Welcome to the RVAsec 2015 CTF & Bug Bash!

This year you are competing with your fellow RVAsec CTF participants by finding and reporting vulnerabilities in bounty programs that are available through Bugcrowd. All Bugcrowd bounty programs are in scope for this competition, many of which pay out cash as rewards for valid vulnerabilities.

The goal of the competition is to earn the most points, which means you will want to find the most severe vulnerabilities that you can find. Every valid vulnerability will be rewarded points and those points will be reflected on the RVAsec leaderboard.

To be rewarded for your findings you need to report a valid non-duplicate vulnerability. It's typically safe to assume that low-level vulns have been already found by other researchers, so aim high.

What do I need to do?

- **Do reconnaissance!** Read the bounty brief for the bounty program(s) that you will be hacking on. The briefs tell you what is in scope and what isn't, so this is an important step.

- **Don't have Bugcrowd account yet?** - Register an account on Bugcrowd at https://bugcrowd.com/user/sign_up . Make sure to include "_rvasec" at the end of your username. ****Important**** - If your username does not include _rvasec , you will not be tracked on the Leaderboard.

Steps to follow:

1. **Start hacking and report your findings.** Each bounty page has a "Report Bug" button in the top right. Click that and report your bug, including the important information needed to help reproduce and validate your vuln. You will need to go through this process for each individual vuln that you find.

2. **???** (Actually, this is where the Bugcrowd team validates the bug and decides whether it's valid, a duplicate, etc, and then rewards you accordingly)

3. **Profit.** Once your bug has been validated, your reward will be updated on the Bug Bash Leaderboard and within Bugcrowd.

Vulnerability submissions will be ranked and judged by priority during the validation process. This determines the reward/payout amount. General guidelines for vulnerability priorities**:**

P1 - CRIT - 20 points
Vulnerabilities that cause a privilege escalation on the platform from unprivileged to admin, allows remote code execution, financial theft, etc. Examples: Remote Code Execution, Vertical Authentication bypass, SSRF, XXE, SQL Injection, User authentication bypass

P2 - HIGH - 15 points
Vulnerabilities that affect the security of the platform including the processes it supports. Examples: Lateral authentication bypass, Stored XSS, some CSRF depending on impact

P3 - MED - 10 points
Vulnerabilities that affect multiple users, and require little or no user interaction to trigger. Examples: Reflective XSS, Direct object reference, URL Redirect, some CSRF depending on impact

P4 - LOW - 5 points
Issues that affect singular users and require interaction or significant prerequisites (MitM) to trigger. Examples: Common flaws, Debug information, Mixed Content

P5 - BIZ ACCEPTED RISK - 2 points
Non-exploitable weaknesses and “won’t fix” vulnerabilities. Examples: Best practices, mitigations, issues that are by design or acceptable business risk to the customer such as use of CAPTCHAS.