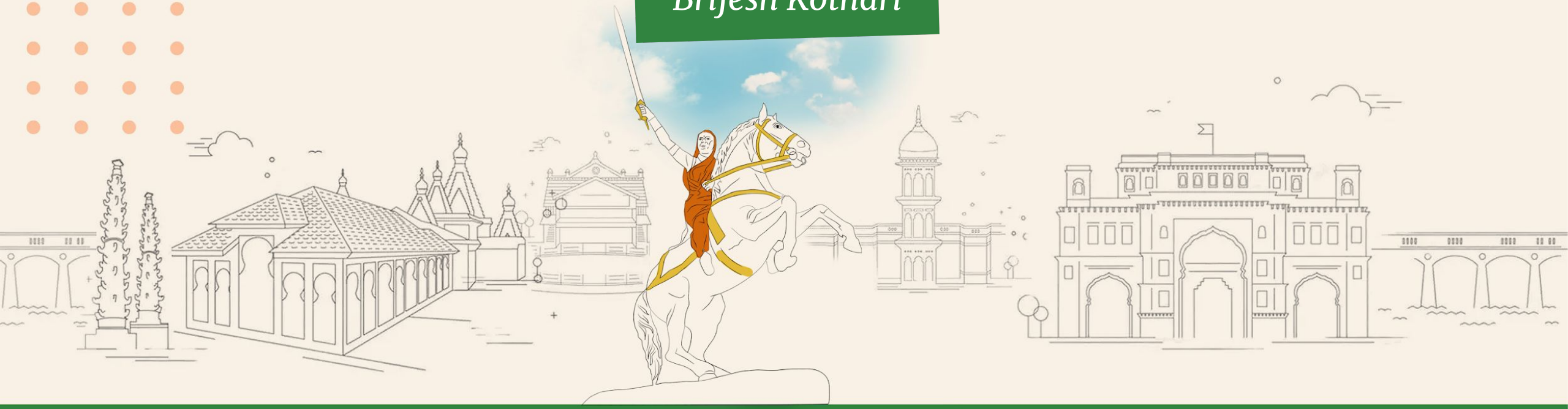
WORDCAMP KOLHAPUR 2025

5 Tips for Creating a Secure WordPress Plugin

Brijesh Kothari



A Little About Me

WordPress Plugins: 11 Years

Experience: Softaculous, WP Inspired

Plugins Used by: Millions

I'm here to share **insights, lessons, and strategies** I've developed over the years.

CSRF Protection with Nonce

WORDCAMP KOLHAPUR 2025

Render

```
<?php
wp_nonce_field(‘slug-options');
?>
```

Validate

```
if(isset($_POST[‘my-button’])){
check_admin_referer(slug-options');
}
```

Never Trust User Input

WORDCAMP KOLHAPUR 2025

Sanitize

Validate

Sanitation is okay, but validation/rejection is better

```
-> sanitize_text_field( $_POST['title'] );
-> sanitize_email( $_POST[email'] );
-> sanitize_url( $_POST[‘url’] );
-> sanitize_user( $_POST[‘username’] );
```

```
-> in_array( $input, [‘john’, ‘doe’]);
-> 1 === $input
-> $val = (int) $input;
-> is_email( $input );
```

XSS Protection

Escape

Escape as late as possible

```
-> <h4><?php echo esc_html( $title ); ?></h4>

-> <div onclick='<?php echo esc_js( $value ); ?>' />

-> <img alt="" src="<?php echo esc_url( $media_url ); ?>" />

-> <ul class="<?php echo esc_attr( $stored_class ); ?>">

-> <p><?php echo wp_kses( $_POST['content'] ); ?></p>
```

