



Contribution ID: 23

Type: **not specified**

Trawling: Transforming email automation into a critical threat

Tuesday 10 June 2025 14:00 (1 hour)

Automated email is a cornerstone of modern business communication. **Welcome messages, purchase confirmations, appointment notifications**, and other automated emails are constantly sent from official company accounts, with varying degrees of personalization based on user data. However, this very automation opens the door to a **serious and often underestimated vulnerability**.

In this talk, we will introduce “**Trawling**”, an **innovative and previously undocumented methodology** for exploiting email automation, transforming what seemed like **low-impact attacks into a critical threat**. By manipulating the **reflected fields** in these automated emails, an attacker can **partially or entirely alter the message content**, including the **insertion of malicious links** or other harmful instructions—all while the message is sent from the **company’s legitimate account**.

A key aspect of this research is the **exploitation of email tagging to redirect and amplify attacks**. This technique allows attackers to send **modified messages to external victims without raising suspicion**, facilitating the **large-scale distribution of malicious emails**. Additionally, we will explore different distribution methods, such as **forced user registration and email account verification**, which enable attackers to **maximize the impact** of this technique.

This session will provide attendees with an **in-depth understanding** of this vulnerability and its exploitation, offering **strategies to mitigate these attacks** before they become widely used in the real world.

Length

60 minutes

Optional: Speaker / convener biography

Experienced security researcher and penetration tester specializing in web pentest, bug bounty and severity escalation of security findings, with four years of professional expertise. Recognized with three published CVEs (Microsoft CVE-2025-21207, CVE-2024-3068, CVE-2023-44393) and ranked Top 2 on HackerOne Mexico.

Holds eWPTXv2 and PNPT certifications, demonstrating advanced skills in web application security and penetration testing. Currently focused on developing cutting-edge cybersecurity research and uncovering undocumented attack techniques.

Driven by a passion for maximizing the exploitation and impact of security findings, while providing effective solutions to strengthen organizations’ defenses.

Primary author: RETA BERLANGA, Eduardo

Presenter: RETA BERLANGA, Eduardo

Session Classification: Talks

Track Classification: Talks and presentations