SMACKDAB INC. OFFICIAL POLICY

BUG BOUNTY PROGRAM TERMS

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

SMACKDAB BUG BOUNTY PROGRAM TERMS

Effective Date: 12/09/2025

Last Updated: 12/09/2025

Version:

1.1

EFFECTIVE IMMEDIATELY: no new submissions will be accepted. The bug bounty program is temporarily closed for internal review and updates.

Document Location: https://smackdab.ai/legal/bug-bounty-program

1. OVERVIEW & RELATIONSHIP TO OTHER POLICIES

Smackdab Inc. (“Smackdab,” “we,” “us,” or “our”) operates this Bug Bounty Program (“Program”) to reward security researchers (“you,” “your,” “Researcher”) who help us identify and remediate security vulnerabilities in our systems.

These Bug Bounty Program Terms (“Terms”) govern eligibility for rewards and the conditions under which Smackdab may provide monetary bounties.

This Program sits on top of, and does not replace, our:

- Responsible Disclosure Policy (VDP); and
- Security Policy and other legal agreements (including the Terms of Service, Privacy Policy, and DPA).

If there is any conflict:

- The VDP governs scope, rules of engagement, and safe harbor.
- These Bug Bounty Program Terms govern bounty eligibility, reward decisions, and payout conditions.

Smackdab is in a pre-launch / soft-launch phase and operates this Program with a limited security budget. Reward ranges are intentionally modest and may increase in the future as the business grows.

Participation in this Program is voluntary and at Smackdab's sole discretion. Smackdab may modify, suspend, or terminate this Program at any time.

---

2. PROGRAM SCOPE

2.1 Systems In Scope

Unless otherwise stated on this page, bounty eligibility generally follows the In-Scope Systems described in the VDP, including:

- app.smackdab.ai and related production service endpoints
- Public APIs documented at docs.smackdab.ai
- Official Smackdab mobile applications (iOS and Android)

Additional or temporary in-scope targets may be announced from time to time on this page or via our security channels.

2.2 Out-of-Scope Systems

The following are out of scope for bounty purposes, even if they may be in scope for VDP reporting:

- smackdab.ai (marketing website) and any associated WordPress infrastructure. Vulnerabilities on this system may be reported under our VDP but are not eligible for monetary bounties.
- Any third-party platforms or services not operated by Smackdab (including cloud providers, partners, integrations) unless the issue is clearly in Smackdab's configuration.
- Development, staging, demo, or internal environments, unless explicitly listed as in-scope on this page.
- Social media accounts, marketing microsites, or domains not listed as in scope.

You must still follow all VDP rules regarding prohibited activities (for example, no social engineering, no DoS, no accessing other customers' data).

2.3 Vulnerability Types Generally Excluded From Bounties

The following categories are typically ineligible for monetary rewards, though we may still appreciate and triage reports:

- Informational or low-impact issues that do not meaningfully affect confidentiality, integrity, or availability.
- Missing or low-impact security headers (for example, lack of X-Frame-Options on non-sensitive pages, or non-exploitable CSP findings).
- Clickjacking on pages without sensitive actions.

- CSRF on non-sensitive actions (for example, logout).
- Rate-limiting issues that do not lead to meaningful abuse or privilege escalation.
- Open redirects without clear security impact.
- SPF/DMARC/DKIM configuration suggestions that do not create exploitability.
- Account lockout, password complexity, or other hardening suggestions that do not lead to an exploitable weakness.
- Vulnerabilities that require a rooted or jailbroken device or a compromised local environment.

We may, at our discretion, award a bounty for issues in these categories if you demonstrate novel exploitation or significant business impact.

2.4 Known-Issue Categories

Smackdab is actively improving several known classes of issues (for example: user enumeration, missing rate limiting, basic reflected XSS, certain SSRF patterns, and oversized file uploads causing performance degradation).

We maintain an internal list of known-issue categories and vulnerabilities that have already been reported or are currently in remediation.

