HACKTROPHY BUG BOUNTY PROJECTS RULES

Being aware of increasing level of security demanded by our customers we offer ways how to rope the internet ethical hackers community in process. This community consists of high-level skilled experts who we would like to invite to cooperate and benefit from their skills by means of vulnerability reward program. This Hacktrophy bug bounty program (hereinafter only as the "**Program**") is developed and operated by security company Hacktrophy which guarantees qualified management of the Program. Following instructions may help those who would like to help make internet a more safe place.

Program description

This Program encourages and rewards contributions (submission of qualified vulnerabilities as described in these rules) by ethical hackers (hereinafter only as the "**Ethical hacker**"). Hacktrophy will allow to the Customer (hereinafter only as the "**Customer**") to access the Program and to connect with Ethical hackers.

Types of the Program, which Hacktrophy offers are specified in the Customer terms and conditions.

Services in scope

Any Customer`s name-owned web service or application that handles reasonably sensitive user data is intended to be in scope, including security vulnerabilities in APIs and other services accessible from internet.

Program exlusions

- **Third-party websites.** Some Customer-branded services hosted in less common domains may be operated by our vendors or partners. We can't authorize you to test these systems on behalf of their owners and will not reward such reports. Security vulnerabilities in third-party applications (e.g. java, plugins) or websites.
- **Attacks** againts Customer`s infrastructure, 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. Security vulnerabilities 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.

Always remember: If in doubt, contact us first.

Qualifying vulnerabilities

A security vulnerability is an error, flaw, mistake, failure, or fault in a computer program or system that impacts the security of a device, system, network, or data and may be a way to cause real damage both material and immaterial. Any security vulnerability may be considered for this Program; however, it must be a new, previously unreported and unexcluded vulnerability in order to be eligible for reward or recognition. Typically the in-scope submissions will include high impact vulnerabilities; however, any vulnerability at any severity that may cause damage might be rewarded. Any design or implementation issue that substantially affects integrity of user data is likely to be in scope for the Program.

Common examples include:

- Remote Code Execution
- Vertical Privilege Escalation
- XML External Entities Injection with significant impact

- SQL Injection with significant impact
- LFI/RFI
- Horizontal Privilege Escalation
- Stored XSS with significant impact
- CSRF with significant impact
- Direct object reference with significant impact
- Internal SSRF
- Session fixation
- Reflective XSS with impact
- Insecure Deserialization with significant impact
- Direct object reference
- CSRF with impact
- Path Traversal
- DOM XSS
- SSL misconfigurations with little impact
- SPF configuration problems
- XSS with limited impact
- CSRF with limited impact
- SSL/TLS issues (weak crypto, improper setup)
- URL redirect
- Clickjacking

Note that the scope of the program is limited to technical vulnerabilities in Customer-owned web applications and related extensions.

In the event of multiple vulnerability reports, the Customer is entitled to refuse further reports of such vulnerability for 30 days and to fix such vulnerability within this period. Upon the expiration of this period, the Customer is obliged to accept which contents the same vulnerability if he did not fix it by his own fault.

The Customer can explicitly state other that above mentioned vulnerabilities, which will qualify for a reward in his published Project.

Non-qualifying vulnerabilities

Depending on their impact, some of the reported issues may not qualify. Although we review them on a case-by-case basis, here are some of the common low-risk issues that typically do not earn a monetary 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
- Vulnerabilities used to enumerate or confirm the existence of users or tenants
- Vulnerabilities requiring unlikely user actions
- URL Redirects (unless combined with another vulnerability to produce a more severe vulnerability)

Monetary rewards aside, Ethical hackers who work with us to resolve security vulnerabilities within the Program will be credited on our website, under conditions specified in the Ethical hacker Terms and Conditions.

The Customer can explicitly exclude other that above mentioned vulnerabilities, which will not earn a reward in his published Project.

Rewards

Rewards for qualifying vulnerabilities range from 40,00 € to any amount stated by the Customer in the published Project depending on the severity of the potential security impact of reported vulnerability.
The amount of rewards for Ethical Hackers for vulnerability reports within a particular Customer Project is decided by the Customer on the basis of the Hacktrophy's proposed amount of rewards in such a way that Customer effectively utilizes Hacktrophy's services in accordance with the purpose of his participation in the Program. The Customer is entitled to change the amount of rewards for Ethical hackers offered within a particular Project at any time during the Project duration at its own discretion.

Reward amounts are set in each Project independently.

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

The amount of the reward for the Ethical hacker is usually set according to the conditions stated in the published Project and category of vulnerability selected by the Ethical hacker, and confirmed by Hacktrophy who must approve the category of vulnerability (and reward amount) definitely, under conditions specified in the Customer Terms and Conditions.

We don't pay rewards to individuals who act with the intention of detecting failures in the security for other purposes than are aimed with the Program, or violating any law, or publish or disrupt or compromise a data of any person different from them or who are on any legally binding sanctions lists. You are responsible for any tax implications depending on your country of residency and citizenship. There may be additional restrictions on your ability to enter the Program depending upon your local law.

We are entitled to cancel the Program at any time without any reason.

Security testing must not violate any law, or publish, disrupt or compromise any data that is not your own.

Investigating and reporting security vulnerabilities

When investigating a vulnerability, please, never attempt to access anyone else's data and do not engage in any activity that would be disruptive or damaging to your fellow users or to Customer.

Each Ethical hacker has to be signed up to the Program in order to submit a vulnerability report. The Ethical hacker can sign up to the Program by filling out requested data in the sign up form. 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. Within each Project, an assigned moderator usually communicates on behalf of the Customer. However, the Customer can engage in communication on submitted reports with Ethical hackers at any time. We ask Ethical hackers to actively communicate on their reports, in particular to provide the Customer with assistance in repairing the reported security vulnerability.

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.

Other conditions of vulnerability reports submission and its processing in both, Basic Program and Premium Program, are stipulated in the Customer Terms and Conditions and in the Ethical hacker Terms and Conditions.

Other instructions:

Please submit your report as soon as you have discovered a potential security issue. In case the Ethical hacker will not include all necessary details in the form for any reason, the report may be considered ineligible.

Please perform due diligence: confirm that the discovered software had any noteworthy vulnerabilities, and explain why you suspect that these features may be exposed and may pose a risk in a specific use. Reports that do not include this information will typically not qualify.

In essence, our pledge to you is to respond promptly and in exchange, we ask for a reasonable advance notice. Reports that go against this principle will usually not qualify, but we will evaluate them on a case-by-case basis. At the same time, we ask you for patience while evaluating submitted reports, as the Program may receive a large number of reports, or certain types of vulnerabilities require a time-consuming review.

It is against the spirit of the Program to privately disclose security vulnerability to third parties for purposes other than actually fixing the vulnerability through Hacktrophy platform. Consequently, such reports will typically not qualify. Such a conduct is considered as the serious breach of our terms and conditions that results in the immediate exclusion of the Ethical hacker from the Program. In such case the Ethical hacker has no claim for a reward payment and could face criminal consequences.

“First in, best dressed.” Ethical hacker will qualify for a reward only if he was the first person to alert us to a previously unknown flaw.

After signing up to the Program, 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.

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.

If Hacktrophy and the Ethical hacker agree and under the terms and conditions set forth in the generally binding legal regulations valid in the Slovak Republic, the reward for the vulnerability report for the Ethical Hacker may also be paid in one of the cryptocurrencies.

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.

We reserve the right to modify all terms and conditions of this Program anytime. Prior to take participation in the Program the Ethical hacker must agree to Ethical hacker terms and conditions. Please check this site regularly as we routinely update our Program terms, which are effective upon posting.