Analyzing Cryptographic Vulnerabilities on HackerOne

Atefeh Fakhari

Seminar Software Composition, MCS 2020

Supervisor : Mohammadreza Hazhirpasand

Objective

We are interested in looking for what types of cryptographic vulnerability exist on HackerOne.

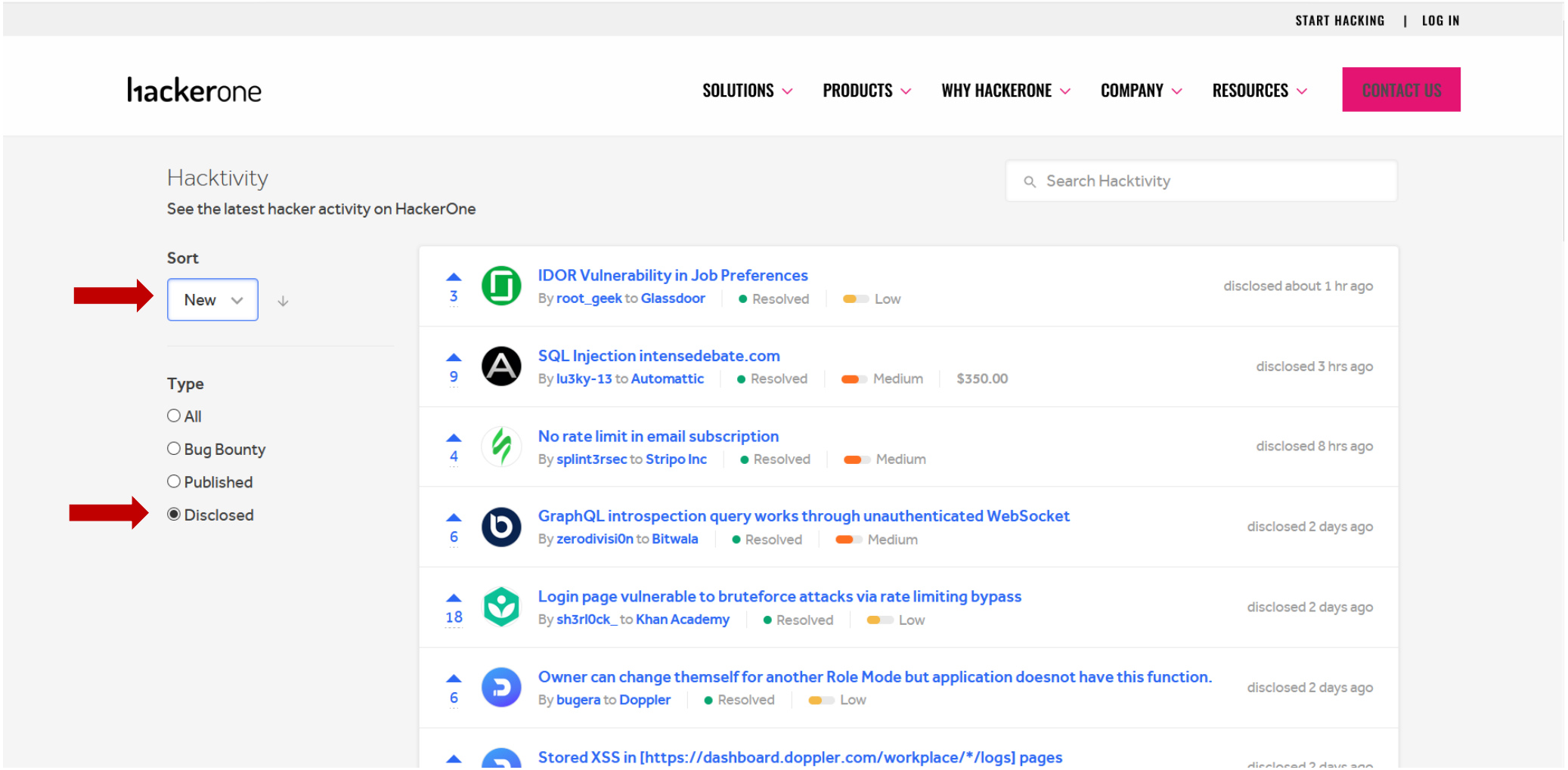
What is HackerOne?

