

Sensitive Endpoints Accessible

What This Means

This finding indicates that one or more sensitive endpoints on your site are publicly accessible without restriction.

These endpoints may expose functionality that is commonly targeted by automated attacks.

Why It Matters

Sensitive endpoints are entry points into your application.

Examples include:

- `wp-login.php`
- `xmlrpc.php`
- REST API endpoints

If left unrestricted, attackers may:

- perform brute force login attempts
- probe application behavior
- abuse exposed functionality
- automate large-scale attacks

Restricting access reduces unnecessary exposure.

How Steel Security Detects This

Steel Security checks whether commonly targeted endpoints are accessible without restriction.

If these endpoints respond to requests in an unrestricted manner, they are flagged.

How to Fix It

To resolve this issue:

- restrict access to sensitive endpoints
 - limit exposure based on usage and requirements
 - apply Steel Security hardening controls related to endpoint protection
-

What to Expect After Fixing

After applying protections:

- access to sensitive endpoints will be limited
 - automated attack traffic may be reduced
 - legitimate functionality should continue to work if properly configured
-

How to Verify

To verify the fix:

1. attempt to access sensitive endpoints directly
2. confirm that access is restricted under expected conditions

Test both:

- authorized access (should work)
 - unauthorized access (should be limited or blocked)
-

Common Causes

- default WordPress exposure of login and API endpoints
 - lack of access restrictions
 - publicly accessible endpoints without controls
-

Best Practices

- restrict endpoints that are not required
 - limit access where possible
 - monitor access patterns
 - combine with other access and execution controls
-

Related

- [Restrict Sensitive Endpoints](#)
 - [XML-RPC Enabled](#)
 - [Direct PHP Access Allowed](#)
-

Revision #1

Created 2026-04-04 18:46:58 UTC by Jason Wassing

Updated 2026-04-04 18:46:58 UTC by Jason Wassing