SMACKDAB INC. OFFICIAL POLICY

BUG BOUNTY DISCLOSURES

Official legal PDF. This document is generated from the Smackdab website legal source file.

BUG BOUNTY PROGRAM - PUBLIC DISCLOSURES

Last Updated: December 10, 2024 The following is a record of vulnerability reports processed through our Bug Bounty Program. We publish these summaries to provide transparency and help researchers understand what types of findings qualify for rewards. ⚠️ *Technical details are intentionally vague to protect our systems and users. Full reproduction details are not disclosed.*

- * *

🏆 HALL OF FAME

We recognize the following researchers for their contributions to Smackdab security:

Researcher

Recognition

Researcher C

Critical and High severity findings on core application

Researcher D

High severity finding on core application

Researcher B

Medium and Low severity findings on production infrastructure

Researcher A

Low severity findings on marketing website

- * *

📋 PROCESSED REPORTS

#

Date

Researcher

Category

System

Severity

Outcome

010

Dec 2024

Researcher C

IDOR

Core application

Critical

$200

008

Dec 2024

Researcher C

Authentication Bypass

Core application

Critical

$200

007

Dec 2024

Researcher C

Stored XSS

Core application

High

$125

009

Dec 2024

Researcher D

Email Change Logic Flaw

Core application

High

$75

005

Dec 2024

Researcher B

Information Disclosure

Monitoring infrastructure

Medium

$50

012

Dec 2024

Researcher B

Open Redirect / XSS (Grafana)

Monitoring infrastructure

Medium

$50*

001

Dec 2024

Researcher A

XML-RPC Configuration

Marketing website

Low

$25*

002

Dec 2024

Researcher A

CORS Misconfiguration

Marketing website

Low

*combined

011

Dec 2024

Researcher B

Exposed Admin Interface

Marketing website

Low

*combined

003

Dec 2024

Researcher A

WordPress Configuration

Marketing website

Info

No bounty

004

Dec 2024

Researcher A

WordPress Configuration

Marketing website

Info

No bounty

006

Dec 2024

Researcher B

DNS Configuration (CAA)

Domain configuration

Info

No bounty

* Combined bounty paid for multiple related reports

- * *

📝 REPORT SUMMARIES

#010 - IDOR (Critical)

Identified IDOR allowing an attacker to delete any Policy Group across organizations by manipulating a numeric ID in the delete API request. Remediated by implementing proper authorization checks.

#008 - Authentication Bypass (Critical)

Identified 2FA bypass via response manipulation. Remediated as part of authentication system hardening.

#007 - Stored XSS (High)

Identified stored cross-site scripting vulnerability in snippet management feature. Demonstrated session cookie access. Remediated.

#009 - Email Change Logic Flaw (High)

Identified that a user's email address could be changed without re-entering the current password, enabling potential account takeover via session hijacking. Remediated by adding re-authentication check.

#005 - Information Disclosure (Medium)

Identified unauthenticated Prometheus metrics endpoints exposing internal infrastructure details. No credentials or customer data exposed. Remediated.

#012 - Open Redirect / XSS (Medium)

Identified vulnerability in internal Grafana instances (CVE-2025-4123) that could lead to arbitrary JavaScript execution and session hijacking for targeted DevOps team members. Remediated by upgrading.

#001 & #002 - XML-RPC & CORS (Low)

Reported XML-RPC endpoint and permissive CORS configuration on marketing site. Limited impact due to no customer data on affected system. Combined bounty awarded.

#011 - Exposed Admin Interface (Low)

Reported phpMyAdmin setup wizard was publicly exposed. Classified as Low severity due to affecting the marketing website. Remediated.

- * *

🚫 DECLINED REPORT CATEGORIES

For transparency, the following report types have been submitted and declined under our program terms:

Category

Reason

Terms Reference

WordPress default configurations

Hardening suggestions without exploitability

Section 2.3

DNS record recommendations

No demonstrated exploitation path

Section 2.3

Known CVEs on marketing site

Known-issue category

Section 2.4

Performance/availability suggestions

Not security vulnerabilities

Section 2.3

- * *

For questions about this page or our Bug Bounty Program, contact: security@smackdab.ai

This PDF is the formal downloadable version of BUG BOUNTY DISCLOSURES.