Hacker finds a vulnerability

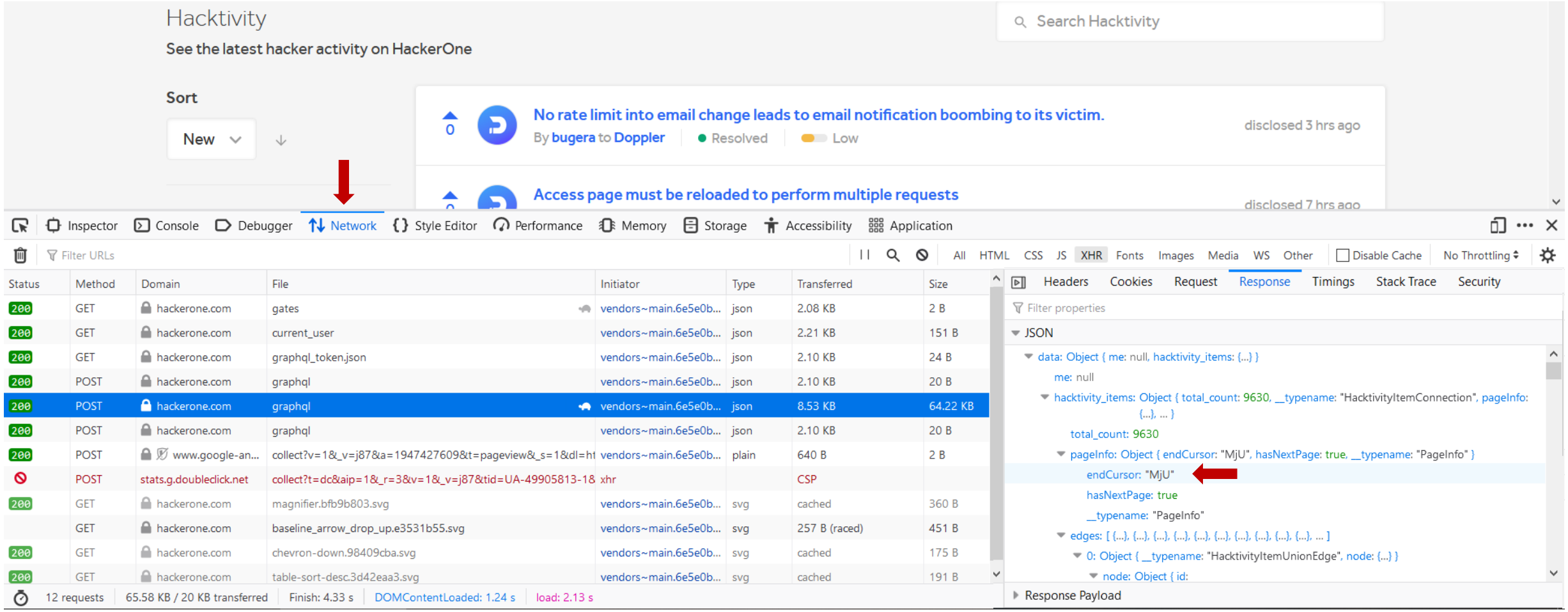
Hacker submits it to the company via their Security page

Company rewards the hacker

HackerOne


START HACKING | LOG IN
hackerone
SOLUTIONS
PRODUCTS
WHY HACKERONE
COMPANY
RESOURCES
CONTACT US
Hacktivity
See the latest hacker activity on HackerOne
Search Hacktivity
Sort
New
Type
All
Bug Bounty
Published
Disclosed
3
IDOR Vulnerability in Job Preferences
By root_geek to Glassdoor
Resolved
Low
disclosed about 1 hr ago
9
SQL Injection intensedebate.com
By lu3ky-13 to Automattic
Resolved
Medium
$350.00
disclosed 3 hrs ago
4
No rate limit in email subscription
By splint3rsec to Stripo Inc
Resolved
Medium
disclosed 8 hrs ago
6
GraphQL introspection query works through unauthenticated WebSocket
By zerodivisi0n to Bitwala
Resolved
Medium
disclosed 2 days ago
18
Login page vulnerable to bruteforce attacks via rate limiting bypass
By sh3rl0ck_ to Khan Academy
Resolved
Low
disclosed 2 days ago
6
Owner can change themself for another Role Mode but application doesnot have this function.
By bugera to Doppler
Resolved
Low
disclosed 2 days ago
Stored XSS in [https://dashboard.doppler.com/workplace/*/logs] pages

