

WANTED Hackers for Bug Bounties

Hackers are in high demand around the world and in nearly every industry. Every military and espionage unit of every country is trying to hire high-quality, experienced hackers as fast as they can to hack their adversaries' computer systems in order to gain a strategic advantage and to spy.

Information security firms can't get enough well-trained hackers to test and improve the security of their clients' networks, platforms, and systems. This is one job category where the demand far outstrips the supply and good hackers are commanding top salaries.

Now, there is yet another opportunity for fledgling hackers to make money, while honing their skills until the big job offer arrives. Several Silicon Valley firms—including PayPal, Google, Facebook, Twitter and Yahoo—are paying bounties to hackers who find security holes in their systems and platforms. In this way, they hope that these white hat hackers will find and report the security flaws before the black hats exploit them.

To collect the bounty, you must first report the flaw to the company and give them time to close the vulnerability before you reveal it publicly. Twitter has reported that it has already resulted in finding 46 bugs in their platform in the short time their program has been active, while PayPal has reportedly paid out over 1,000 bug bounties.

The bounties range anywhere from the Twitter payout of a minimum of \$140 for every security bug reported, all the way up to \$150,000 that Google is offering to anyone who can own a Google Chromebook. Google reportedly has a bug bounty pool of \$2.7 million!

Interestingly, Apple has refused to participate in this program, despite many of its neighbors in Silicon Valley doing so. Considering Apple's atrocious security record of late ([Shellshock](#), iCloud, WireLurker, etc.), maybe Apple should reconsider? (Update: Apple has [started offering bug bounties](#), but only to select security researchers at the moment.)

Here is a brief list of companies who pay for bounties on security holes in their systems and platforms.

- [Adobe Flash Player](#): \$2,000 minimum
- [Facebook](#): \$500 to \$20,000 or more
- [Google](#) (including Blogger and YouTube): \$100 to \$20,000
- [Google Chrome](#): \$0 to \$15,000

- [Microsoft](#): Up to \$100,000
- [PayPal](#): \$0 to \$10,000
- [Ruby on Rails](#): \$1,500 minimum
- [Twitter](#): \$140 minimum
- [Yahoo](#) (including Flickr): \$50 to \$15,000

For more, you can check out [HackerOne](#), who acts as the middlemen for some other companies, or [Zero Day Initiative](#), who buys zero-days of all varieties. Also, Bugcrowd has a very good [bug bounty list](#).

This might be just the way for to you hone your skills and make money doing what you love without the risk of getting caught and going to prison. It doesn't get much better than that, my fledgling hackers!