HACKTROPHY BUG BOUNTY PROJECTS
ETHICAL HACKER TERMS AND CONDITIONS

Welcome to the Hacktrophy Bug Bounty Program (hereinafter only as the "**Program**"). This Program encourages and rewards contributions (submission of qualified vulnerabilities as described in the Projects rules and these terms and conditions) by ethical hackers (hereinafter only as the "**Ethical hacker**") who help make internet more secure. Through this Program Hacktrophy provides monetary rewards and possibly public recognition for security vulnerabilities responsibly disclosed by Ethical hackers under the following terms and conditions.

If you are new to our Program, please review these Ethical hacker terms and conditions and Projects rules in order to find out how to access the Program, submit a vulnerability reports and obtain a rewards for it.

Program description

Provided that the Ethical hacker has agreed to these terms and conditions, Hacktrophy will allow to the Ethical hacker to access the Program and to connect with Customers by submission of qualified vulnerabilities reports according to these terms and conditions. Customers using the Program create Projects in which they offer bounties/rewards for reporting qualifying vulnerabilities by Ethical hackers in accordance with these terms and Conditions (hereinafter only as the "**Project**"). Ethical hackers can browse Customer's Projects and submit vulnerability reports for Project through the Program.

Hacktrophy offers two types of the Program:

Basic Program – after the Project is published, following process of a Ethical hacker's report runs without control of the moderator as described further in these terms and conditions.

Premium Program – whole process of a Ethical hacker's report is controlled by the moderator set by Hacktrophy as described further in these terms and conditions.

Program exclusions

- **Third-party websites.** Some **Customer**-branded services hosted in less common domains may be operated by vendors or partners. We can't authorize the Ethical hacker to test these systems on behalf of their owners and will not reward such reports. Security bugs in third-party applications (e.g. java, plugins) or websites.
- **Attacks against Customer`s infrastructure** which is not accessible via internet, social engineering and phishing attacks against Customer`s employees.

- **Recent acquisitions.** To allow time for internal review and remediation, newly established companies are subject to a six-month blackout period. Bugs reported sooner than that will typically not qualify for a reward.
- **Denial of service (DoS)** attacks and similar methods that require large volumes of data and leverage black hat SEO techniques.

Qualifying vulnerabilities

1. Typically the in-scope submissions will include high impact bugs. However, any vulnerability at any severity that may cause damage might be rewarded. Eligible submissions will include vulnerabilities of the following types:

    - Cross Site Scripting (XSS)
    - Cross Site Request Forgery (CSRF)
    - Mixed-content scripts
    - Unauthorized cross-tenant data tampering or access (for multi-tenant services)
    - Insecure direct object references
    - Injection Vulnerabilities (such as SQL Injection, XML injection or ORM injection)
    - Authentication Vulnerabilities
    - Server-side Code Execution
    - Privilege Escalation
    - Significant Security Misconfiguration
    - Server-side code execution bugs

2. Hacktrophy reserves the right to reject any submission at our sole discretion and to determine at our sole discretion, which bugs are considered as candidates for reward, as well as the final reward recipients, taking into account rules stated in both Basic Program and Premium Program as described in these terms and conditions.

Non-qualifying vulnerabilities

1. The aim of the Program is to uncover significant vulnerabilities that have a direct and demonstrable impact to the security of our Customers. While we encourage any submissions that describe security vulnerabilities in our service, the following are examples of vulnerabilities that will not earn a bounty reward:

    - Missing HTTP Security Headers (such as X-FRAME-OPTIONS) or cookie security flags (such as “httponly”)
    - Server-side information disclosure such as IPs, server names and most stack traces
    - Bugs used to enumerate or confirm the existence of users or tenants
    - Bugs requiring unlikely user actions

- URL Redirects (unless combined with another vulnerability to produce a more severe vulnerability)
- Vulnerabilities in platform technologies that are not unique to the online services in question
- ”Cross Site Scripting” bugs in SharePoint that require “Designer” or higher privileges in the target’s tenant.
- Low impact CSRF bugs (such as logoff)
- Cookie replay vulnerabilities

2. Hacktrophy reserves the right to reject any submission that we determine, in our sole discretion, falls into any of these categories of vulnerabilities even if otherwise eligible for a reward, taking into account rules stated in both Basic Program and Premium Program as described in these terms and conditions.

How to access the Program

The Ethical hacker can sign up to the Program by filling out requested data in the sign up form. The Ethical hacker will receive an e-mail message confirming the sign up. Subsequently, to complete the registration, the Ethical hacker will be asked to confirm the registration e-mail address entered in his sign up form.

It is highly recommended to fill out all information in the sign up form including payment data necessary for the rewards payment. In case, the Ethical hacker's payment data are not filled, Hacktrophy is not responsible for any failure in reward payment.