Data extraction with python



Dataset

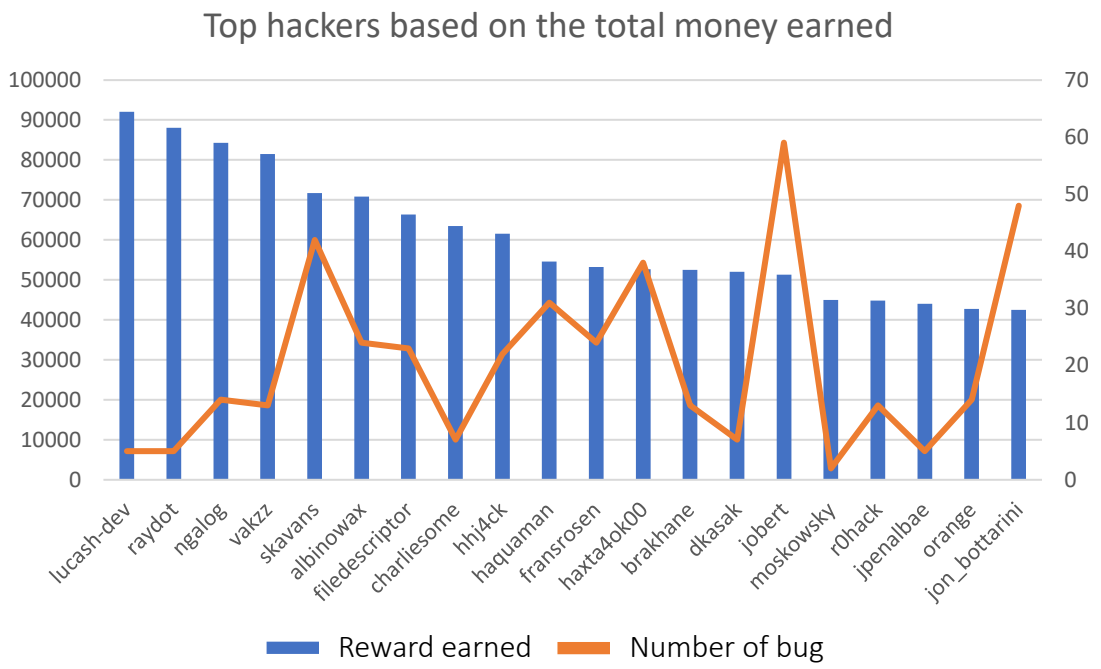
9311 Hacktivity

