absorb

Bug Bounty Program

Last Updated: January 10, 2025

Overview

At **Absorb**, we are deeply committed to safeguarding the security and privacy of our users. We understand that a secure platform builds trust, and user trust is at the heart of everything we do. To uphold this commitment, we have established a "**Bug Bounty Program**" that welcomes the expertise of security researchers and ethical hackers from around the globe.

The program is designed to foster collaboration between our internal security team and the vibrant cybersecurity community. We believe that many minds are better than one, and by opening our platform to scrutiny, we create an additional layer of defense against emerging threats. Your contributions are invaluable to us—they help us uncover vulnerabilities before they can be exploited by malicious actors, allowing us to enhance our infrastructure and keep our users safe.

We encourage skilled security researchers to responsibly disclose any vulnerabilities they discover in our systems. By participating in our Bug Bounty Program, you have the opportunity to make a meaningful impact on our platform's security, directly contributing to a safer digital experience for millions of users. In recognition of your expertise and dedication, we offer rewards commensurate with the severity of the vulnerabilities you find.

At **Absorb**, we know that security is a shared responsibility, and we are proud to partner with those who share our commitment to making the internet a safer place. Whether you are an experienced professional or just beginning your journey in cybersecurity, we welcome your expertise. Together, we can strengthen our defenses and build a platform that our users can trust, today and into the future.

By participating in this Bug Bounty Program, you acknowledge and agree to abide by all terms and conditions outlined herein. Your submission of a vulnerability report signifies your acceptance of the program's rules, including its scope, eligibility criteria, disclosure policy, and other provisions. Any actions taken as part of your participation must align with these terms, and failure to comply may result in disqualification from the Bug Bounty Program and potential legal consequences. By agreeing to these terms, you contribute to a collaborative and secure environment that prioritizes ethical research and responsible vulnerability disclosure.

Scope

A. In-Scope Targets

The following assets and services are currently within the scope of our Bug Bounty Program. We encourage researchers to focus their efforts on these specific domains, applications, and systems:

- Web Applications:
    - Absorblms.com
    - Myabsorb.com
    - Myabsorb.ca
    - Myabsorb.eu
    - Togetherplatform.com
    - Koantic.com
    - Absorbtechnology.com
    - Absorbtechnology.co.uk

B. Out-of-Scope Targets

To prevent wasted efforts and ensure that researchers focus on critical areas, the following are explicitly out of scope:

- Third-party services or integrations not owned or managed by **Absorb**.
- Denial of Service (DoS/DDoS) attacks: Any activity that could degrade the availability of our services is not allowed.
- Social Engineering attacks against **Absorb** employees, customers, or partners.
- Physical Attacks or methods requiring physical access to our offices, data centers, or employee devices.
- Vulnerabilities in out-of-date browsers or unsupported software versions.

C. Eligible Vulnerabilities

We're interested in identifying vulnerabilities that could compromise our platform, user data, or other core systems. Eligible types of vulnerabilities include, but are not limited to:

- Remote Code Execution (RCE)
- Cross-Site Scripting (XSS)
- SQL Injection (SQLi)
- Broken Authentication or Authorization
- Insecure Direct Object References (IDOR)
- Cross-Site Request Forgery (CSRF)
- Privilege Escalation
- Server-Side Request Forgery (SSRF)
- Security Misconfigurations

D. Non-Eligible Vulnerabilities

To streamline efforts, the following types of reports will not be considered eligible for rewards unless they can demonstrate an actual security risk:

- Best Practices: Issues related to security headers (e.g., missing X-Frame-Options).
- Clickjacking on pages that do not include sensitive functionality.
- Rate limiting on non-sensitive actions.
- Reports from automated tools or scanners without proof of concept.
- Missing SPF, DKIM, or DMARC records without evidence of significant exploitability.
- Username Enumeration: Unless it is linked to a significant attack vector.

