Yahoo!

Build Brands Members Love

https://www.yahoo.com · @yahoo

Reports resolved
11249

Assets in scope
63

Average bounty
$500

Submit report

Gold standard

Bug Bounty Program
Launched on Feb 2014

Managed by HackerOne
Safe Harbor
Includes retesting
Collaboration enabled

Bookmark Subscribe

Policy Scope New! Hacktivity Thanks Updates (39) Collaborators Safe Harbor

Rewards

Low	Medium	High	Critical
$100 - $500	$500 - $3,000	$3,000 - $10,000	$10,000 - $15,000

Updating the table to reflect our bounty ranges

Last updated on October 7, 2022. View changes

Policy

Welcome to Yahoo!

Yahoo is a global media and advertising company connecting people to their passions. With one of the largest online audiences in the world, Yahoo brings people closer to what they love — from finance and commerce, to gaming and news — with the trusted products, content and tech that fuel their day. For partners, we provide a full-stack platform to amplify businesses and drive more meaningful connections across advertising, search and media.

We are Paranoid

Our information security team is known as the Paranoids, and we're committed to protecting our brands and our users. As part of this commitment, we invite security researchers to help protect Yahoo and its users by proactively identifying security vulnerabilities via our bug bounty program. Our program is inclusive of all Yahoo brands and offers competitive rewards for a wide array of vulnerabilities. We encourage security researchers looking to participate in our bug bounty program to review our policy to ensure compliance with our rules and also to help you safely verify any vulnerabilities you may uncover.

Response Efficiency

8 hrs
Average time to first response

9 days
Average time to triage

about 1 month
Average time to bounty

85% of reports
Meet response standards
Based on last 90 days

Program Statistics
Updated Daily

>$22,740,000
Total bounties paid

$500
Average bounty

$6,000 - $40,000
Top bounty range

$160,000
Bounties paid in the last 90 days

170
Reports received in the last 90 days

2 days ago
Last report resolved

11249
Reports resolved

1778
Hackers thanked

Top hackers

mayonaise
Reputation:14733

dawgyg

Paranoids

Table of Contents

Rules of Engagement

By submitting reports or otherwise participating in this program, you agree that you have read and will follow the Program Rules and Legal Terms sections of this program Policy.

Program Rules

Violation of any of these rules can result in ineligibility for a bounty and/or removal from the program. Three strikes will earn you a temporary ban. Four strikes means a permanent ban.

1. Test vulnerabilities only against accounts that you own or accounts that you have permission from the account holder to test against.
2. Never use a finding to compromise/exfiltrate data or pivot to other systems. Use a proof of concept only to demonstrate an issue.
3. If sensitive information--such as personal information, credentials, etc.--is accessed as part of a vulnerability, it must not be saved, stored, transferred, accessed, or otherwise processed after initial discovery. All copies of sensitive information must be returned to Yahoo and may not be retained. To ensure you are fully protected under the 'Gold Standard Safe Harbor', you may only use potentially-sensitive data to validate your finding, report it to us and to verify if the applied fix is effective.
4. Researchers may not, and are not authorized to engage in any activity that would be disruptive, damaging or harmful to Yahoo, its brands or its users. This includes: social engineering, phishing, physical security and denial of service attacks against users, employees, or Yahoo as a whole.
5. Abide by the program scope. Only reports submitted to this program and against assets in scope will be eligible for monetary award.
6. Researchers may not publicly disclose vulnerabilities (sharing any details whatsoever with anyone other than authorized Yahoo or HackerOne employees), or otherwise share vulnerabilities with a third party, without Yahoo's express written permission.

Legal Terms

In connection with your participation in this program you agree to comply with Yahoo's Terms of Service, Yahoo's Privacy Policy, and all applicable laws and regulations, including any laws or regulations governing privacy or the lawful processing of data.

Yahoo reserves the right to change or modify the terms of this program at any time. You may not participate in this program if you are a resident or individual located within a country appearing on any U.S. sanctions lists (such as the lists administered by the US Department of the Treasury's OFAC).

Yahoo does not give permission/authorization (either implied or explicit) to an individual or group of individuals to (1) extract personal information or content of Yahoo users or publicize this information on the open, public-facing internet without user consent or (2) modify or corrupt programs or data belonging to Yahoo in order to extract and publicly disclose data belonging to Yahoo.

