

# THE YESWEHACK BLOG

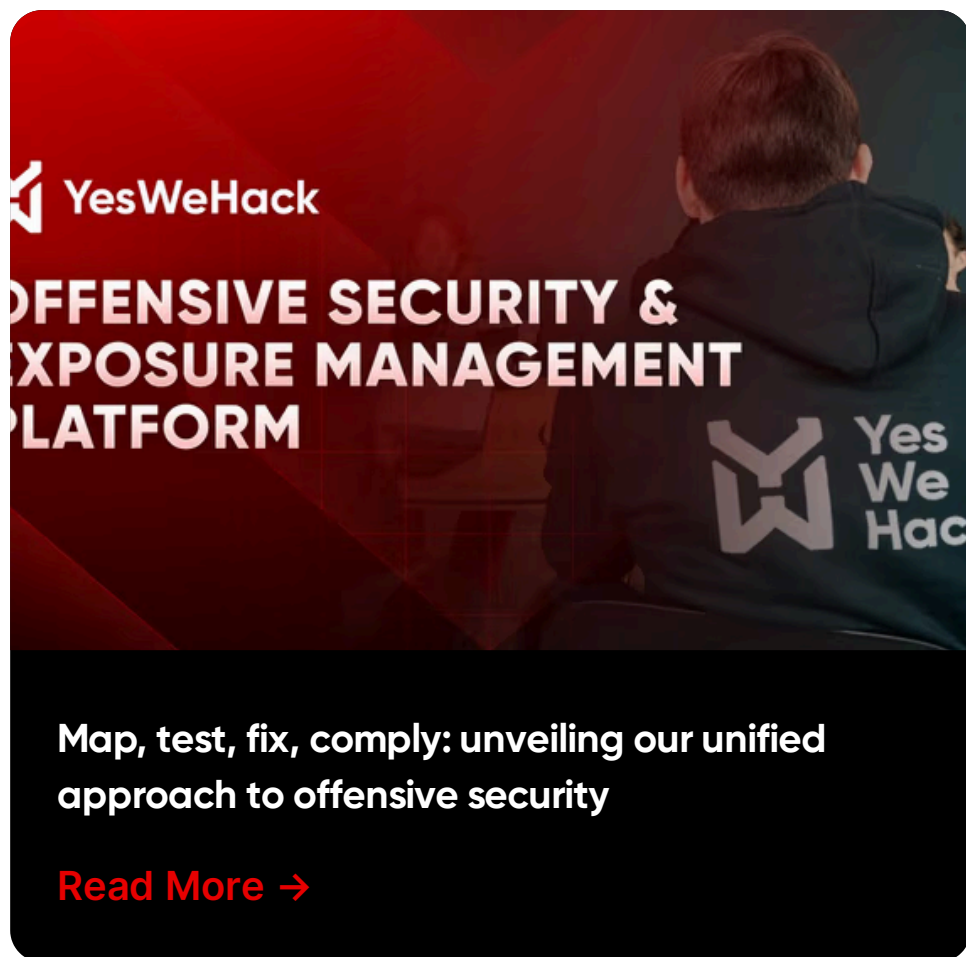



**Map, test, fix, comply: unveiling our unified approach to offensive security**

March 31, 2026

[READ THE POST](#)





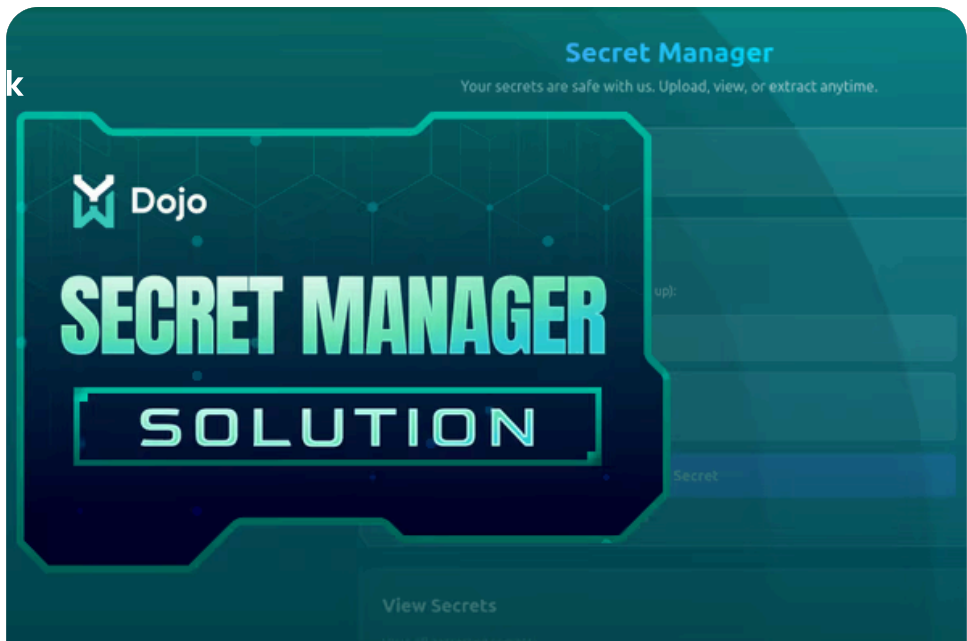
 **YesWeHack**

**OFFENSIVE SECURITY &  
EXPOSURE MANAGEMENT  
PLATFORM**

**Map, test, fix, comply: unveiling our unified  
approach to offensive security**

**Read More ->**






The screenshot shows the Dojo Secret Manager interface. At the top right, it says "Secret Manager" and "Your secrets are safe with us. Upload, view, or extract anytime." The Dojo logo is on the left. A large, stylized graphic in the center contains the text "SECRET MANAGER SOLUTION". Below this, there is a "View Secrets" button. The interface has a dark teal and blue color scheme.