Reports that fall into a known-issue category may:

- Receive reduced or no bounty, especially if they are substantially similar to known issues; but
- Still qualify for triage and remediation, and may be eligible for recognition (for example, Hall of Fame) if they demonstrate a new exploitation path or high impact.

We will indicate in our response if your report falls into a known-issue category.

2.5 Optional Known Issues Pre-Check (Recommended)

Before performing extensive testing, Researchers may request a high-level overview of known-issue categories to avoid duplicating work and to understand what is unlikely to qualify for a bounty.

To request this:

- Email security@smackdab.ai with the subject line:

“Known Issues Request – Bug Bounty Program”

Smackdab will respond with a list of high-level known-issue categories that are already reported or in active remediation. For security reasons, this list will describe categories and general areas of concern, not detailed exploit information, code, or step-by-step instructions.

Reports that fall entirely within an existing known-issue category are typically ineligible for monetary bounty unless the Researcher demonstrates:

- A novel, substantially different exploitation path; or
- A significantly greater impact than the original report.

Requesting the Known Issues List is optional but strongly recommended. It helps Researchers focus on new, high-impact issues and reduces misunderstandings about bounty eligibility.

---

3. ELIGIBILITY TO PARTICIPATE

To be eligible for a bounty:

- You must be at least 18 years of age or the age of majority in your jurisdiction, whichever is greater.

You must not be:

- A resident of, or located in, a country or region subject to comprehensive U.S. sanctions (for example, Cuba, Iran, North Korea, Syria, the Crimea/Donetsk/Luhansk regions of Ukraine, or any other region embargoed by the U.S. government).
- On any U.S. or applicable international sanctions or restricted-party list (for example, OFAC's SDN List).

You must not be an employee, contractor, or current service provider of Smackdab, or an immediate family member thereof, unless explicitly permitted in writing.

You must not be prohibited by law or any prior contractual or employment obligations from participating.

Smackdab may request reasonable information (including identification and tax documentation) to verify eligibility before making any payment.

---

4. RULES OF ENGAGEMENT

By participating in this Program, you agree to:

Comply with the VDP

Follow all in-scope/out-of-scope definitions and prohibited activities specified in the VDP.

Use only your own accounts and data

Never attempt to access data belonging to other customers or users.

Create clearly identifiable test accounts (for example, prefixed with SECURITY*TEST*\), as described in the VDP.

Avoid service disruption

No denial-of-service attacks, resource-exhaustion testing, or excessive automated scanning.

Limit exploitation

Only exploit vulnerabilities to the minimal extent necessary to demonstrate impact.

Do not pivot laterally, maintain persistence, or exfiltrate real data.

Prompt reporting

Report vulnerabilities promptly and securely using the process below.

Do not use or share any discovered data or vulnerability information beyond what is necessary to report it to Smackdab.

Failure to follow these rules or the VDP may disqualify you from receiving any bounty and may void safe-harbor protections.

---

5. REPORTING PROCESS

5.1 How to Submit

Send your report to:

Email: security@smackdab.ai

Subject line: Bug Bounty Report: \[Short Issue Title\]

Your report should follow the structure defined in the VDP, including:

- Clear description of the vulnerability and potential impact.
- Exact affected URLs/endpoints, parameters, or components.
- Step-by-step reproduction instructions.
- Proof-of-concept demonstrating actual impact (without exposing personal data).
- Any relevant logs, screenshots, or traffic captures.
- Your CVSS assessment (if available).
- Your contact information and preferred payout method (if you are seeking a bounty).

5.2 Communication & Timelines

We aim to:

- Acknowledge eligible bounty submissions within 3 business days.

- Complete initial triage (validity and severity assessment) within 10 business days for most reports.
- Provide periodic updates for valid reports until remediation or a clear resolution path is determined.

We will notify you when:

- The vulnerability is validated,
- A fix or mitigation is deployed, and
- A bounty decision has been made (including severity rating and payout amount).

These are targets, not guarantees; complex issues may require more time. We will communicate if significant delays are expected.