When signed up, the Ethical hacker will get access to the list of Projects published by Customer with categories of vulnerabilities qualified for rewards and the amount of the reward for every such reported vulnerability. The Ethical hacker will also be informed if the Project is included in the Basic Program or in the Premium Program.

Reporting

Note, that in case, the Ethical hacker's payment data are not filled in the sign-up form, Hacktrophy is not responsible for any failure in reward payment.

Basic Program

All reports are send directly to the Customer, who shall decide on it.

The Ethical hacker shall report a vulnerability found in the chosen Project through the form by filling in all necessary details and data describing a vulnerability. In case the Ethical hacker will not include all necessary details in the form for any reason, the report may be considered ineligible.

The Customer is obliged to decide on each report within 7 days from its submission by the Ethical hacker. In case, the Customer does not decide on the report within 7 days from its submission, the Ethical hacker is entitled to notify the moderator in order to solve the problem.

Customer's decision on reports

1. The Customer accepts the report without reservations:
   - the Customer notifies the Ethical hacker on the report acceptance;
   - amount of the reward for the Ethical hacker is set automatically according to the conditions stated in the published Project and category of vulnerability selected by the Ethical hacker;
   - the Ethical hacker will receive an e-mail notification from Hacktrophy that the Customer's payment of the reward for the Ethical hacker is awaited;
   - once the Customer has paid the reward for the Ethical hacker to Hacktrophy, Hacktrophy will pay it to the Ethical hacker;
   - the Ethical hacker will receive a receipt of the reward payment via e-mail.

2. The Customer accepts the report but does not accept the category of vulnerability (and the resulting reward amount) selected by the Ethical hacker:
   - the Customer will send a complaint to the moderator, who is entitled to set the right category of vulnerability (and reward amount) definitely;
   - the Ethical hacker will be notified on the moderator's decision via e-mail;
   - in case the report was considered as the valid report, the Ethical hacker will receive an e-mail notification from Hacktrophy that the Customer's payment of the reward for the Ethical hacker is awaited;
   - once the Customer has paid the reward for the Ethical hacker to Hacktrophy, Hacktrophy will pay it to the Ethical hacker;
   - the Ethical hacker will receive a receipt of the reward payment via e-mail.

3. The Customer rejects the report and the Ethical hacker accepts the rejection:
   - the Customer will receive the closure report.

4. The Customer rejects the report and the Ethical hacker does not accept the rejection:
   - the Ethical hacker will send a complaint to the moderator, who either refuses the complaint or accepts it and sets the right category of vulnerability (and reward amount) definitely,
   - the Ethical hacker will be notified on the moderator's decision via e-mail;
   - in case the complaint of the Ethical hacker was accepted, the Ethical hacker will receive an e-mail notification from Hacktrophy that the Customer's payment of the reward for the Ethical hacker is awaited;

- once the Customer has paid the reward for the Ethical hacker to Hacktrophy, Hacktrophy will pay it to the Ethical hacker;
- the Ethical hacker will receive a receipt of the reward payment via e-mail.

5. The Customer rejects the report, but uses the report for the repair of the reported vulnerability underhand (cheating):
   - in case the Ethical hacker accepts the rejection, the Customer will receive the closure report;
   - the Ethical hacker will send a complaint to the moderator, who sets the right category of vulnerability (and reward amount) definitely;
   - in case the Ethical hacker complained and it was proved that the Customer has acted fraudulently, the Ethical hacker will receive an e-mail notification from Hacktrophy that the Customer's payment of the reward for the Ethical hacker is awaited;
   - once the Customer has paid the reward for the Ethical hacker to Hacktrophy, Hacktrophy will pay it to the Ethical hacker;
   - the Ethical hacker will receive a receipt of the reward payment via e-mail;
   - in case the Customer fails to pay the reward for the Ethical hacker to Hacktrophy, although the report was considered by the moderator as the valid report, the Customer will be excluded from the Program immediately. Note, that in such case the reward cannot be paid and Hacktrophy is not responsible for any claims arising therefrom.

Remark: In case the Ethical hacker will report a vulnerability of a different kind, i. e. a vulnerability which is not specifically stated in the published Project with a reward amount for such vulnerability, the Customer in cooperation with the moderator shall decide on it definitely. In such case above mentioned procedures shall apply accordingly.

In the Basic Program, the Customer is entirely responsible for fixing of the reported vulnerability and discusses the fix process with the Ethical hacker.

Upon Ethical hacker's request the Customer can decide on disclosure and publishing of the completion report. The Customer is entitled to refuse the disclosure of the completion report without any reason. However, the Customer pledges to respect if the Ethical hacker wishes not to be disclosed.

Premium Program

The Ethical hacker shall report a vulnerability found in the chosen Project through the form by filling in all necessary details and data describing a vulnerability. In case the Ethical hacker will not include all necessary details in the form for any reason, the report may be considered ineligible.

