Persistent HTML Injection from Unauthenticated User Rendered in Admin Panel

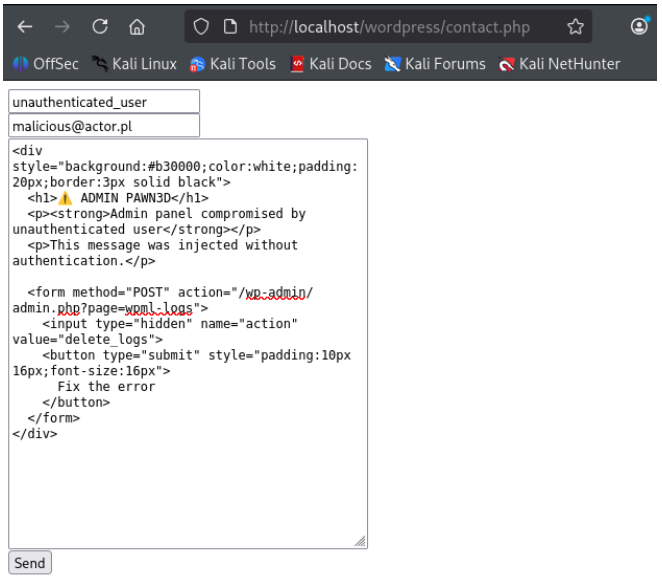
Affected component:
Wordpress Plugin: WP Mail Logging 1.15.0 (Active Installations: 300,000+)

Tested Environment:
WordPress: 6.9
Server: Apache + PHP (local environment)
Authentication: Unauthenticated user
Attack Target: Admin panel and email logs

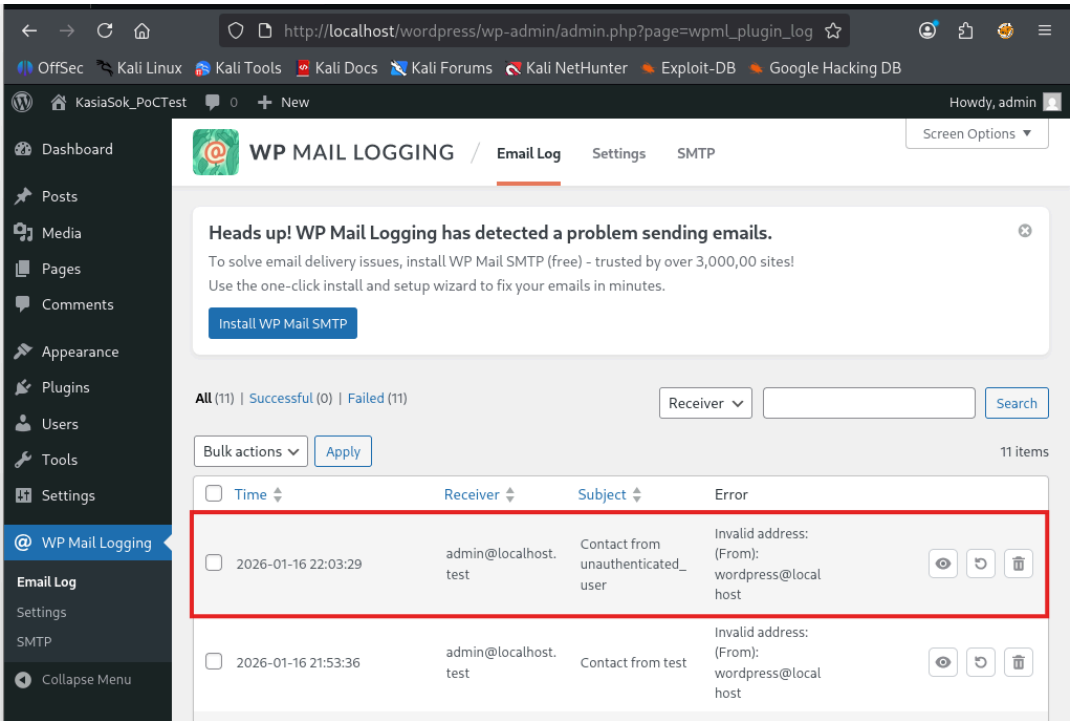
Security Classification:
Vulnerability Type: Persistent HTML Injection
Attack Vector: Network
Privileges Required: None
User Interaction: Required (admin views log)
Impact Scope: Admin panel
Scope changed (Frontend ⟶ Admin Panel)

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.