Rewards

We value the contributions of security researchers in helping us identify and address vulnerabilities to improve the security of our systems. Rewards for valid submissions are based on the severity, impact, and quality of the report, as determined by our internal evaluation process. Below is an overview of our reward structure:

A. Reward Structure

Severity Level	Reward Range	Example Vulnerabilities
Critical	$5,000+	Severe vulnerabilities with a high impact on security, privacy, or system integrity (e.g. Remote Code Execution (RCE), unauthorized data access, or significant authentication bypass).
High	$1,000 - $5,000	Significant vulnerabilities that could lead to unauthorized access or data breaches (e.g. privilege escalation, SQL injection, or access to sensitive data).
Medium	$500 - $1,000	Vulnerabilities that could potentially impact user data or system stability (e.g. Cross-Site Scripting (XSS), significant security misconfigurations).
Low	$100 - $500	Minor security issues with limited impact (e.g. minor input validation issues or misconfigurations with limited impact).

B. Eligibility for Rewards

To qualify for rewards, only vulnerabilities identified within the defined in-scope assets and systems will be considered eligible. Submissions must include a detailed and clear proof of concept (**PoC**) that demonstrates how the vulnerability can be exploited and explains its potential impact on the system, including risks to data security, system integrity, or user privacy. The PoC should be thorough enough to allow for efficient validation and remediation of the issue by our team. Furthermore, the reported vulnerability must be unique and not previously reported, discovered, or known to **Absorb**. Duplicate reports or issues that have already been resolved or acknowledged will not be eligible for rewards. This ensures that the program remains focused on identifying and addressing novel security issues that improve the overall safety and resilience of our systems.

C. Factors infliuncing Rewards

The reward for a reported vulnerability is determined by evaluating several key factors that reflect its severity, impact, and the quality of the submission. Impact assesses the potential damage or risk posed by the vulnerability, such as unauthorized access to sensitive data, compromise of system integrity, or disruption of critical business operations. Vulnerabilities with high potential to harm user privacy, data security, or organizational reputation will be weighted more heavily. Exploitability evaluates how easily the vulnerability can be exploited in a real-world scenario, taking into account factors such as whether the exploit requires specialized skills, specific conditions, or significant effort. Vulnerabilities that can be easily and reliably exploited pose a higher risk and are therefore more highly rewarded.

Additionally, Report Quality is a crucial component in determining rewards. Submissions that include clear, detailed, and well-organized explanations of the issue, accompanied by a comprehensive PoC demonstrating the exploit and its impact, will receive greater consideration. High-quality reports that also provide actionable suggestions for remediation help expedite the resolution process and add significant value to the Bug Bounty Program. This ensures that rewards not only reflect the technical severity of the vulnerability but also the effort and professionalism of the researcher, encouraging thorough and impactful contributions to the program.

D. Payment Process

Rewards for validated vulnerabilities will be paid within ninety (90) days following the successful validation and approval of the report by our security team. The payment process is designed to be prompt and efficient, ensuring that researchers are compensated fairly for their contributions. However, to maintain compliance with legal and regulatory standards, researchers may need to complete a verification process, which may include providing personal identification, tax documentation, or other relevant information to confirm their eligibility for payment.

Furthermore, researchers must agree to comply with all applicable tax laws and legal requirements based on their jurisdiction. This includes being responsible for reporting and paying any taxes owed on the rewards received. By adhering to these processes, we aim to ensure a transparent, secure, and compliant reward distribution system that recognizes the efforts of researchers while meeting organizational and regulatory obligations. These measures help maintain the integrity of the Bug Bounty Program and provide assurance to both researchers and the organization.

E. Additional Terms

Reports for vulnerabilities classified as low-severity or non-exploitable may not be eligible for monetary rewards, as they pose minimal risk to system functionality, data security, or user privacy. However, we value all contributions and, at our discretion, may offer recognition for these findings to acknowledge the researcher's efforts.

