HACKTROPHY BUG BOUNTY PROJECTS RULES

Being aware of increasing level of security demanded by our customers we search for 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 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.

Hacktrophy offers two types of the Program:

Basic Program – after the Project is published, following process of an Ethical hacker's report runs without control of the moderator. All reports are send directly to the Customer, who shall decide on it. The Customer is entirely responsible for fixing of the reported vulnerability and discusses the fix process with the Ethical hacker.

Premium Program – whole process of a Ethical hacker 's report is controlled by the moderator set by Hacktrophy. The Hacktrophy moderator will review every report and valuate its eligibility and relevance. 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.

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 bugs 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 bugs 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. 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.

Always remember: If in doubt, contact us first.

Qualifying vulnerabilities

A security bug 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 bug 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 bugs; however, any vulnerability at any severity that may cause damage might be rewarded. Any design or implementation issue that substantially affects the confidentiality or integrity of user data is likely to be in scope for the Program.

Common examples include:

- 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

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

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
- 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

Monetary rewards aside, Ethical hackers who work with us to resolve security bugs 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 bugs range from 40,00 € to any amount stated by the Customer in the published Project. The following table outlines the usual average rewards chosen for the most common classes of bugs, as suggested by Hacktrophy:

Risk Level	Vulnerability Examples	Reward Amount (€)
Critical	• Remote Code Execution • Vertical Privilege Escalation • XML External Entities Injection with significant impact • SQL Injection with significant impact • LFI/RFI	Range 500 – 7500
High	• 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	Range 300 – 1500
Medium	• Direct object reference • CSRF with impact • Path Traversal • DOM XSS	Range 80 – 550
Low	• SSL misconfigurations with little impact • SPF configuration problems • XSS with limited impact • CSRF with limited impact • SSL/TLS issues • URL redirect • Clickjacking	Range 40 – 160
Acceptable Risk	• Debug information • Use of CAPTCHAs • Code obfuscation • Rate limiting, etc.	0

However, the Customer can set any reward amounts in his Project regardless of Hacktrophy recommendation.

The Customer will set a reward amounts in each of his published 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.

In the Basic Program amount of the reward for the Ethical hacker is usually set automatically according to the conditions stated in the published Project and category of vulnerability selected by the Ethical hacker, under conditions specified in the Customer Terms and Conditions.

In the Premium Program 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 the moderator 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.

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

Investigating and reporting bugs

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. The Ethical hacker will also be informed if the Project is included in the Basic Program or in the 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.

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.

It is against the spirit of the Program to privately disclose the flaw to third parties for purposes other than actually fixing the bug. 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.

First in, best dressed. You will qualify for a reward only if you were the first person to alert us to a previously unknown flaw.

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 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.