The Hacktrophy moderator will review every report and valuate its eligibility and relevance.

The moderator will decide on each report within 5 days from its submission by the Ethical hacker.

Moderator's decision on reports

1. The Moderator accepts the report without reservations:
   - amount of the reward for the Ethical hacker is set according to the conditions stated in the published Project and category of vulnerability selected by the Ethical hacker, and confirmed by the moderator who must approve the category of vulnerability (and reward amount) definitely;
   - the Ethical hacker will receive an e-mail notification from Hacktrophy that the Customer's payment of the reward for the Ethical hacker is awaited;
   - once the Customer has paid the reward for the Ethical hacker to Hacktrophy, Hacktrophy will pay it to the Ethical hacker;
   - the Ethical hacker will receive a receipt of the reward payment via e-mail.

2. The Moderator rejects the report, because:
   - the report has been evaluated as a false positive report;
   - the report is out of the scope of the Project, in such case the moderator is entitled to set a special reward for the Ethical hacker, in case it was previously agreed with the Customer;
   - in case there was set a special reward for the Ethical hacker, the Ethical hacker will receive an e-mail notification from Hacktrophy that the Customer's payment of the reward for the Ethical hacker is awaited;
   - once the Customer has paid the reward for the Ethical hacker to Hacktrophy, Hacktrophy will pay it to the Ethical hacker;
   - the Ethical hacker will receive a receipt of the reward payment via e-mail.

Remark: In case the Ethical hacker will report a vulnerability of a different kind, i. e. a vulnerability which is not specifically stated in the published Project with a reward amount for such vulnerability, the Customer in cooperation with the moderator shall decide on it definitely. In such case above mentioned procedures shall apply accordingly.

The Customer is entirely responsible for fixing of the reported vulnerability and discusses the process of vulnerability fixing with the Ethical hacker and the moderator.

Upon Ethical hacker's request the Customer can decide on disclosure and publishing of the completion report. The Customer is entitled to refuse the disclosure of the completion report without any reason. However, the Customer pledges to respect if the Ethical hacker wishes not to be disclosed.

Reward payment

In case the Ethical hacker's report was accepted according to these terms and conditions, the Ethical hacker will receive an e-mail notification from Hacktrophy that the Customer's payment of the reward for the Ethical hacker is awaited.

Only the report submitted in accordance with these terms and conditions by the signed up Ethical hacker within the conditions of the published Project will be considered as the valid vulnerability report. Any exceptions must be expressly and individually decided by the Customer in cooperation with the moderator as described in these terms and conditions.

The Ethical hacker will receive the payment of the reward only in case the Customer has paid the reward for the Ethical hacker to Hacktrophy. Subsequently, Hacktrophy will pay the reward to the Ethical hacker.

The Ethical hacker notes, that in case the Ethical hacker is a resident in the state with which the Slovak republic has not concluded an international treaty for the avoidance of double taxation or international agreement on the exchange of tax information or in the state which is not a party to an international treaty providing for the exchange of information for tax purposes in a similar range, by which this state and the Slovak republic are bound, the reward can be reduced by a withholding tax at the rate stipulated by the Income Tax Act valid and effective in the Slovak republic.

Other terms and conditions

1. The parties to this agreement are the Ethical hacker and Hacktrophy. Prior to take participation in the Program the Ethical hacker must agree to these terms and conditions.

2. The Ethical hacker will qualify for a reward only if he was the first person to alert Hacktrophy to a previously unknown issue.

3. There is no legal entitlement for a reward. Eligibility for rewards, determination of the recipients and amount of reward is left up to the discretion of the Customer respectively of Hacktrophy.

4. Services according to this agreement are provided on servers and through software, which are located in the Slovak republic. Therefore, the place of supply of services according to this agreement is the Slovak republic.

5. Ethical hacker's testing must not violate any law, or disrupt or abuse any data or data access that is not Ethical hacker's. Ethical hacker's testing activities must not negatively impact Hacktrophy, Customer, and Hacktrophy's or Customers's online environment availability or performance. When carrying out any of the activities connected with testing the Ethical hacker must abide the law. There may be additional restrictions depending upon applicable local laws.

6. By submitting the vulnerability report, the Ethical hacker affirms that he has not disclosed and agrees that he will not disclose the bug or his submission to anyone other than the Customer and Hacktrophy via the Program. Absent the Customer's or Hacktrophy's prior written consent, any disclosure outside of the Program would violate this agreement and terms and disallow to claim reward. It is understood and agreed that money damages would not be a sufficient remedy for any breach of this terms and conditions by the Ethical hacker or his representative(s) and that the Customer and/or Hacktrophy shall be entitled to specific performance as a remedy for any such breach, including injunctive relief. Such remedy shall not be deemed exclusive to cover damages for any such breach but shall be in addition to all other remedies available at law or equity to the Customer and/or Hacktrophy.