Yahoo employees (including former employees that separated from Yahoo within the prior 12 months), contingent workers, contractors and their personnel, and consultants, as well as their immediate family members and persons living in the same household, are not eligible to receive bounties or rewards of any kind under any Yahoo programs, whether hosted by Yahoo or any third party.

Safe Harbor

Gold Standard Safe Harbor applies

Please submit a report to us before engaging in conduct that may be inconsistent with or unaddressed by this Policy.

Responsible Disclosure of Vulnerabilities

We are continuously working to evolve our bug bounty program. We aim to respond to incoming submissions as quickly as possible and make every effort to have bugs fixed within 90 days of being triaged.

All products and services owned by Yahoo are included in either our public or Elite bug bounty program. Please review the program scope before submitting a report. *Elite scope is accessible to invited researchers only.*

Testing

Web traffic to and from Yahoo properties produces petabytes of data every day. When testing, you can make it easier for us to identify your testing traffic against our normal data and the malicious actors out in the world. Please do the following when participating in Yahoo bug bounty programs:

- Where possible, register accounts using your <username>+x@wearehackerone.com addresses. Some of our properties will require this to be eligible for a bounty.

Reputation:14096


nnwakelam
Reputation:12713


todayisnew
Reputation:9747


mlitchfield
Reputation:7547

- Provide your IP address in the bug report. We will keep this data private and only use it to review logs related to your testing activity.
- Include a custom HTTP header in all your traffic. Burp and other proxies allow the easy automatic addition of headers to all outbound requests. Report to us what header you set so we can identify it easily.

Identifier	Format	Example
Your Username	X-Bug-Bounty: HackerOne-<username>	X-Bug-Bounty: HackerOne-flyingtoasters
Unique Identifier	X-Bug-Bounty: ID-<sha256-flag>	X-Bug-Bounty: ID-6223b07c5323f18b59a70c3ce1b057c56d0eb39de620db6307279deb737ce60c
Event Identifier	X-Bug-Bounty:LiveHackingEvent-<eventid>	X-Bug-Bounty: LiveHackingEvent-H1-213
Tool Identifier	X-Bug-Bounty: <toolname>	X-Bug-Bounty: BurpSuitePro
Verbose Tool Identifier	X-Bug-Bounty: <toolname>-version-<version>	X-Bug-Bounty: BurpSuitePro-version-2020.1

When testing for a bug, please also keep in mind:

- Only use authorized accounts so as not to inadvertently compromise the privacy of our users
- When attempting to demonstrate root permissions with the following primitives in a vulnerable process please use the following commands:
  - Read: cat /proc/1/maps
  - Write: touch /root/<your H1 username>
  - Execute: id, hostname, pwd (though, technically cat and touch also prove execution)
- Minimize the mayhem. Adhere to program rules at all times. Do not use automated scanners/tools - these tools include payloads that could trigger state changes or damage production systems and/or data.
- Before causing damage or potential damage: Stop, report what you've found and request additional testing permission.

Crafting a Report

If our security team cannot reproduce and verify an issue, a bounty cannot be awarded. To help streamline our intake process, we ask that submissions include:

- Description of the vulnerability
- Steps to reproduce the reported vulnerability
- Proof of exploitability (e.g. screenshot, video)
- Perceived impact to another user or the organization
- Proposed CVSSv3 Vector & Score (without environmental and temporal modifiers)
- List of URLs and affected parameters
- Other vulnerable URLs, additional payloads, Proof-of-Concept code
- Browser, OS and/or app version used during testing

Note: Failure to adhere to these minimum requirements may result in the loss of a reward.

All supporting evidence and other attachments must be stored only within the report you submit. Do not host any files on external services.

Program Scope

Vulnerabilities on a specific brand or web property should be reported to the program to which it is listed "in scope". Please see our detailed scope list at the bottom of this page for a full list of assets that are in scope of this program. This list is subject to change without notice.

To reduce the amount of assets listed in each program we operate, out of scope assets are only listed on our public program policy page.
If you've found a vulnerability that affects an asset belonging to Yahoo, but is not included as in scope on any of the Yahoo programs, please report it to this program.

Rewards

You will be eligible for a bounty only if you are the first person to disclose an unknown issue. Qualifying bugs will be rewarded based on severity, to be determined by Yahoo in its sole discretion. Rewards may range from HackerOne Reputation Points and swag to monetary rewards up to $15,000 USD. Awards are granted entirely at the discretion of Yahoo.