**Dojo challenge #49 Secret Manager solution**

[Read More →](#)

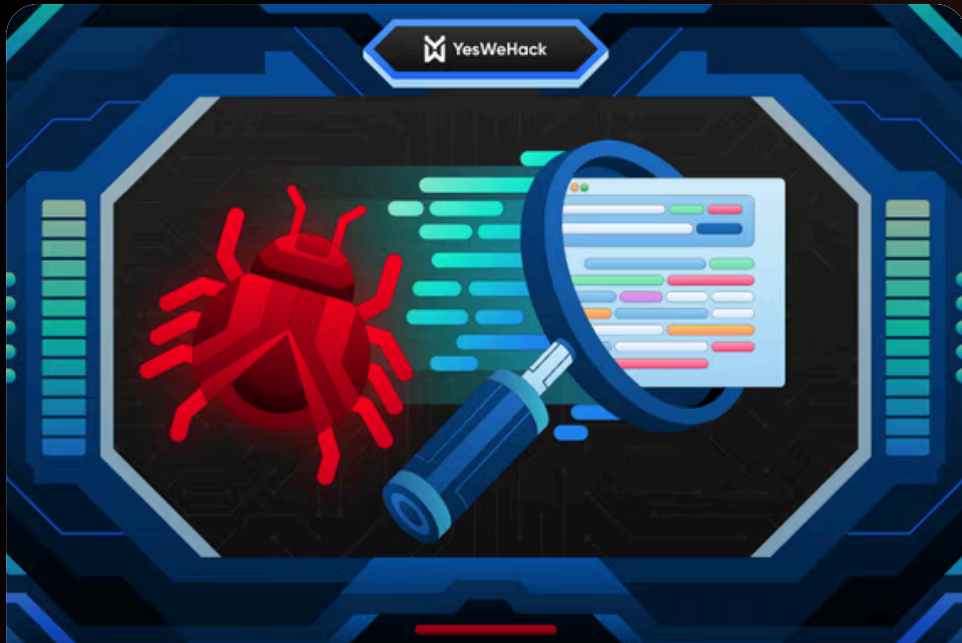


The screenshot shows the YesWeHack interface. The YesWeHack logo is at the top left. The main text reads "CONTINUOUS COVERAGE", "0 FALSE POSITIVES", and "FASTER REMEDIATION" (the last one is on a red background). On the right side, there are three status boxes: "CVE PUBLISHED 12h ago", "CVE IDENTIFIED 1h ago", and "ASK FOR RETEST". The background is dark with some blurred text and icons.

**Continuous Pentesting with zero false positives:  
a fully managed, platform-driven approach**



[Read More →](#)



**Open-source security testing: the Bug Bounty guide to code analysis**

[Read More →](#)



YesWeHack

YesWeHack

# PREVENTING MASS EXPLOITATION AT SCALE

Introducing Autonomous Pentest: identify actively exploited vulnerabilities across your attack surface

[Read More →](#)





**'We must learn how to use AI': Wlayzz on future-proofing Bug Bounty and how a duplicate became his favourite discovery**

[Read More →](#)

The article cover features a blue background with a yellow maze. A blue Python snake is positioned at the top of the maze. In the background, there are several computer window icons, one of which displays a red exclamation mark. The text 'PYTHON PITFALLS: TURNING DEVELOPER MISTAKES INTO VULNERABILITIES' is written in a bold, white, pixelated font across the center. The YesWeHack logo is in the top left corner. At the bottom of the cover, the title 'Python pitfalls: Turning developer mistakes into vulnerabilities' and a 'Read More →' link are displayed on a black background.

**PYTHON PITFALLS:  
TURNING  
DEVELOPER  
MISTAKES INTO  
VULNERABILITIES**

**Python pitfalls: Turning developer mistakes into vulnerabilities**

[Read More →](#)





**Notepad++ hijack, pwning Claude Code, top web hacking techniques of 2025 – ethical hacker news roundup**

[Read More →](#)



**Dojo challenge #48 RubitMQ solution**



[Read More →](#)

[LOAD MORE](#)

## **DON'T WAIT FOR THREATS TO STRIKE**

### **ADOPT A PROACTIVE SECURITY POSTURE NOW**

Harness the power of crowdsourced security to supercharge the discovery and remediation of vulnerabilities.

[BOOK YOUR DISCOVERY CALL](#)





## Products

[Bug Bounty](#)

[Continuous Pentesting](#)

[Autonomous Pentest](#)

[Vulnerability Disclosure Policy](#)

[Pentest Management](#)

[Our AI Approach](#)

[Live Hacking Events](#)

## Researchers

[Start Hunting](#)

[Public Programs](#)

[Tools](#)

[Ranking](#)

[Dojo](#)

[Training modules](#)

[Vulnerable Code Snippets](#)

## Resources



[Blog](#)

Case Studies



Help Center

API

Github

Newsletter

## Company

About YesWeHack

Trust & Security

Career

Press

Events

Contact

## FOLLOW US

---



Gartner Peer Insights

Click to load reviews





[Change Cookie Preferences](#)

[Cookies Policy](#)

[Privacy Policy](#)

[Legal Notices](#)

©2026 YESWEHACK

