HiddenLayer Raises $100M Series B LEARN MORE

HIDDENLAYER Platform Solutions Services Resources Partners Compan

SAI SECURITY ADVISORY

Missing Authorization for Interactive Sessions

June 9, 2025

Products Impacted

This vulnerability is present in all versions of BackendAI. We tested on version 25.3.3 (commit f7f8fe33ea0230090f1d0e5a936ef8edd8cf9959).

CVSS Score: 8.1

We value your privacy

We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept All", you consent to our use of cookies.

Customize Reject All Accept All

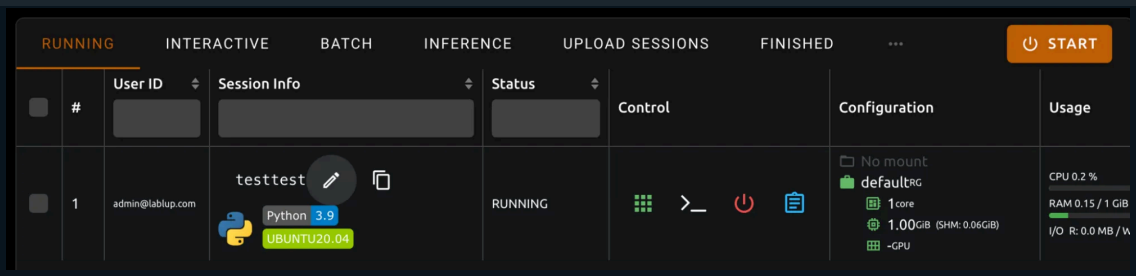
Details

HiddenLayer Raises $100M Series B LEARN MORE

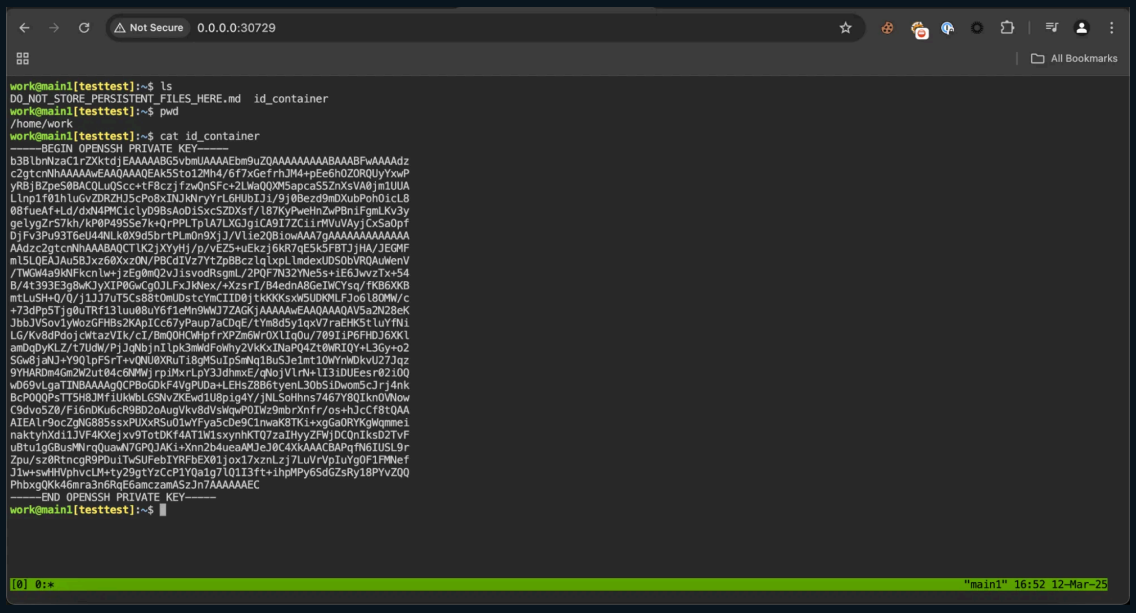
HIDDENLAYER Platform Solutions Services Resources Partners Company

A threat actor can scan the ports until they find an open interactive session and access it without any authorization or prior authentication.