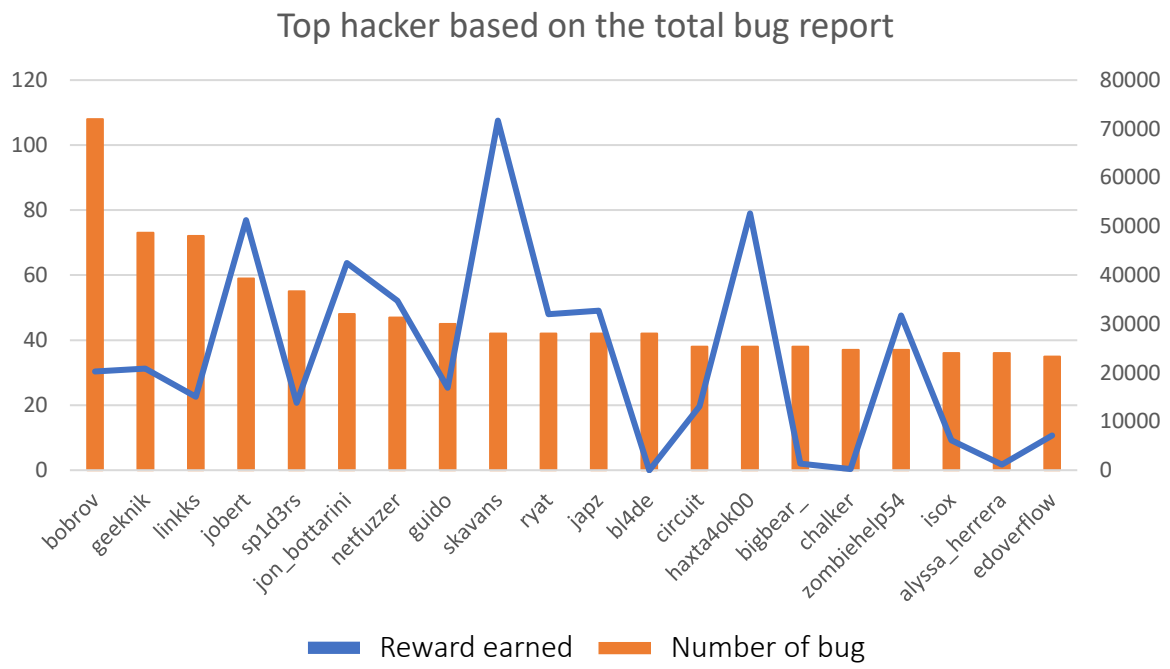
3160 Hackers

315 Companies

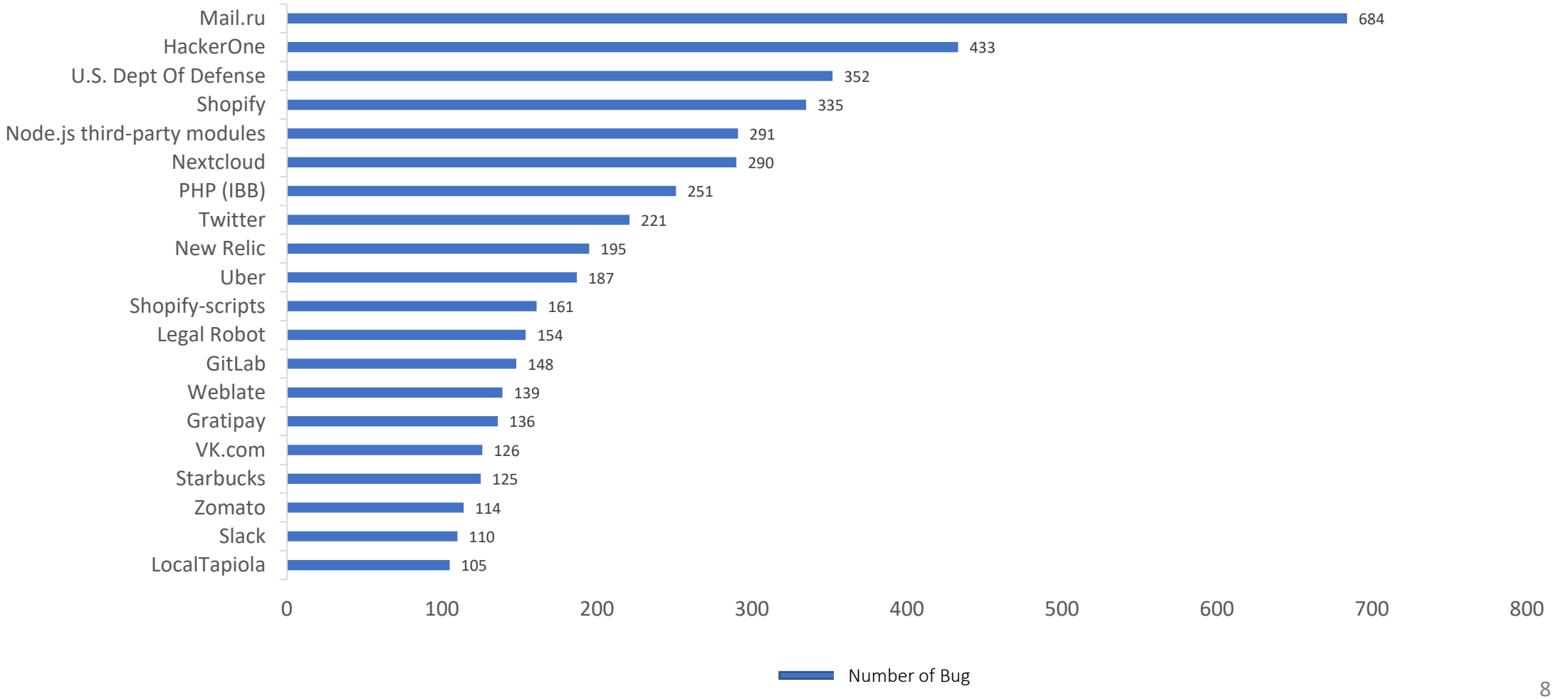
