bug bounty from a program's perspective

hack in the box ams -- april 14, 2017

rob fletcher, fletcher@uber.com

product security team

previous bug bounty participant

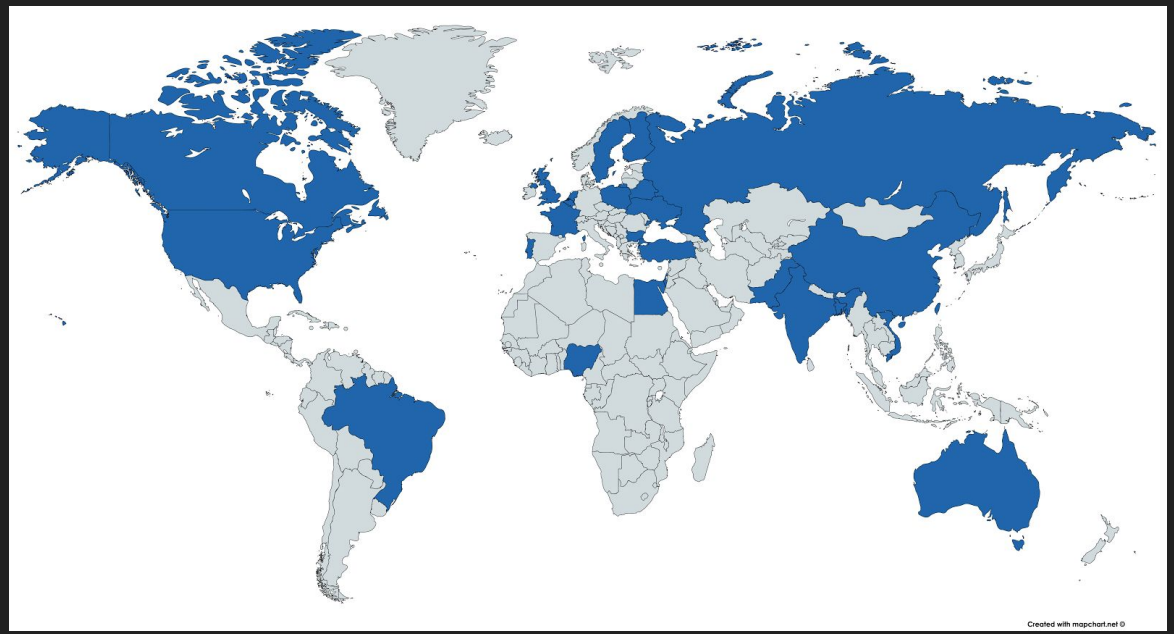
actively involved in managing uber bug bounty -- security.uber.com