---

6. SEVERITY ASSESSMENT & BOUNTY RANGES

Smackdab is an early-stage startup with a limited security budget. Our goal is to offer modest but meaningful rewards that reflect impact while remaining sustainable for our business.

We use the CVSS v3.1 framework together with Smackdab’s business context to determine severity. In general, the following ranges apply:

Critical (CVSS 9.0–10.0)

Example: unauthenticated remote code execution, direct access to large volumes of sensitive customer data, complete account takeover at scale.

Bounty range: 100–300 USD

High (CVSS 7.0–8.9)

Example: authenticated remote code execution, significant privilege escalation, direct access to sensitive data for a single account, serious injection vulnerabilities.

Bounty range: 50–150 USD

Medium (CVSS 4.0–6.9)

Example: stored or reflected XSS with meaningful impact, CSRF on sensitive actions, information disclosure that facilitates further attacks.

Bounty range: 25–75 USD

Low (CVSS 0.1–3.9)

Example: minor information leaks, clickjacking on semi-sensitive pages, low-impact misconfigurations.

Bounty range: 0–25 USD

We may, at our discretion, provide recognition without a monetary bounty for some low-severity issues.

6.1 How Smackdab Determines a Specific Amount Within a Range

For each valid report, we first determine severity (Low, Medium, High, or Critical). Within that severity band, we determine the specific payout amount based on three primary factors:

---

1. IMPACT AND BLAST RADIUS

- Whether the issue affects a single user, a single tenant, or multiple tenants or systems.
- Whether the issue leads to loss of confidentiality, integrity, or availability of customer or system data.

---

2. EXPLOITABILITY

- How easily a typical attacker could reproduce and reliably exploit the vulnerability.
- Whether exploitation requires rare conditions, unusual configurations, or advanced skills.

---

3. REPORT QUALITY AND ASSISTANCE

- Clarity and completeness of the writeup (steps, proof-of-concept, screenshots, logs).
- Whether the report includes context on impact, suggested mitigations, or testing of Smackdab’s patch.

As a rule of thumb:

- The lower end of a severity range is used for:
- Limited impact (for example, single-user or hard-to-reach contexts),
- Complex or unrealistic exploitation scenarios, or
- Minimal but sufficient report quality.
- The middle of a severity range is used for:
- Typical, clearly exploitable issues within that severity,
- Moderate to strong impact at the tenant level, and
- Solid, well-documented reports.
- The upper end of a severity range is reserved for:

- Broad impact (for example, multi-tenant or system-wide issues),
- Simple and reliable exploitation by a typical attacker, and
- Excellent report quality, including clear proof-of-concept and meaningful assistance with validation or remediation.

Reports that fall entirely into a known-issue category, or are substantially similar to previously reported vulnerabilities, will generally be rewarded (if at all) at the lower end of the applicable range, or may be ineligible for a bounty, even if the impact is significant. Novel, higher-impact variations of known issues may still qualify for payouts closer to the middle or upper end of the associated severity range.

6.2 Discretion and Maximum Payout

In addition to the factors listed above:

- Smackdab may, at its discretion, adjust payouts within the published ranges to reflect overall risk, duplication, or mitigation complexity.
- Smackdab may provide lower or no rewards for issues deemed low-impact or primarily theoretical.

Smackdab will not exceed a maximum payout of 300 USD for any single report under this Program. Bounty determinations are made at Smackdab’s sole discretion and are final.

---

7. DUPLICATE REPORTS, CHAINS, AND NON-QUALIFYING SUBMISSIONS

7.1 Duplicates

Bounties are generally awarded to the first valid report we receive that we can reproduce.

If multiple Researchers report the same underlying issue, only the earliest reproducible report will be eligible for a bounty.

Later duplicate reports may still be eligible for recognition (for example, Hall of Fame listing) at our discretion, but not for monetary rewards.

If your report is substantially similar to an issue that is already known or in active remediation, we may classify it as a duplicate of a known issue and treat it accordingly under this section and Sections 2.4 and 2.5.