To reproduce this, we created a session with all settings set to default.



Then, we accessed the web terminal in a new tab

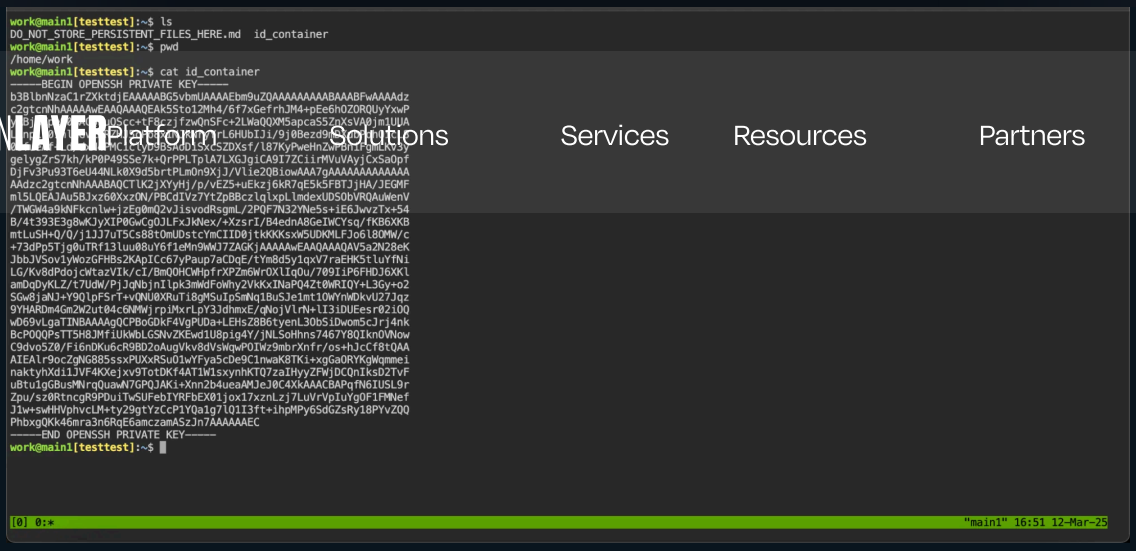


However, while simulating the threat actor, we access the same URL in an “incognito window” — eliminating any cache, cookies, or login credentials — we can still reach it, demonstrating the absence of proper authorization controls.

We value your privacy

We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept All", you consent to our use of cookies.

HiddenLayer Raises $100M Series B LEARN MORE



Related SAI Security Advisory

All SAI Security Advisory

CVE-2026-87988 September 11, 2026

_POSIX
nds
ting
full
host filesystem

CVE-
8798
En
var
pre
str

We value your privacy

We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept All", you consent to our use of cookies.

HiddenLayer Raises $100M Series B LEARN MORE

Mistral Vibe automatically approves a large set of commands that are not subject to the expected workspace path restrictions, allowing files anywhere on the host to be accessed without user approval.

READ MORE

pe
ch
en
via
inj

MIST

Mistra
consi
variab
check
comm
appro
enviro
behav
progra
abuse
execu

READ

We value your privacy

We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept All", you consent to our use of cookies.

HiddenLayer Raises $100M Series B LEARN MORE

27001 SOC 2

HIDDENLAYER Platform Solutions Services Resources Partners Company

Modules
AI Discovery
AI Supply Chain Security
AI Attack Simulation
AI Runtime Security

Security
AI Guardrails
Model Scanning
Red Teaming
Agent Harness Security

By Industry
Technology
Financial Services
US Federal Government
Healthcare

By Role
CISO
AI Leaders
Application Developers

Insights
Case Study
Reports and Guides
Webinars
Podcast
Security Advisory

Alliance
Featured Partners
AWS
Databricks

Company
About Us
Careers
The Newsroom
Research

Security Privacy Policy Cookie Settings © 2026 HiddenLayer, Inc. All rights reserved.

We value your privacy

We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept All", you consent to our use of cookies.