Check Privileges

Make sure the user has permission to perform the action

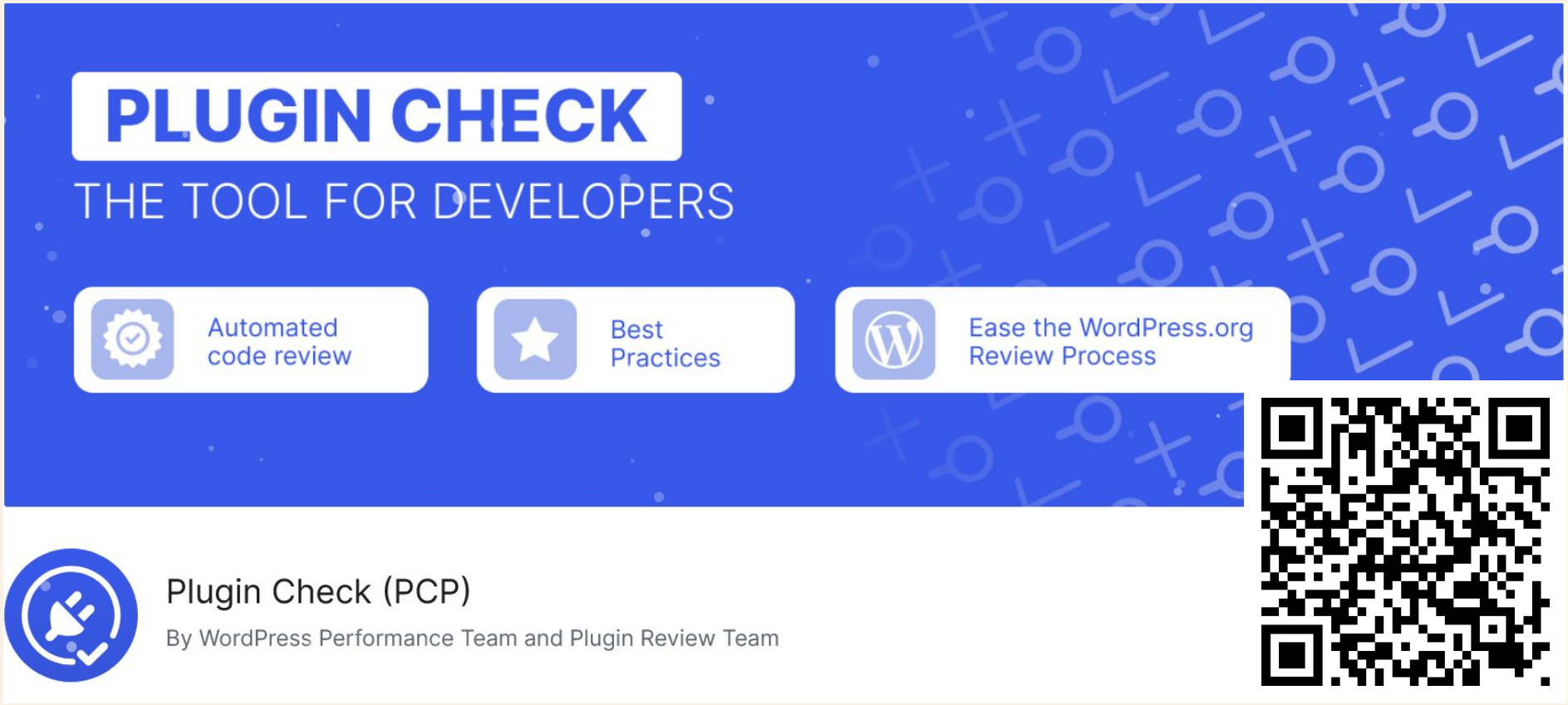
```
-> if(!current_user_can( 'edit_posts' )) return false;
-> if(!current_user_can( ‘activate_plugins’ )) return false;
-> if(!current_user_can( ‘manage_options’ )) return false;
-> if(!current_user_can( ‘moderate_comments’ )) return false;
-> if(!current_user_can( ‘delete_users’ )) return false;
```

Handle Vulnerabilities

WORDCAMP KOLHAPUR 2025

1. Read the report carefully
2. Replicate the vulnerability
3. Fix it
4. Test the fix
5. Release a **New Version**
6. Notify the Team who reported

Plugin Check Tool



Can I use AI ?

Can I use AI to write a Plugin ?

- Don’t copy code blindly
- Try to understand each and every line of code
- Double check if you are using the correct filter
- Check for all possible vulnerabilities we discussed

WORDCAMP KOLHAPUR 2025

Thank You

Join our WhatsApp Community for
WordPress Plugins Problem Solving