7.2 Vulnerability Chains

When multiple issues must be combined to achieve impact (a “vulnerability chain”):

- We typically treat the chain as one report, and
- Pay a single bounty based on the overall impact of the chain.

If separate vulnerabilities in a chain would each independently qualify for a bounty, we may, at our discretion, adjust the reward upward, subject to the overall Program maximum.

7.3 Non-Qualifying Submissions

The following generally do not qualify for bounties:

- Reports without a clear security impact or exploitability.
- Reports that provide only automated scanner output, without analysis or demonstrated impact.
- Social engineering, phishing, vishing, or physical intrusion attempts.
- Issues that rely on outdated browsers or unsupported client platforms.
- Attacks that only affect users who have rooted or jailbroken devices or disabled core security mechanisms.

We encourage you to focus on high-impact, realistically exploitable vulnerabilities.

---

8. CONFIDENTIALITY & COORDINATED DISCLOSURE

You agree to:

- Treat your communications with Smackdab as confidential; and
- Not disclose any details of a vulnerability publicly until:
- We have confirmed remediation; and
- We have either approved your planned disclosure or 90 days have passed from initial acknowledgment, whichever occurs later, unless otherwise agreed in writing.

We may request:

- Additional time for complex or high-impact issues; or
- Redaction of specific technical or architectural details in your public writeup.

We are generally supportive of responsible public research and will work with you to coordinate publication timelines.

---

9. SAFE HARBOR

Smackdab’s Safe Harbor commitments are defined primarily in the VDP. In summary:

If you act in good faith, follow the VDP and these Terms, limit your testing to in-scope systems, and avoid causing harm:

- Smackdab will not pursue legal action against you solely for your participation in this Program.
- If a third party initiates legal action in connection with your compliant research, we will make it known that your actions were authorized under our policies (to the extent we can do so lawfully).

This safe harbor does not apply to:

- Actions that violate applicable law;
- Actions outside the scope or in violation of the VDP or these Terms;
- Intentional data exfiltration, extortion, or use of vulnerabilities for any purpose other than testing and reporting to Smackdab.

Safe harbor does not bind law enforcement or regulators.

---

10. PAYMENTS, TAXES, AND COMPLIANCE

Payment Method

All bounty payments are made exclusively via PayPal, in United States dollars (USD).

To receive a bounty, you must:

- Have a valid PayPal account in good standing that is able to receive payments from the United States; and
- Provide the PayPal account details we request during the payout process.

We do not currently support alternative payout methods such as bank transfer, Wise, cryptocurrency, or gift cards. If you are unable to receive payments via PayPal, you may still report vulnerabilities under our Vulnerability Disclosure Policy, but you will not be eligible for monetary bounties under this Program.

Tax Obligations

You are responsible for reporting and paying any applicable taxes on bounty payments.

For certain amounts or jurisdictions, we may require you to complete tax forms (for example, IRS Form W-9 or Form W-8BEN) prior to payment and may withhold taxes as required by law.

KYC and Verification

Smackdab may request reasonable identity or residency verification, and may screen you against applicable sanctions and restricted-party lists, to comply with sanctions, anti-money-laundering, tax, and other legal requirements.

No Assignment of Employment

Participation in the Program does not create an employment, partnership, agency, or joint-venture relationship between you and Smackdab.

---

11. PROGRAM CHANGES & TERMINATION

Smackdab may:

- Modify the scope, eligibility conditions, bounty ranges, or any other aspect of this Program at any time; or
- Pause or terminate the Program entirely, or for specific systems or regions, at any time.

Changes will be published on this page with an updated “Last Updated” date. Material changes may also be announced through our security channels.

For vulnerabilities reported before the effective date of a change, the Program terms in effect at the time of your report will generally apply. For vulnerabilities reported after a change, the updated Terms will apply.

---

12. CONTACT

For questions about these Terms or the Bug Bounty Program, contact:

Email: security@smackdab.ai

This PDF is the formal downloadable version of BUG BOUNTY PROGRAM TERMS.