5,342,500

Top 20 hackers





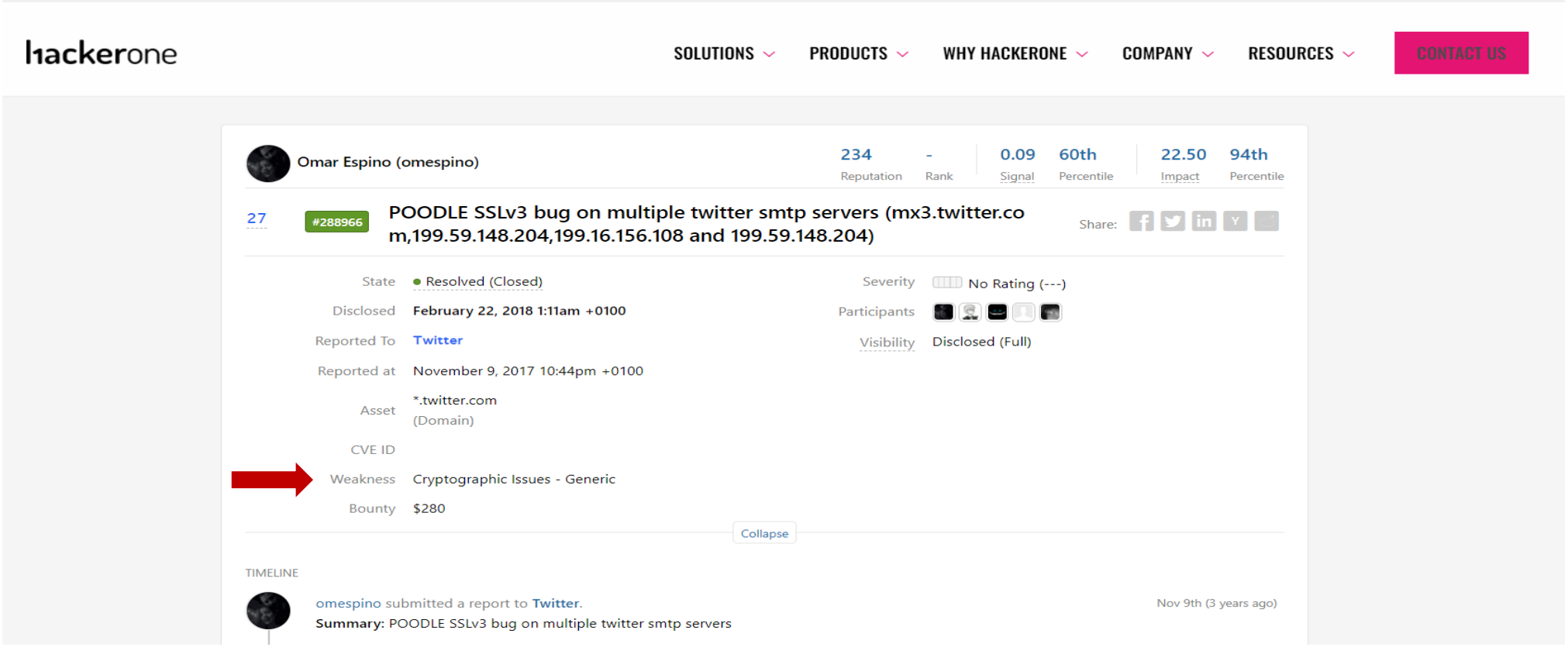
Top 20 companies



Analyzing cryptographic