At Yahoo's discretion, providing more complete research, proof-of-concept code and detailed write-ups may increase the bounty awarded. Conversely, Yahoo may pay less for vulnerabilities that require complex or over-complicated interactions or for which the impact or security risk is negligible. Rewards may be denied if there is evidence of program policy violations. *A reduction in bounty is also warranted for reports that require specific browser configurations.* Reports in third party software are not eligible for bounties.

Payout Table

Where a monetary bounty is presented, eligible reports will be awarded based on severity after identifying final impact, as determined by Yahoo.

Severity	Payout Range
Critical	$10,000 - $15,000
High	$3,000 - $10,000
Medium	$500 - $3,000
Low	$100 - $500
Informative	$0 - $0

Valued Vulnerabilities

All reports will be awarded based on the Common Weakness Enumeration classification. This table provides the CWEs that we will accept, the severity ranges we will classify reports within for the CWE, and some examples of common vulnerability and attack names that we classify within each CWE that we will accept. This table serves only as a guide and

the severity classification of a particular vulnerability will be determined by Yahoo in its sole discretion.

Note: Non-listed vulnerabilities may also be eligible. Some vulnerability types may fall under a variety of severity ratings determined by scope/scale of exploitation and impact.

Severity (low)	Severity (high)	CWE-ID	Common Weakness Enumeration	Bug Examples
None	Medium	CWE-16	Misconfiguration	Brand SDTO (a.k.a. Subdomain Takeover); Untrusted DNS Target; Dangling CNAME Takeover; Non-Primary Brand SDTO; DNS Zone Takeover
Critical	Critical	CWE-78	OS Command Injection	Code Injection; LDAP Injection; Remote Code Execution
Low	Medium	CWE-79	Cross-Site Scripting	Stored XSS; POST-Based XSS; GET-Based XSS; DOM-Based XSS; CSS Injection
High	Critical	CWE-89	SQL Injection	SQL Injection
Critical	Critical	CWE-91	XML Injection	XML Injection
Medium	Medium	CWE-93	CRLF Injection	CRLF Injection
Critical	Critical	CWE-120	Classic Buffer Overflow	Buffer Overflow
High	Critical	CWE-134	Uncontrolled Format String	Insecure Deserialization
Medium	Critical	CWE-138	Improper Neutralization of Special Elements	Path Normalization
Low	High	CWE-200	Information Exposure	User Enumeration with Personal Information; Credentials on GitHub; Confidential Information Exposure; Information Disclosure
Low	Low	CWE-203	Information Exposure Through Discrepancy	PHP Admin Information page; MySQL Information page (w/ credentials); Apache Status page
High	High	CWE-250	Execution with Unnecessary Privileges	Privilege Escalation to System Account
Low	Medium	CWE-284	Improper Access Control	Environment Exposure
Medium	Critical	CWE-287	Improper Authentication	Lack of Authentication
Low	Low	CWE-304	Missing Critical Step in Authentication	T2 Login Page exposed
Medium	High	CWE-306	Missing Authentication for Critical Function	Exposed Administrative Interface
Informative	Low	CWE-307	Improper Restriction of Excessive Authentication Attempts	Lack of Rate Limiting on Login; CAPTCHA Bypass
Low	Low	CWE-311	Missing Encryption of Sensitive Data	Cleartext Submission of Passwords
Informative	Low	CWE-327	Use of a Broken or Risky Cryptographic Algorithm	Weak CAPTCHA
Medium	High	CWE-352	Cross-Site Request Forgery	State-Changing CSRF; Non-State-Changing CSRF
Informative	Informative	CWE-359	Privacy Violation	Privacy Violation
Medium	High	CWE-434	Unrestricted Upload of File with Dangerous Type	Unfiltered File Upload
Informative	Low	CWE-427	Uncontrolled Search Path Element	Closed Redirect
Medium	High	CWE-444	Inconsistent Interpretation of HTTP Requests	HTTP Request Smuggling

