Security

WordPress Security

security scan:

https://hackertarget.com/wordpress-security-scan/

Prevention

- Keep WordPress, themes, and plugins updated
- Use strong passwords and 2FA
- Install a security plugin
- Limit login attempts
- Use security headers
- Regular backups
- Consider a Web Application Firewall (WAF)

Disable xmlrpc

```
// Disable XML-RPC completely
add_filter('xmlrpc_enabled', '__return_false');

// Remove X-Pingback header
add_filter('wp_headers', function($headers) {
  unset($headers['X-Pingback']);
  return $headers;
});

// Disable pingbacks
add_filter('pings_open', '__return_false', 10, 2);

// Remove RSD link (Really Simple Discovery)
remove_action('wp_head', 'rsd_link');

// Remove Windows Live Writer manifest link
remove_action('wp_head', 'wlwmanifest_link');
```

Test:
curl -I https://yoursite.com/xmlrpc.php

Securing WordPress REST API Endpoints

```
# Block access to WordPress REST API
RewriteEngine On
RewriteCond %{REQUEST_URI} ^/wp-json/ [NC]
RewriteRule .* - [R=403,L]
```

WordPress Authentication via functions.php

```
add_filter('rest_endpoints', function($endpoints) {
    // Remove user endpoints
    if (isset($endpoints['/wp/v2/users'])) {
        unset($endpoints['/wp/v2/users']);
    }
    if (isset($endpoints['/wp/v2/users/(?P[\d]+)'])) {
        unset($endpoints['/wp/v2/users/(?P[\d]+)']);
```

```
    }
    return $endpoints;
});
```

Recommended Approach:

1. **Remove user enumeration** (always do this):

```
add_filter('rest_endpoints', function($endpoints) {
    if (isset($endpoints['/wp/v2/users'])) {
        unset($endpoints['/wp/v2/users']);
    }
    if (isset($endpoints['/wp/v2/users/(?P[\d]+)'])) {
        unset($endpoints['/wp/v2/users/(?P[\d]+)']);
    }
    return $endpoints;
});
```

- **Require authentication for sensitive endpoints** while keeping public content accessible for legitimate use cases like mobile apps or headless WordPress setups.
- **Use web server rules** only if you don't need the API at all or can whitelist your own services.

3. WordPress Authentication via functions.php

```
// Disable REST API for non-authenticated users
add_filter('rest_authentication_errors', function($result) {
    if (!is_user_logged_in()) {
        return new WP_Error(
            'rest_disabled',
            'REST API is disabled for public access',
            array('status' => 401)
        );
    }
    return $result;
});
```

Selectively Block Specific Endpoints

```
add_filter('rest_endpoints', function($endpoints) {
 // Remove user endpoints
 if (isset($endpoints['/wp/v2/users'])) {
 unset($endpoints['/wp/v2/users']);
 }
 if (isset($endpoints['/wp/v2/users/(?P[\d]+)'])) {
 unset($endpoints['/wp/v2/users/(?P[\d]+)']);
 }
 return $endpoints;
});
```

Unique solution ID: #1031

Security

Author: n/a
Last update: 2026-01-06 09:54