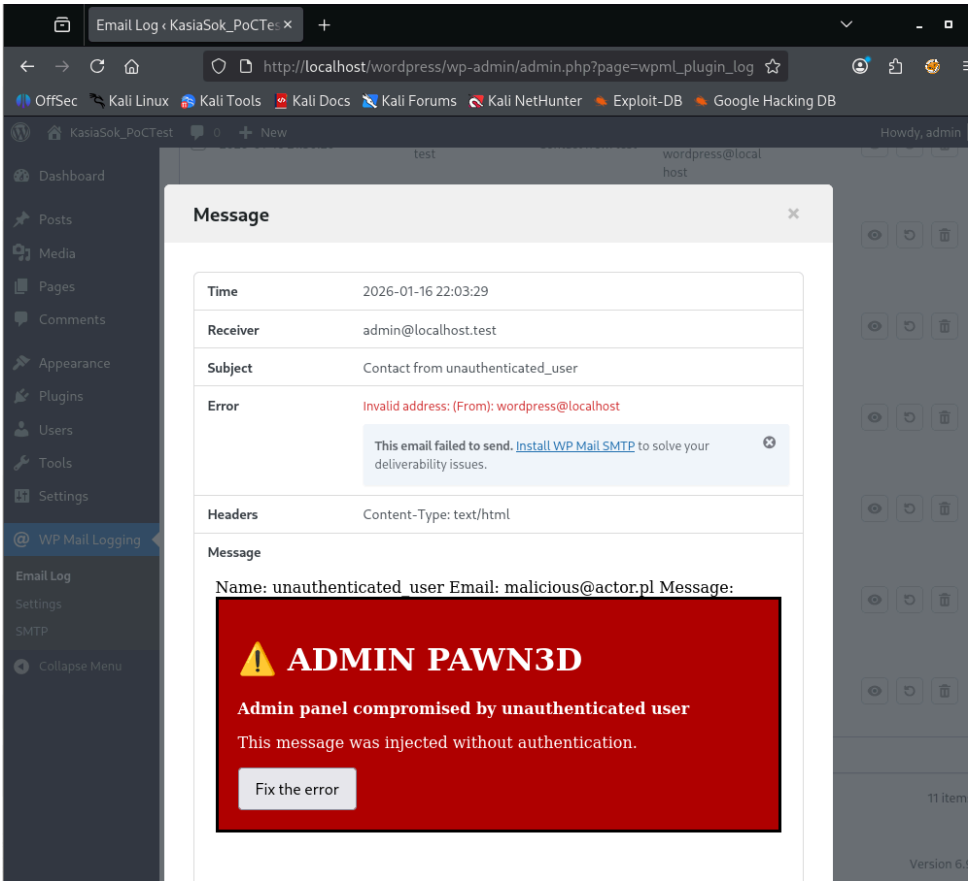
Vulnerability Details:
The plugin logs email content without sufficient sanitization or output escaping.
HTML supplied by an unauthenticated user is stored and later rendered directly in the admin interface when viewing email logs.



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



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



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

_

Researcher: Kasia Sok

16 / 01 / 2026

Persistent HTML Injection from Unauthenticated User Rendered in Admin Panel

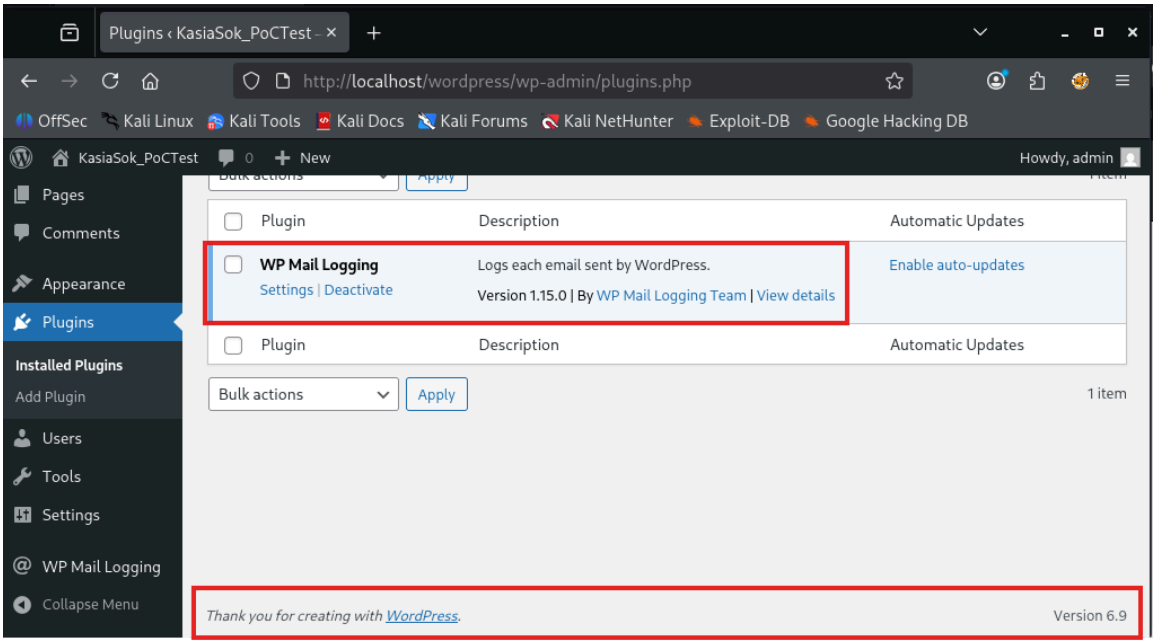
Impact:
Inducing administrators to take unsafe actions through persistent UI deception and phishing
Persistent social engineering leading to credential disclosure
Abuse of administrator trust in the admin panel UI
Potential stepping stone to full site compromise via chained vulnerabilities