All Hackers

Severity (low)	Severity (high)	CWE-ID	Common Weakness Enumeration	Bug Examples
Medium	Medium	CWE-494	Download of Code Without Integrity Check	S3 Bucket Upload
Low	Low	CWE-601	Open Redirect	Open Redirect
Critical	Critical	CWE-611	Improper Restriction of XML External Entity Reference	XXE
Low	Low	CWE-706	Use of Incorrectly-Resolved Name or Reference	Incorrectly Resolved Name
Medium	High	CWE-732	Incorrect Permission Assignment for Critical Resource	Horizontal Privilege Escalation; Vertical Privilege Escalation; IDOR (RW, Cross Org); IDOR (RW, Same Org)
Low	High	CWE-798	Use of Hard-coded Credentials	Hard Coded Credentials
Informative	High	CWE-829	Inclusion of Functionality from Untrusted Control Sphere	Server Side Includes Injection; Local File Inclusion; Directory Traversal; Production Host Dependency Confusion; non-Production Host Dependency Confusion
Medium	High	CWE-862	Missing Authorization	Horizontal Privilege Escalation; Vertical Privilege Escalation; IDOR (RO, Same Org); IDOR (RO, Cross Org)
Informative	High	CWE-863	Incorrect Authorization	Authorization Bypass; Account Takeover; Social Media Takeover (Brand, <12mo, w/creds); Social Media (w/o creds)
Medium	Critical	CWE-918	Server-Side Request Forgery	Semi-Blind SSRF (Service level); Semi-Blind SSRF (Host level); Blind SSRF; Semi-Blind SSRF (File Contents); Semi-Blind SSRF (File Existence); Unrestricted SSRF; Content-Restricted SSRF (Multiple); Content-Restricted SSRF (Single)
Low	Low	CWE-941	Incorrectly Specified Destination in a Communication Channel	Incorrect Destination

Borderline Out-of-Scope, No Bounty

These issues are eligible for submission, but not eligible for bounty or any award. Once triaged, they will be closed as Informative only if found to be valid or Spam if found to be not valid. When reporting vulnerabilities, please consider (1) attack scenario / exploitability, and (2) security impact of the bug.

Any non-Yahoo Applications	"Self" XSS
Missing Security Best Practices	HTTP Host Header XSS
Confidential Information Leakage	Clickjacking/UI Redressing
Use of known-vulnerable library (without proof of exploitability)	Intentional Open Redirects
Missing cookie flags	Reflected file download
SSL/TLS Best Practices	Incomplete/Missing SPF/DKIM
Physical attacks	Social Engineering attacks
Results of automated scanners	Login/Logout/Unauthenticated CSRF
Autocomplete attribute on web forms	Using unreported vulnerabilities
"Self" exploitation	Issues related to networking protocols
Flash-based XSS	Software Version Disclosure
Verbose error pages (without proof of exploitability)	Denial of Service attacks
Yahoo software that is End of Life or no longer supported	Account/email Enumeration
Missing Security HTTP Headers (without proof of exploitability)	Internal pivoting, scanning, exploiting, or exfiltrating data

Note: 0-day and other CVE vulnerabilities may be reported 30 days after initial publication (CVE List Status of Published). We have a team dedicated to tracking CVEs as they are released; hosts identified by this team and internally ticketed will not be eligible for bounty.

Do Not Report

The following issues are considered out of scope:

- Those that resolve to third-party services
- Issues that do not affect the latest version of modern browsers
- Issues that we are already aware of or have been previously reported
- Issues that require unlikely user interaction

- Disclosure of information that does not present a significant risk
- Cross-site Request Forgery with minimal security impact
- CSV injection
- General best practice concerns
- All Flash-related bugs

Special Situations

Some situations exist that may earn partial bounties or bonuses on top of a base bounty per report. Here are a few of the most common examples.

Same Bug, Different Host

For each report, please allow Yahoo sufficient time to patch other host instances. If you find the same bug on a different (unique) host, prior to the report reaching a triaged state, file it within the existing report to receive an additional 5% bonus (per host, not domain). Any reports filed separately *while we are actively working to resolve the issue* will be treated as a duplicate.

Same Bug, Different Path

For each report, please allow Yahoo sufficient time to patch related paths. If you find the same bug on a different (unique) path, prior to the report reaching a triaged state, file it within the existing report to receive an additional 5% bonus (per path). Any reports filed separately *while we are actively working to resolve the issue* will be treated as a duplicate.

Same Payload, Different Parameter

In some cases, rewards may be consolidated into a single payout. For example, multiple reports of the same vulnerability across different parameters of a resource, or demonstrations of multiple attack vectors against a fundamental framework issue. We kindly ask you to consolidate reports rather than separate them.

Note: Additional payloads, parameters, hosts and paths will not receive multiple bonuses.

Last updated on November 16, 2022. View changes

> Looking for what's in scope? Check out the new Scope tab above.

© HackerOne