exploit

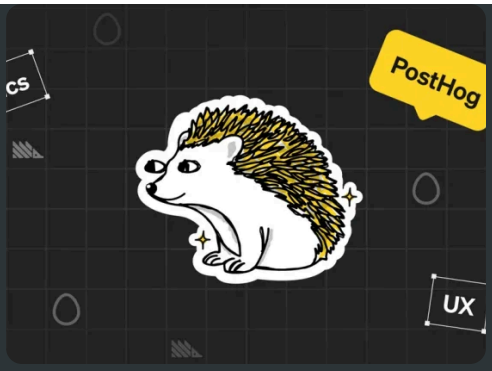
0DAY ADVISORY AUTHENTICATION CVE CYBER DJANGO EXPLOIT HACKING LOGPOINT METASPLOIT MIDDLEWARE PRODUCT SECURITY VULNERABILITY

JAN 1, 2026

The Story of a Perfect Exploit Chain: Six Bugs That Looked Harmless Until They Became Pre-Auth RCE in a Security Appliance

It was May 2024, and our internal security team was evaluating the LogPoint SIEM/SOAR platform to replace our existing platform, potentially. As part of a habit I've built over the years —and honestly, part of our 3rd party due diligence– I gave myself 24 hours to do what I always do with any technology we're about to trust: try to break it.

Read the story



DEC 15, 2025

Inside PostHog: How SSRF, a ClickHouse SQL Escaping 0day, and Default PostgreSQL Credentials Formed an RCE Chain (ZDI-25-099, ZDI-25-097, ZDI-25-096)

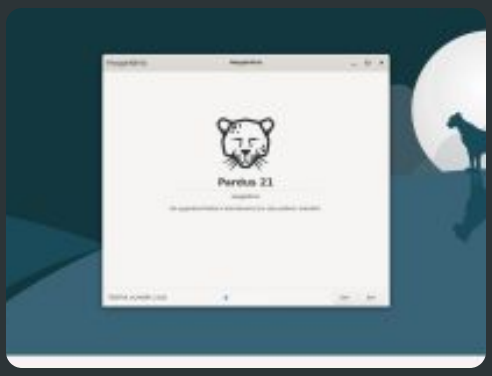
It was yet another day at the office. Our team was internally discussing moving to a different platform analytics solution. Our team was really leaning more towards Posthog. It's one of the brilliant *-I personally believe it's the best-* products on the market. And that's where the story has begun…
(more…)

DEC 21, 2021

CVE-2021-3825 | LiderAhenk 0day - All your PARDUS Clients Belongs To Me

LiderAhenk is an open source software system that enables centralized management, monitoring and control of systems and users on the corporate network.

In this blog post, you will see how bad it can get when you have a critical security vulnerability on your centralized client management system.
(more…)



SEP 13, 2021

CVE-2021-3806 | Pardus 21 Linux Distro - Remote Code Execution 0day

A couple of days ago, I came up with news that Pardus will organize a report-bug contest. I love to contribute to open-source projects. So that was a pretty good chance to revisit one of my old friends, Pardus, and uncover security and/or privacy issues.
(more…)

MAR 21, 2021

CVE-2021-21425 | Unexpected Journey #7 - GravCMS Unauthenticated Arbitrary YAML Write/Update leads to Code Execution

It has been a while since I haven't published a post on our beloved blog. Today I would like to share technical details and POC for a pretty funny vulnerability that I've found at GravCMS.
(more…)

MAR 18, 2020

Vesta Control Panel Second Order Remote Code Execution 0day Step-by-Step Analysis

I believe that doing a security research is all about trying to understand high-level of architecture of the products and finding a creative attack vectors.

I hope this blog post will show some the readers how to start doing security research.
(more…)

DEC 19, 2018

CVE-2018-20323 | MailCleaner Community Edition Remote Code Execution

In this article, I would like to share a remote code execution vulnerability details of MailCleaner Community Edition product.
(more…)

JUN 22, 2018

Unexpected Journey #6 - All ways lead to Rome ! Remote Code Execution on MicroFocus Secure Messaging Gateway

It has been a quite while since I haven't released a new part of unexpected journey article serie. Particularly this small 0-day research project has been certainly didactic to me. Thus, I've decided to write down the process of achieving remote code execution on MicroFocus Secure Messaging Gateway product.
(more…)

MAR 7, 2018

Advisory | ManageEngine Applications Manager Remote Code Execution and SQLi

It is an interesting coincidence that almost 1 year ago we identified a critical security issue in a different product (Eventlog Analyzer) of this company. Now, this time we've came across with another product of this company during penetration test. To be honest I've seen more than 20 different high/critical vulnerability during the analysis of the product but I will only share two of them now, as a full disclosure.
(more…)

NOV 6, 2017

CVE-2017-16666 | Xplico Unauthenticated Remote Code Execution

The goal of Xplico is extract from an internet traffic capture the applications data contained. For example, from a pcap file Xplico extracts each email (POP, IMAP, and SMTP protocols), all HTTP contents, each VoIP call (SIP), FTP, TFTP, and so on. Xplico isn't a network protocol analyzer. Xplico is an open source Network Forensic Analysis Tool (NFAT).
(more…)