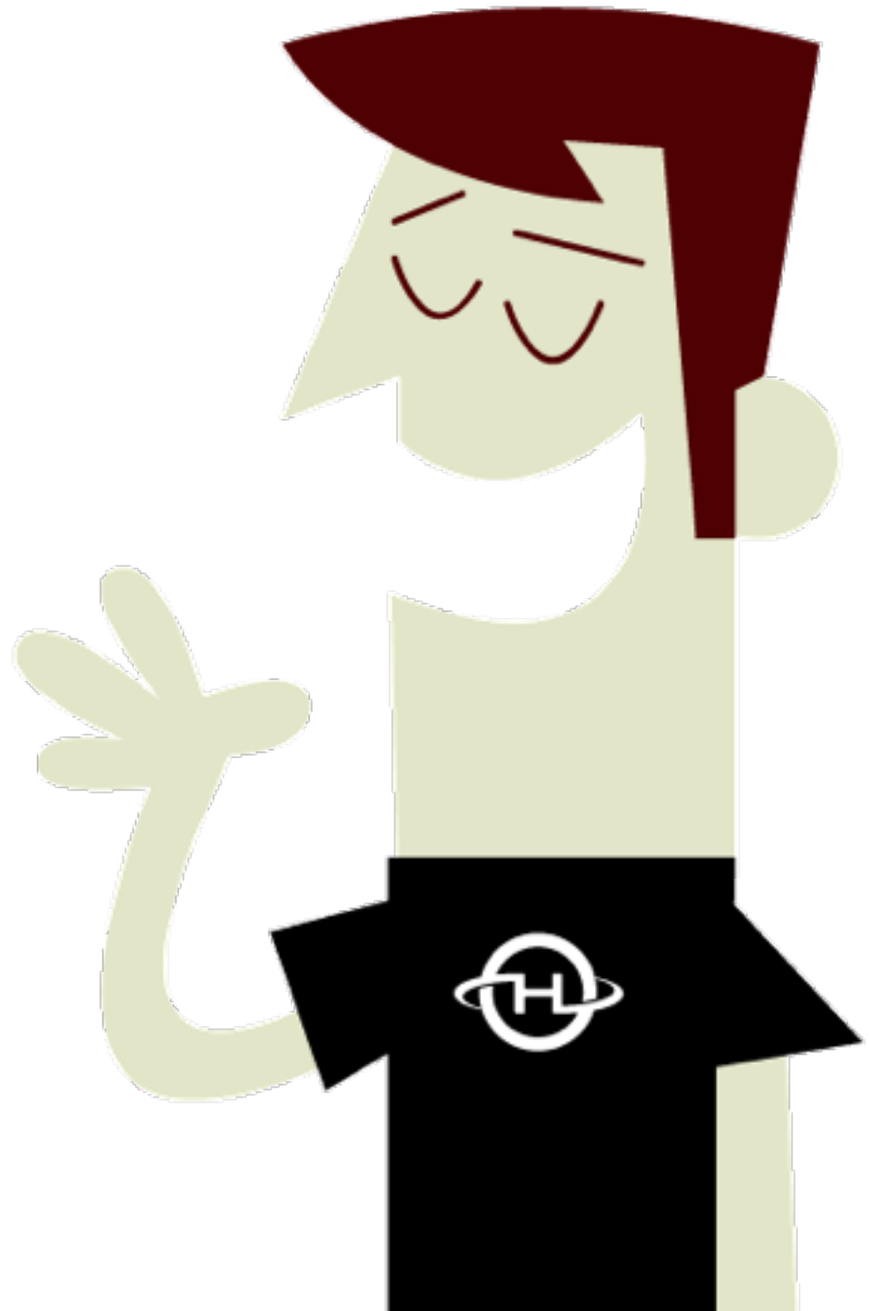
Stopping the XML-RPC Hack

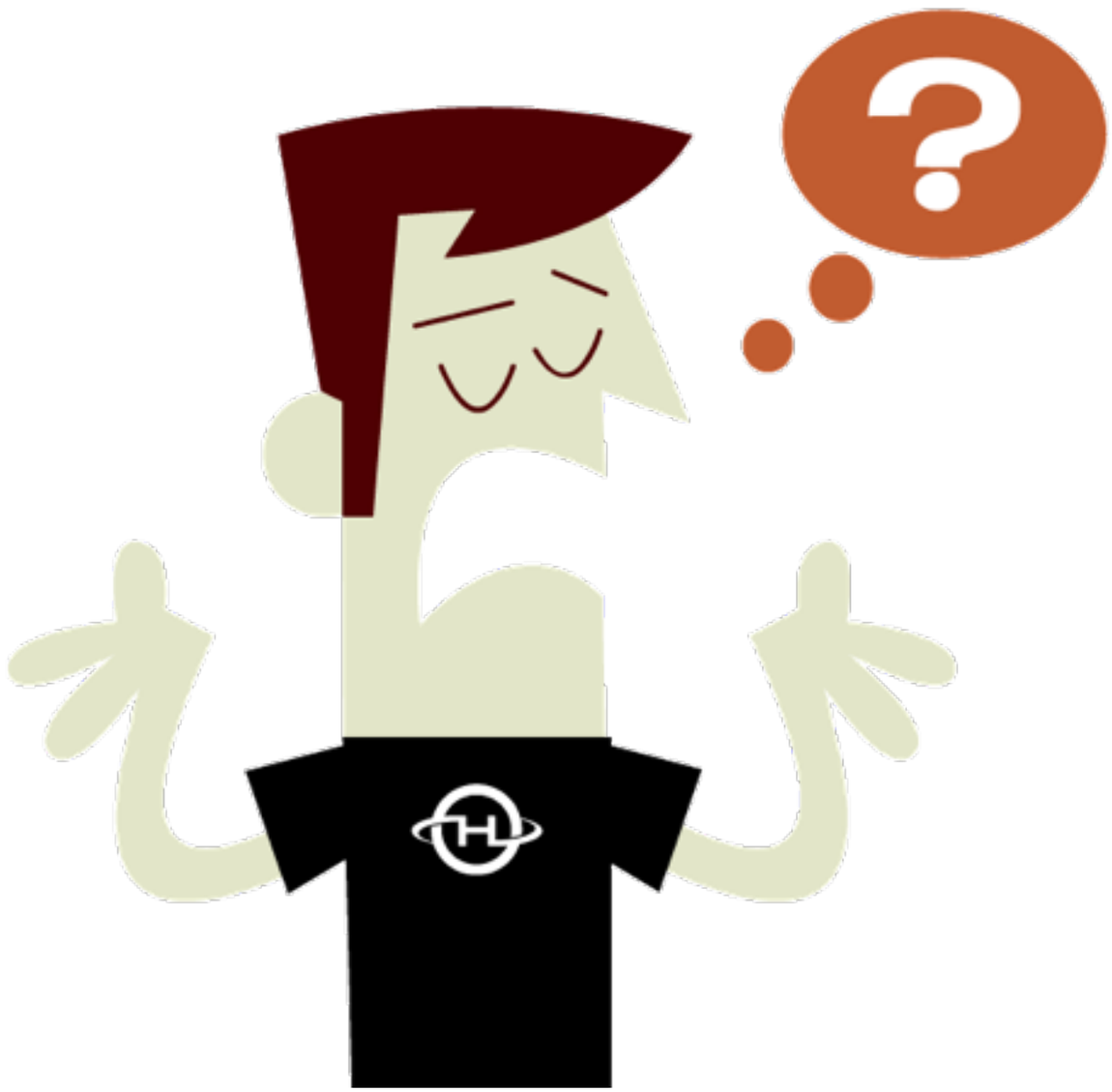
Simple Solutions for a Serious Problem

Adam Soucie

- Highforge
- Web Developer
- Content writer



What is XML-RPC?



- Allows WordPress to post on your behalf
- Allows access to WordPress clients
- Allows for ping backs and trackbacks

Why is it dangerous?

- Hijacks your website without your knowledge
- Uses your site for a DDoS attack
- Potentially gets your domain labelled as a spammer

How do you stop it?

- Add a filter to functions.php
- Prevent access to XMLRPC.php using .htaccess
- Use a plugin

Method 1: Functions.php

- Completely disables XMLRPC.php
- Uses a filter
- One line of code
- Alternative for Jetpack users is 5 lines

Complete disable XML-RPC...

```
add_filter('xmlrpc_enabled', '__return_false');
```

…or just block Pingbacks

```
add_filter( 'xmlrpc_methods', 'remove_xmlrpc_pingback_ping' );
function remove_xmlrpc_pingback_ping( $methods ) {
    unset( $methods['pingback.ping'] );
    return $methods;
} ;
```

Method 2: .htaccess

- One command
- Blocks access at the server level for extra security
- Can also whitelist IPs to allow limited access

To block all access...