Additionally, to maintain fairness and efficiency, rewards for any vulnerability will be granted only to the first valid and complete report received for a particular issue. Subsequent submissions identifying the same vulnerability, referred to as duplicate reports, will not be eligible for rewards. This approach incentivizes prompt reporting and ensures that researchers are appropriately recognized for their discoveries while minimizing duplication of effort within the program. By upholding these principles, we aim to create a balanced system that rewards impactful contributions and encourages collaboration toward enhancing system security.

Reporting Guidelines

To report a vulnerability, please follow these steps:

- **Submit your report**: Use our security@absorblms.com to send your report. Ensure that all required fields are filled out, and provide as much relevant information as possible. A well-structured and detailed submission allows us to promptly evaluate and address the issue
- **Include details**: Provide a clear and concise description of the vulnerability, including the specific component, feature, or endpoint affected. Include step-by-step instructions to reproduce the issue, ensuring that even someone unfamiliar with your testing process can replicate the findings. Clearly outline the potential impact of the vulnerability, such as its effect on data security, user privacy, or system availability.

- **Proof of concept**: Enhance your submission by including a PoC that demonstrates the exploitability of the vulnerability. This could be in the form of screenshots, videos, or code snippets that illustrate the issue. A PoC helps our team understand the issue quickly and confirms the vulnerability's existence and scope.
- **Impact assessment**: Explain the potential impact of the vulnerability on our systems, users, and data. For example, detail whether the issue could result in unauthorized access, data leakage, denial of service, or other security risks. A thorough assessment helps us prioritize the remediation process and allocate resources appropriately.
- **Mitigation suggestions**: If possible, provide suggestions on how to mitigate or resolve the vulnerability. This could include recommendations for configuration changes, code fixes, or process improvements. While optional, mitigation suggestions are highly valued as they can expedite the resolution process and enhance the overall effectiveness of the remediation effort.

Response Process

Absorb will follow the below process upon receipt of a report:

- **Acknowledgment**: We will acknowledge receipt of your vulnerability report to confirm that your submission has been received and logged into our tracking system. Our acknowledgment will include a reference ID for your report, allowing you to track its status and ensure transparency throughout the process.
- **Assessment**: Our security team will thoroughly assess the report to determine its validity, reproducibility, and severity. This includes verifying the vulnerability, evaluating its potential impact on our systems and users, and prioritizing it based on risk. During this phase, we may reach out to you for additional details or clarification to aid in our investigation.
- **Resolution**: If the vulnerability is confirmed as valid, our team will work on developing and implementing a fix. The timeline for resolution will depend on the complexity and severity of the issue, with critical vulnerabilities being addressed on a priority basis. Throughout the process, we will provide periodic updates to inform you of the progress and expected resolution timeframe.
- **Reward**: Once the vulnerability is successfully resolved and the fix has been deployed, we will evaluate the report for reward eligibility based on its severity, impact, and the quality of your submission. Rewards will be issued promptly according to the terms of this program, and we may also provide recognition for your valuable contribution to improving our security posture.

Disclosure Policy

We are committed to collaborating with security researchers to identify, verify, and address reported vulnerabilities in a timely and responsible manner. Upon receiving a vulnerability report, our security team will evaluate the issue and work diligently to implement a fix that minimizes risks to our systems, users, and stakeholders.

To ensure the integrity and security of our platform, we ask that researchers allow us a reasonable and mutually agreed-upon period to resolve the vulnerability before making any public disclosure. This timeline may vary depending on the complexity and severity of the issue, but we will maintain open communication with you throughout the process to provide updates on progress and resolution status.

Legal

This Bug Bounty Program is designed to foster a collaborative approach to improving the security of our systems and services. By participating, you agree to abide by the terms and conditions outlined below to ensure the program remains ethical, legal, and productive. These rules are essential to maintaining trust and cooperation between researchers and **Absorb**, ensuring a secure and responsible process for identifying and resolving vulnerabilities.

