oDesk Bug Bounty Program Guidelines

This is oDesk's very own bug bounty program! If you want to learn how you could get rewarded for helping us keep our site – and its users – secure, read on…

Through our bounty program, we'll provide rewards to eligible bug hunters who discover and discretely report verified oDesk site security bugs. We are excited about this program, but we also need you to understand that our decisions are final with respect to who gets a reward, what we reward, and if a reward is provided at all.

HOW SHOULD I REPORT A BUG TO ODESK?

Send us an email at security-reports@odesk.com including your full name, country of residence and a description of the security bug you discovered, including how the bug impacts or could impact oDesk site security or oDesk site users. We also suggest you attach a "proof of concept" test-case to the bug report that demonstrates how the vulnerability could be exploited. A test-case helps us analyze submissions faster and more accurately.

And keep the following in mind:

- We are not responsible for reports that we do not receive or for submissions that we receive but are incomplete or indecipherable;
- Our lack of response to your submission does not mean we are ignoring you. We may get 10s, 100s or 1000s of submissions a day, with only a small portion of them being legitimate. We take our time to verify submissions. Going public with a potential security bug is a sure way to ensure that you do not get a reward.
- We reserve the right to withhold a reward if we believe you have acted in a way that has endangered the security of the site or site users – for example, by publicly disclosing a bug or testing a vulnerability on a real user.

WHO'S ELIGIBLE FOR A REWARD?

You are eligible to participate in this program if:

- You are either an individual researcher participating in your own individual capacity, or you work for an organization that permits you to participate. You are responsible for reviewing your employer's rules for participating in this program;
- You are not the author of the code that's been infected with the bug, nor were you otherwise involved in its integration into our site;
- You did not create the bug about which you're reporting;

- You are not one of our current employees (sorry guys); and
- You do not reside in a country under any current U.S. Sanctions.

WHAT KINDS OF REPORTS AND SUBMISSIONS QUALIFY FOR A REWARD?

We reward eligible bug reporters whose submissions describe security bugs that make our site vulnerable to (i) cross-site scripting (XSS), (ii) cross-site request forgery (CSRF/XSRF), (iii) authentication or authorization issues, (iv) remote code execution, (v) privilege escalation, and:

- Are present in the most updated version of our site;
- Could (i) compromise the integrity of our site users' data or (ii) enable unauthorized access to our site's infrastructure;
- Are original and were previously unreported;
- Are remotely exploitable;
- Are not in, or caused by, any 3rd-party software or sites (e.g., Java, plugins, extensions); and
- Do not consist of username enumeration, marketplace spam vectors, denial of service vulnerabilities or phishing/fraud-related activities. Please report phishing/fraud-related activities to: https://support.odesk.com/home.

WHAT KIND OF REWARDS DO YOU OFFER AND HOW DO YOU DETERMINE WHICH REWARD TO PROVIDE?

It depends. We offer a range of rewards (minimum value of $100), which may include gift cards. We decide the appropriate award for qualified bug report submissions based on our own discretion, but it's a pretty safe bet that the criticality of the reported bug often will be an important factor.

A few other reward-related points:

- We retain sole discretion in determining which submissions are qualified;
- If two or more people report a bug together, we'll split the reward amongst them;

- If two or more eligible people submit separate qualified reports claiming to have discovered the same bug, the person whose report we received first gets the reward; and
- When a single bug manifests in multiple forms, it will be classified as a single vulnerability (and only one bounty will be paid).

WHEN IS THIS GUIDE GOING TO REFERENCE LEGAL STUFF?

Now! In addition to any terms, requirements, or prohibitions contained in this document, this program and your participation in this program is governed by oDesk's Terms of Service, which governs your use of the oDesk platform and website and which is accessible at https://www.odesk.com/info/terms/. This program is void where prohibited by law. Reward recipients are solely responsible for all taxes and associated responsibilities incurred as a result of receipt of a reward, which may require signing a reward release from oDesk.