Ultra.cc Bug Bounty Program

Ultra.cc Bug Bounty Program

Security is core to our values, and we value the input of security researchers to help us maintain a high standard for security and privacy for our users. This includes encouraging responsible vulnerability research and disclosure. This policy sets out our definition of good-faith in the context of finding and reporting vulnerabilities, as well as what you can expect from us in return.

Expectations

When working with us according to this policy, you can expect us to:

- Work with you to understand and validate your report, including timely initial response to the submission;
- Work to remediate discovered vulnerabilities promptly; and
- Recognize your contribution to improving our security if you are the first to report a unique vulnerability, and your report triggers a code or configuration change.

Scope

The following are the list of platforms that are within this scope of the program.

- Ultra.cc Website [https://ultra.cc]
- Ultra.cc Control Panel [https://cp.ultra.cc]
- Ultra.cc App Hosting Solutions Infrastructure [`<servername>`.usbx.me]

Out of Scope

- WHMCS Client Area [https://my.ultra.cc] - These should be reported to the WHMCS software developer via their Bug Bounty Program
- Security bugs that do not affect our default applications configuration.
- Security bugs that do not affect our dockerized containers.
- Timing attacks which reveal information.
- Methods to reveal information about other running processes.
- Denial of service attacks or other volume-based attacks
- Phishing attacks
- Usage of large-scale vulnerability scanners, scrapers, or automated tools that produce excessive amounts of traffic

Rewards

Ultra.cc Website and User Control Panel

Category	UP TO* PayPal Credit	UP TO* Service Credit
XSS	EUR 100	EUR 200
XSS (Bypassing CSP)	EUR 200	EUR 300
CSRF	EUR 300	EUR 450
Authentication Bypass	EUR 500	EUR 750
SQL Injection	EUR 1000	EUR 1500
Arbitrary code execution	EUR 1000	EUR 1500
Arbitrary code execution (with privilege escalation)	EUR 2000	EUR 3000
Persistent code change	EUR 1000	EUR 1500

Ultra.cc App Hosting Solutions Infrastructure

Category	UP TO* PayPal Credit	UP TO* Service Credit
Authentication Bypass (SSH, FTP, VPN, etc.)	EUR 500	EUR 750
Authentication Bypass of Supported Apps	EUR 100	EUR 200
Local privilege escalation	EUR 500	EUR 750

`*` Payout Determination Policy

We determine payout values based on the risk and impact to our systems and users. Our evaluations are fair and honest, reflecting the actual security threat posed by the vulnerability. For instance, a researcher might identify a logical flaw, but if this flaw requires particular conditions that are unlikely to occur in a real-world scenario, the payout will be adjusted accordingly.

Additionally, vulnerabilities that involve accessing data already available to the researcher through another tab or session will be assessed based on the risk of unauthorized access or exposure. While we value all contributions, the payout for such findings will reflect their limited impact.

Receiving Your Award

- The awards are categorized under two credit categories; you can opt for the following:
  - PayPal Credit
  - Service Credit
- To receive PayPal Credit, you must have a valid PayPal account.

- If you opt for service credit, it is not transferable and only be used with Ultra.cc services.

Ground Rules

- Make sure to check the Changelog channel in our Discord server for any recently launched updates/features;
- Play by the rules. This includes following this policy, the Terms of Service any other relevant agreements;
- Report any vulnerability you've discovered promptly;
- Avoid violating the privacy of others, disrupting our systems, destroying data, and/or harming user experience;
- Only use the Ticket System to contact us with the technical details of discovered vulnerabilities;
- Handle the confidentiality of details of any discovered vulnerabilities according to our Disclosure Policy;
- Perform testing only on in-scope systems, and respect systems and activities which are out-of-scope;
- If a vulnerability provides unintended access to data: Limit the amount of data you access to the minimum required for effectively demonstrating a Proof of Concept; and cease testing and submit a report immediately if you encounter any user data during testing, such as Personally Identifiable Information (PII), or proprietary information. You may also request for an isolated server for you to further demonstrate your proof of concept;
- You should only interact with test accounts you own; and
- Do not engage in extortion.

Safe Harbor

When conducting vulnerability research according to this policy, we consider this research conducted under this policy to be:

- Authorized in view of any applicable anti-hacking laws, and we will not initiate or support legal action against you for accidental, good faith violations of this policy;
- Authorized in view of relevant anti-circumvention laws, and we will not bring a claim against you for circumvention of technology controls;
- Exempt from restrictions in our policies that would interfere with conducting security research, and we waive those restrictions on a limited basis; and
- Lawful, helpful to the overall security of the Internet, and conducted in good faith.

You are expected, as always, to comply with all applicable laws. If a third party initiated legal action against you and complied with this policy, we will take steps to make it known that your actions were conducted in compliance with this policy. If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please submit a report through the Ticket System before going any further.

Disclosure Policy

If you believe you have discovered a vulnerability, please create a ticket through the Ticket System.

- The Report of your research must include the exact steps of reproduction of the vulnerability with prompt descriptions. You may use this template to submit your report: https://github.com/ZephrFish/BugBountyTemplates/blob/master/Example.md

- Only use our official Support Ticket Platform for any inquiries regarding the program.
- Publicly disclosing your research/submission without explicit, written permission from Ultra.cc and evaluation is a straight violation of the Rules of this Bug Bounty Program, and you'll be ineligible for a reward.

Ultra.cc Bug Bounty Hall of Fame