fan of gifs, stand-up comedy, and recently chess

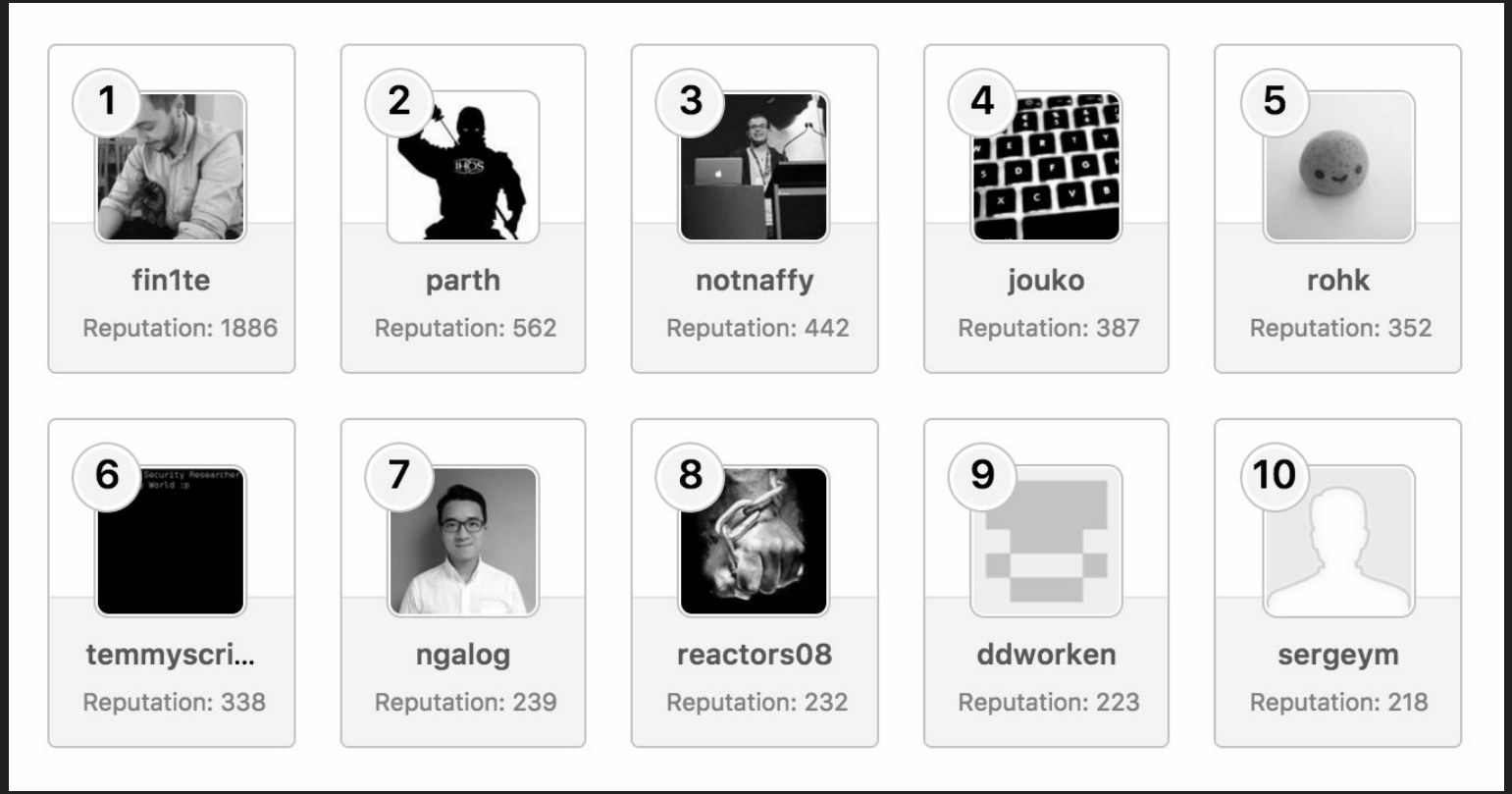
uber bug bounty program

security.uber.com - public program started on March 22, 2016

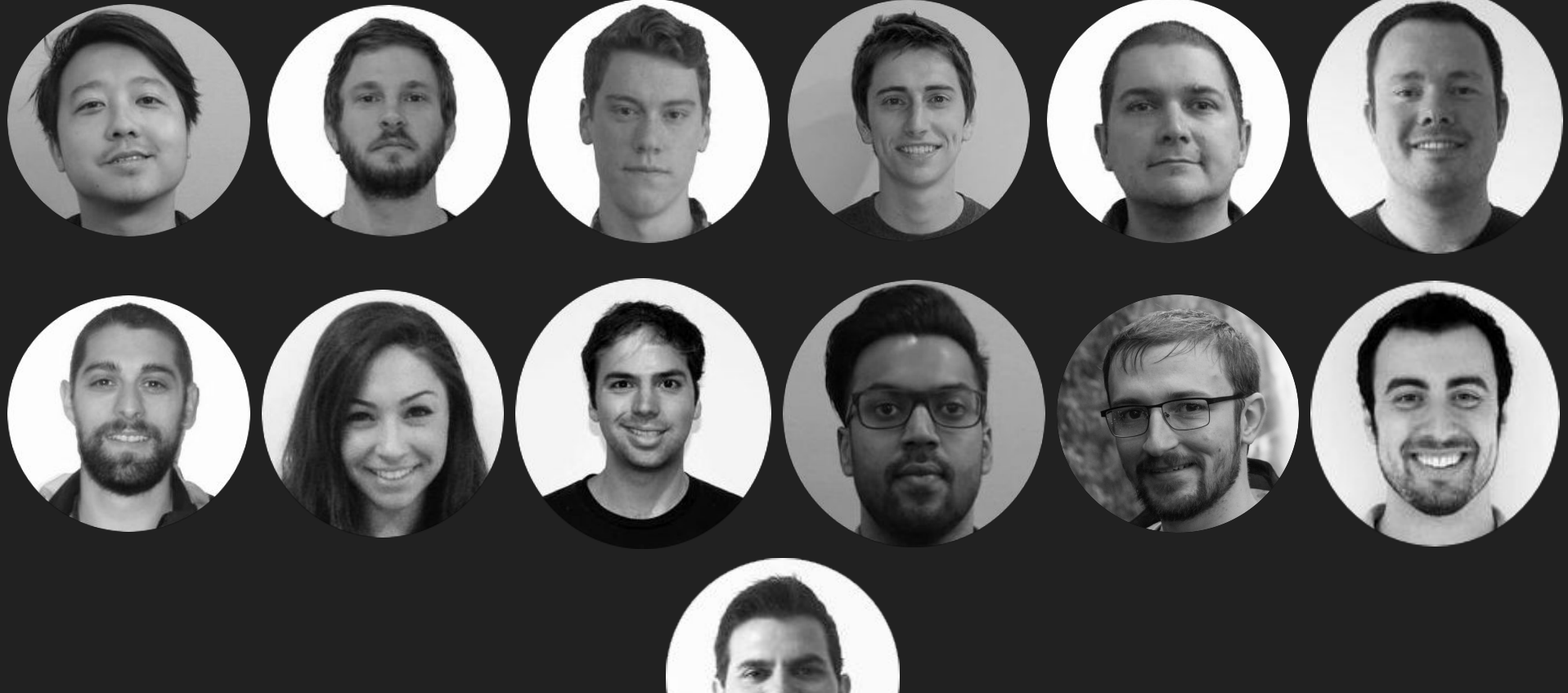
$974,000+ (€918,478+) in bounties; 500+ reports awarded bounty



the researchers



the team



agenda

soup to nuts: an ideal bug bounty experience

maximize report value: user security is our top priority

uber bug bounty program updates

soup to nuts: an ideal bug bounty experience

i·de·al - a person or thing regarded as perfect

GOOOOOOOAAAAAAAAAALLLLLLLL:
provide insight into our program's experiences and philosophies

benefit of the doubt: assume best intent

example: respectful peer-to-peer interactions vs adversarial interactions

program advantage: maintain healthy relationships with researchers

researcher advantage: maintain healthy relationships with programs

treat everyone with respect

evaluating security impact: willingness to learn and teach

example: understanding mitigations vs dire straits

program advantage: understand risk and prioritize

researcher advantage: higher bounty

be willing to teach; be willing to learn

report quality: succinct and reproducible

example: one-click POC vs speculative

program advantage: better reproducibility means we get our fix out faster

researcher advantage: faster time to bounty

be concise

concise - giving a lot of information clearly and in a few words; brief but comprehensive.

professionalism: patience and empathy

example: being proffesional vs “Bloody Mother Fucker..You already ruined the report via making me angry....and make me abuse you....!!”

program advantage: increased ability to understand nuances of report

researcher advantage: increased reputation in security community

bug bounty reports ≠ youtube comments

agenda

~~soup to nuts: an ideal bug bounty experience~~

maximize report value: user security is our top priority

uber bug bounty program updates

report value: user security is our top priority

security impact, not cleverness/complexity

scale of exposure

severity of exposure

$$$$	ATO; user datastore access
$$$	location data
$$	rate limiting issues
$	authorized data exposure

agenda

~~soup to nuts: an ideal bug bounty experience~~

~~maximize report value: user security is our top priority~~

uber bug bounty program updates

program updates: more money, faster

increase minimum bounty from $100 (€93.72) to $500 (€468.58)

award minimum bounty ($500) at time of triage

full bounty at time of resolution

Thanks for coming! Questions?

security.uber.com - come hack us and make money!