7. All individuals who have been awarded with rewards will additionally be recognized on Hacktrophy public page, unless they specifically wish not to be, or they will receive other non-financial reward provided by Hacktrophy.

8. Except for other activities which are against the law, the following activities are strictly prohibited, unless the Customer expressly states otherwise:

    - Denial of Service testing.
    - Performing automated testing of services that generates significant amounts of traffic.
    - Using of any data that is not wholly your own in any way.
    - Moving beyond “proof of concept” repro steps for server-side execution issues (i.e. proving that you have sysadmin access with sqli is acceptable, running xp_cmdshell is not).
    - Attempting phishing or other social engineering attacks against Hacktrophy, Hacktrophy's employees, contractors, customers and any other person. The scope of this Program is limited to technical vulnerabilities.

9. Generally, the Ethical hacker is eligible to participate in this Program if:

    - He is 18 years of age or older. If the Ethical hacker is at least 18 years old but is considered a minor in his place of residence, he must ask his parent’s or legal guardian’s permission prior to participating in this Program; and

- he is either an individual ethical hacker participating in his own individual capacity, or he works for an organization that permits him to participate. The Ethical hacker is responsible for reviewing his employer's rules for participating in this Program.

10. There are no restrictions on the number of qualified submissions an individual submitter can provide and to be paid for.

11. In the event that multiple bug reports for the same issue from different parties are received, the reward will be granted to the first submission.

12. If you would like to remain anonymous to the public, we will honor your request, but we must know your data in order to pay you. For payment of an award you need to provide your payment data.

13. The Ethical hacker is responsible for all taxes associated with and imposed on any reward he may receive from Hacktrophy. Hacktrophy may reduce any reward by the amount of any tax imposed on you that Hacktrophy is required to pay directly to a taxing or other governmental authority.

14. It is Ethical hacker's responsibility to comply with any policies or compliance rules of his employer that may affect his eligibility to participate in this Program. If the Ethical hacker is participating in violation of his employer's policies, he may be disqualified from participating or receiving reward payment(s). All payments will be compliant with local laws, regulations, and ethical rules. Hacktrophy disclaims any and all liability or responsibility for disputes arising between an employee and their employer related to this matter.

15. In case the report is accepted, please note:

    - The Ethical hacker may not designate someone else as the reward recipient unless he is considered a minor in his place of residence.
    - If the Ethical hacker is unable or unwilling to accept the reward, we reserve the right to rescind it.
    - The Ethical hacker can donate the reward to a charity. In such case the Ethical hacker should request Hacktrophy to donate his reward to the specified charity organization.
    - If the Ethical hacker accepts a reward, he will be solely responsible for all applicable taxes related to accepting the payment(s).
    - If the Ethical hacker is eligible for this Program but is considered a minor in his place of residence, Hacktrophy may process/provide the reward payment to his parent/legal guardian on his behalf.

16. By providing his submission, the Ethical hacker:

- Undertakes to disclose the bug or his submission only via the Program and acknowledges that the disclosure of the bug to anyone other than the Customer and Hacktrophy (via the Program), in any way, for a reward or for free, would be qualified as a criminal offense with the corresponding consequences.
- Agrees to license intellectual property in his submission to Hacktrophy which includes an irrevocable, perpetual, royalty-free, worldwide, unlimited, nonexclusive, sub-licensable, unrestricted right and license (i) to use, review, assess, test, and otherwise analyze his submission; to reproduce, modify, distribute, display, and perform publically, and to commercialize and create derivative works of, his entry and all its content, in whole or in part, in connection with this Program; and (ii) to feature his submission and all content in connection with the marketing, sale, or promotion of this Program (including but not limited to internal and external sales meetings, conference presentations, tradeshows, and screen shots of the submission in press releases) in all media (now known or later developed).
- Understands and acknowledges that Hacktrophy may have developed or commissioned materials similar or identical to his submission, and he waives any claims he may have resulting from any similarities to his submission.
- Understands that he qualifies for a one-time payment for each eligible vulnerability and is not guaranteed any additional compensation or credit for use of his submission.
- Acknowledges his legal obligation to co-operate with investigative and prosecuting authorities requested in accordance with applicable laws.

17. This Program is hosted in the Slovak republic and submissions are collected on computers in the Slovak republic. This Program will be governed by the laws of the Slovak republic (incl. directly applicable acts of European Union), and you consent to the exclusive jurisdiction and venue of the courts of the Slovak republic for any disputes that arise out of this Program.

18. The decisions made by Hacktrophy are final and binding. Hacktrophy may change or cancel this Program at any time, for any reason.

19. Hacktrophy thanks you for your participation.

    Happy Hunting!