Bug Bounties

By SSHC™ (Andy, Vishal, Andre, Jason and Frank)

What the hack are Bug Bounties?

“Get paid to hack things”

- A platform rewarding anyone that discovers and discloses security vulnerabilities for specific software products/systems.

- The company will provide a scope as a guideline for what is/isn’t allowed.

- Each vulnerability disclosed is prioritised from low to critical priority.

- Responsible disclosure guidelines are outlined in the bounty program’s scope.

Private vs Public Bug Bounties

Private	Public
- Recommended as a starting program - Selected number of established hackers to undertake the program	- Recommended to be used after a private program. - Large influx of low quality bug reports

Valve Pays £15,000 To Hacker Who Found Steam Bug That Generates Free Games

1. Crafting a specific URL, anyone with access to those tools could make the service spit out keys for games that didn’t belong to them.

2. Artem Moskowsky managed to manipulate the system into giving him 36,000 keys for *Portal 2*.

3. How long it would have been before Valve caught on and shut it down

4. One in July on SQL Injection that **netted him an additional £19,300.**

The deets

~: Hit the */partnercdkeys/assignkeys* endpoint on the developer portal (partner.steamgames.com)

- appid (ID of the game)
- keyid (ID of a set of CD keys)
- keycount (number of keys to return in a set of CD keys)
- Unknown parameter name to bypass ownership verification

~: Make one API call with a zero keycount

~: Must be an authenticated user

~: Audit logs not bypassed, no prior/ongoing exploitation

~: Improper access control

The Impacto

- Illegal and misuse of keys can be sold on the market for a cheaper price.
- Generating keys isn’t just limited to Portal 2, a hacker can generate a key to any game.
- Portal 2 is selling for price of $10USD but there are games up to an average price of $60USD.
  - 36000 x 10 = $360,000 USD or 36000 x 60 = $2,160,000 USD
- Giving unauthorised generated keys to buyers can lead to banned or temporarily locking accounts for fraudulent games.
- Profits of a game lets studios develop more games however if they do not receive these profits it can force bankruptcy and close.
- Bug bounty is one the modern method to help companies fix vulnerabilities and offer a reward

References (ESSENTIAL)

1. Cimpanu. C, 2018, ZDNet, Steam bug could have given you access to all the CD keys of any game, Accessed on 05 Feb 2019 - <https://www.zdnet.com/article/steam-bug-could-have-given-you-access-to-all-the-cd-keys-of-any-game/>
2. Grayson. N, 2018, Kotaku UK, Valve Pays £15,000 To Hacker Who Found Steam Bug That Generates Free Games. Accessed on 04 Feb 2019 - <http://www.kotaku.co.uk/2018/11/13/valve-pays-15000-to-hacker-who-found-steam-bug-that-generates-free-games>
3. HackerOne. Docs, n.d. Viewed on 5/2/19 Private vs Public - <https://docs.hackerone.com/programs/private-vs-public-programs.html>
4. Moskowsky. A, 2018, Hackerone, Getting all the CD keys of any game, Accessed on 04 Feb 2019 - <https://hackerone.com/reports/391217>
5. Nichols. S, 2018, The Register, I found a security hole in Steam that gave me every game’s license keys and all I got was this... Oh nice: $20,000. Accessed on 05 Feb 2019 - <https://www.theregister.co.uk/2018/11/09/valve_steam_key_vulnerability/>