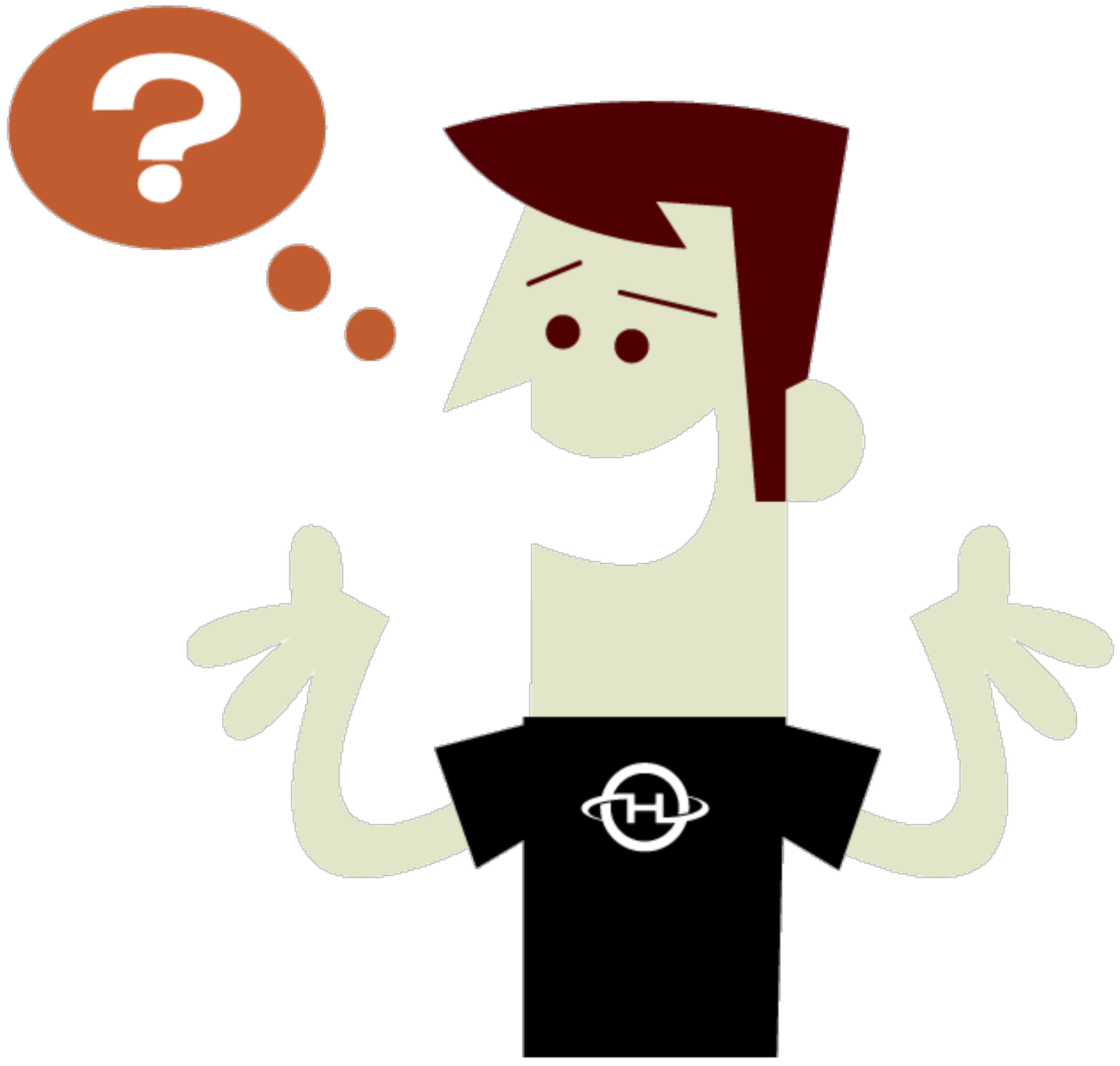
```
<Files xmlrpc.php>
Order Deny,Allow
Deny from all
</Files>
```

...or to Whitelist IPs

```
<Files xmlrpc.php>
Order Deny,Allow
Deny from all
Allow from 987.654.321
</Files>
```

Method 3: Use a plugin

- Mimics the Functions.php method
- Perfect for non-coders
- Disable XML-RPC is the most common one



Any questions?

Illustrations by:

Tina Fiume

More info:

www.adamsoucie.com

www.highforge.com