- **Compliance with Laws**

By participating in this program, you agree to comply with all applicable local, state, national, and international laws. This includes adhering to cybersecurity laws and regulations in your jurisdiction and avoiding actions that may result in legal liability for yourself or **Absorb**.

- **No Unauthorized Access**

Participants must not access, modify, or delete any data that does not belong to them. Any attempt to access sensitive data, including user information or proprietary company data, without explicit authorization is a breach of this agreement and will result in immediate disqualification from the Bug Bounty Program and may result in legal action.

- **No Disruption**

You must ensure that your testing activities do not disrupt or degrade our services. Actions such as Denial of Service (DoS) attacks or activities that negatively impact system availability or user experience are strictly prohibited.

- **No Social Engineering**

Social engineering attacks, such as phishing, vishing, or impersonation, against employees, contractors, or users of **Absorb** are not permitted. The Bug Bounty Program is focused on technical vulnerabilities, and any attempt to manipulate individuals to gain unauthorized access is strictly forbidden.

- **No Physical Attacks**

Participants are prohibited from engaging in physical attacks against our infrastructure, including offices, data centers, or any physical property of **Absorb**. All activities under this Bug Bounty Program must be conducted remotely and within the digital domain.

- **No Automated Scanning**

Automated scanning tools are not allowed unless explicitly authorized by **Absorb**. Tools that generate excessive traffic or false positives can degrade service quality. Any vulnerabilities discovered through automated tools must be manually verified before submission to ensure accuracy and relevance.

- **Confidentiality**

You agree to keep all details of discovered vulnerabilities confidential until they have been resolved and publicly disclosed by **Absorb**. Premature disclosure could expose users to risks and will be treated as a violation of this agreement.

- **No Public Disclosure**

Participants are prohibited from publicly disclosing vulnerabilities without prior written consent from **Absorb**. Unauthorized disclosure will result in disqualification from the Bug Bounty Program and may lead to legal action. This ensures vulnerabilities are addressed responsibly without exposing users to potential harm.

- **Intellectual Property**

All reports, suggestions, or feedback submitted as part of this Bug Bounty program become the property of **Absorb**. By participating, you grant **Absorb** a perpetual, irrevocable, worldwide, royalty-free license to use, modify, and distribute your submissions for any purpose.

- **No Compensation for Ineligible Reports**

Absorb reserves the right to determine the eligibility of any report. Reports that do not meet the criteria outlined in this Bug Bounty Program or that identify vulnerabilities outside the defined scope will not be eligible for rewards or compensation.

- **Termination**

We reserve the right to terminate or modify this Bug Bounty Program at any time without prior notice. Continued participation after modifications constitutes your acceptance of the revised terms. This flexibility ensures the program remains aligned with organizational goals and legal requirements.

- **Indemnification**

By participating, you agree to indemnify, defend, and hold harmless **Absorb**, its affiliates, and their officers, directors, employees, and agents from any claims, damages, or liabilities arising from your participation in the Bug Bounty Program. This protects **Absorb** from risks associated with unauthorized or harmful activities.

- **Governing Law**

This Bug Bounty Program and its terms are governed by the laws of Delaware, without regard to conflict of laws principles. Any disputes arising from participation will be resolved under the applicable legal framework in the specified jurisdiction.

These terms are critical to maintaining a secure, ethical, and professional Bug Bounty Program. By adhering to these rules, participants and **Absorb** can work together effectively to enhance security and protect users.

Contact

If you have any questions, need clarification on the scope or rules of the Bug Bounty Program, or wish to report a vulnerability, please contact us at security@absorblms.com

For urgent matters, such as reporting a critical vulnerability with immediate security implications, please include "Urgent" in the subject line of your email or select the appropriate priority option in the submission form.

Our security team is available to address inquiries and review submissions during normal business hours Monday–Friday, 9:00 AM–5:00 PM MST. We will respond to your submission in accordance with the Response Process outlined herein.

We appreciate your efforts in contributing to the security of our systems and are committed to working collaboratively with researchers to address potential vulnerabilities.