0day

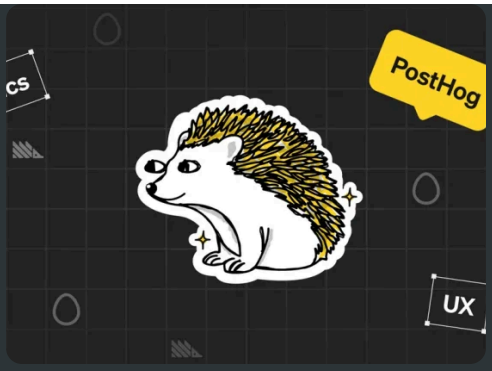
0DAY ADVISORY AUTHENTICATION CVE CYBER DJANGO EXPLOIT HACKING LOGPOINT METASPLOIT MIDDLEWARE PRODUCT SECURITY VULNERABILITY

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 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…)

SEP 19, 2017

Advisory | DenyAll Web Application Firewall Unauthenticated Remote Code Execution (CVE-2017-14706)

DenyAll Web Application Firewall is the foundation for next generation application security products. It combines ease of configuration - with its workflow engine and management APIs - with a proven ability to secure web applications. It embeds negative and positive security, in-context, user behavior analysis, and soon-to-be added rWeb

advanced security engines, to efficiently protect your web applications while minimizing false positives.
(more…)

SEP 12, 2017

Advisory | osTicket v1.10 Unauthenticated SQL Injection (CVE-2017-14396)

osTicket is a widely-used and trusted open source support ticket system. It seamlessly routes inquiries created via email, web-forms and phone calls into a simple, easy-to-use, multi-user, web-based customer support platform. osTicket comes packed with more features and tools than most of the expensive (and complex) support ticket systems on the market.
(more…)

JUN 10, 2017

Unexpected Journey #5 - From weak password to RCE on Symantec Messaging Gateway (CVE-2017-6326)

If you are following our blog, you must familiar with Unexpected Journey article series. In this article, I will share our latest real-life pentest experience as well as the technical details of our brand new ~~0day~~ that helps us to execute operating system commands on Symantec Messaging Gateway.
(more…)

MAY 17, 2017

Advisory | Cryptolog Unauthenticated Remote Code Execution

CRYPTOLOG is a log manager that collects, normalizes, and categorizes massive logs generated across your network and turn it into valuable information on an intuitive interface where advance search, analysis and correlation monitoring becomes easier and more efficient.
(more…)