Example payload:

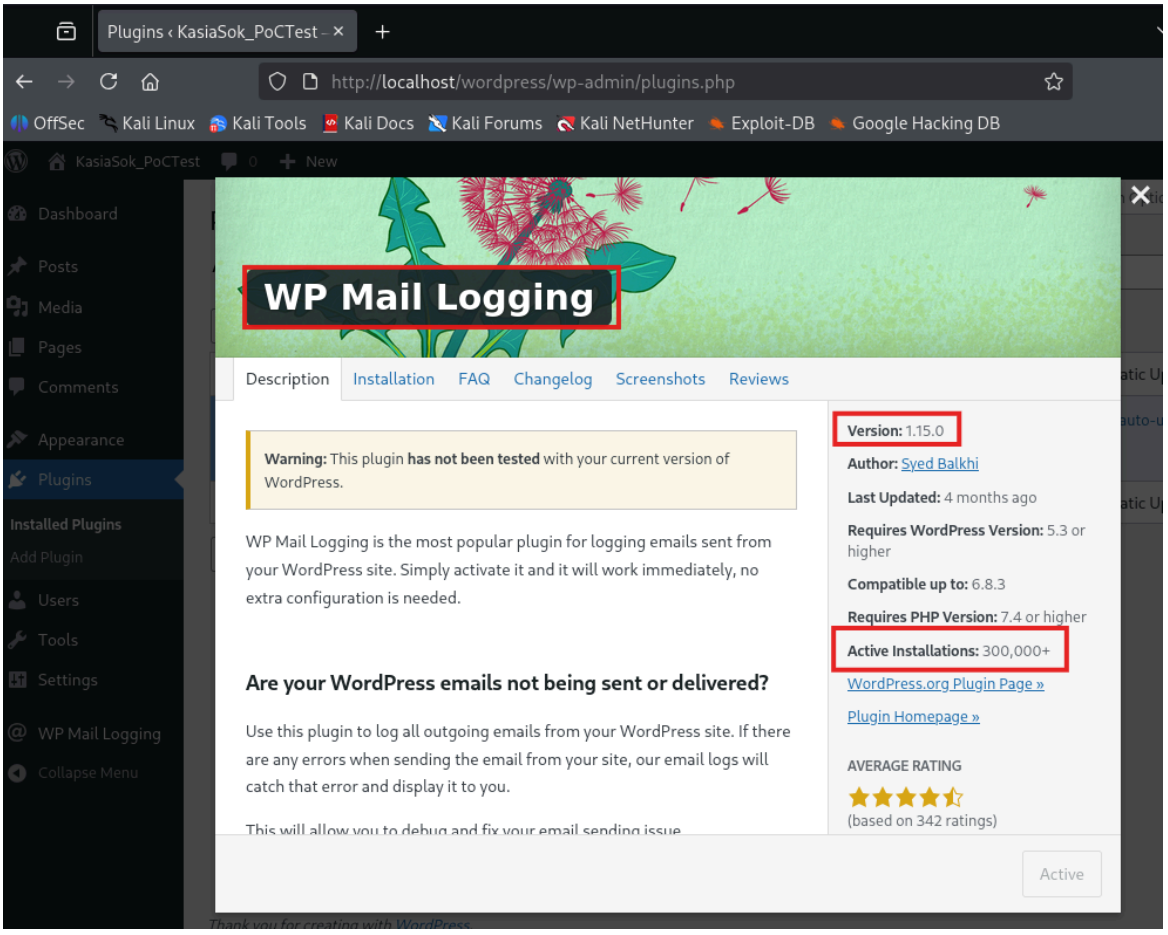
```
<div style="background:#b30000;color:white;padding:20px;border:3px solid black">
 <h1>⚠️ ADMIN PAWN3D</h1>
 <p><strong>Admin panel compromised by unauthenticated user</strong></p>

  <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)



PoC 4: Wordpress 6.9 + WP Mail Logging 1.15.0



PoC 5: Active Installation 300,000+

–
Researcher: Kasia Sok
16 / 01 / 2026
Persistent HTML Injection from Unauthenticated User Rendered in Admin Panel

_

Researcher: Kasia Sok

16 / 01 / 2026

Persistent HTML Injection from Unauthenticated User Rendered in Admin Panel