vulnerability

Weaknesses

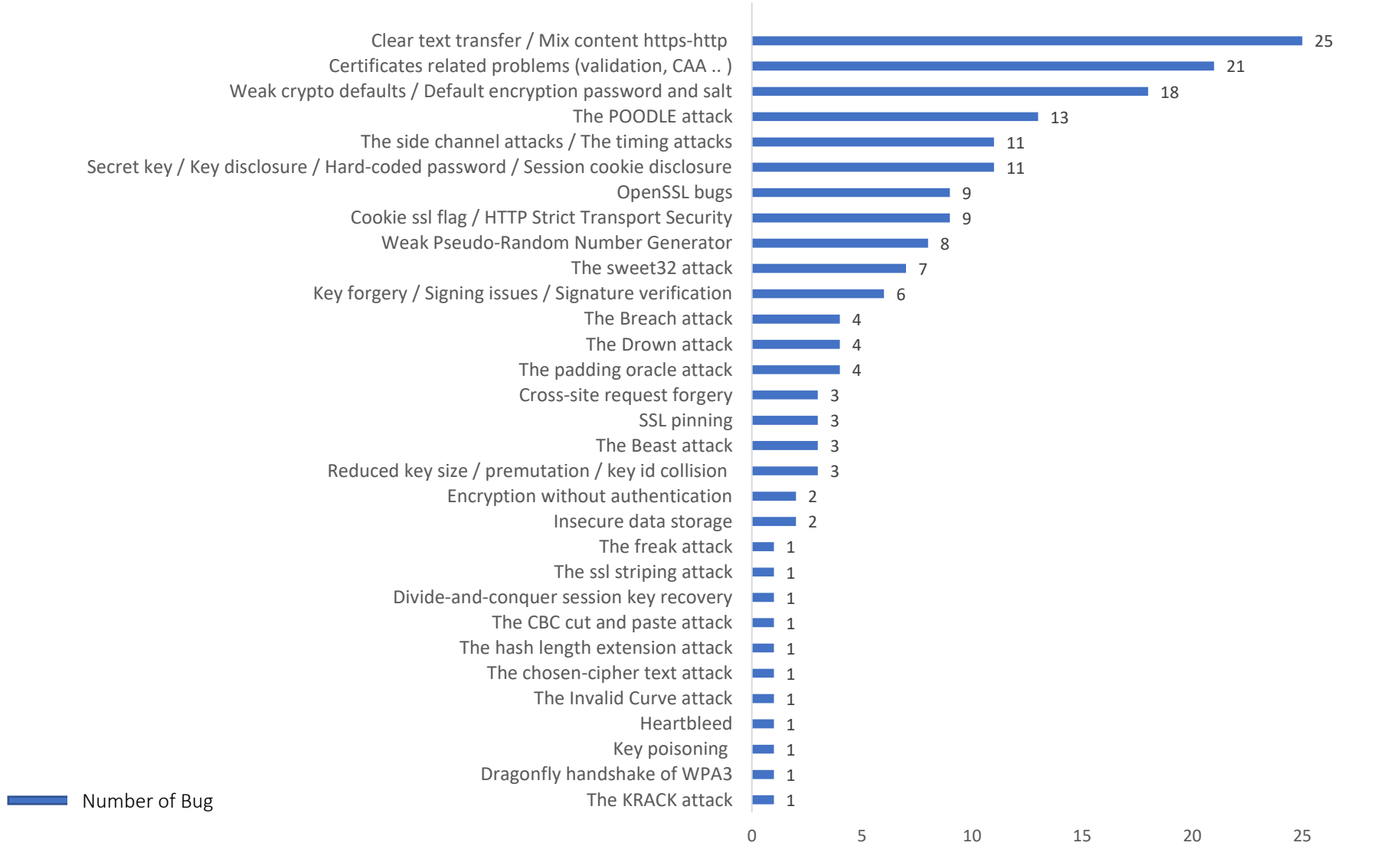
There are 121 unique weaknesses



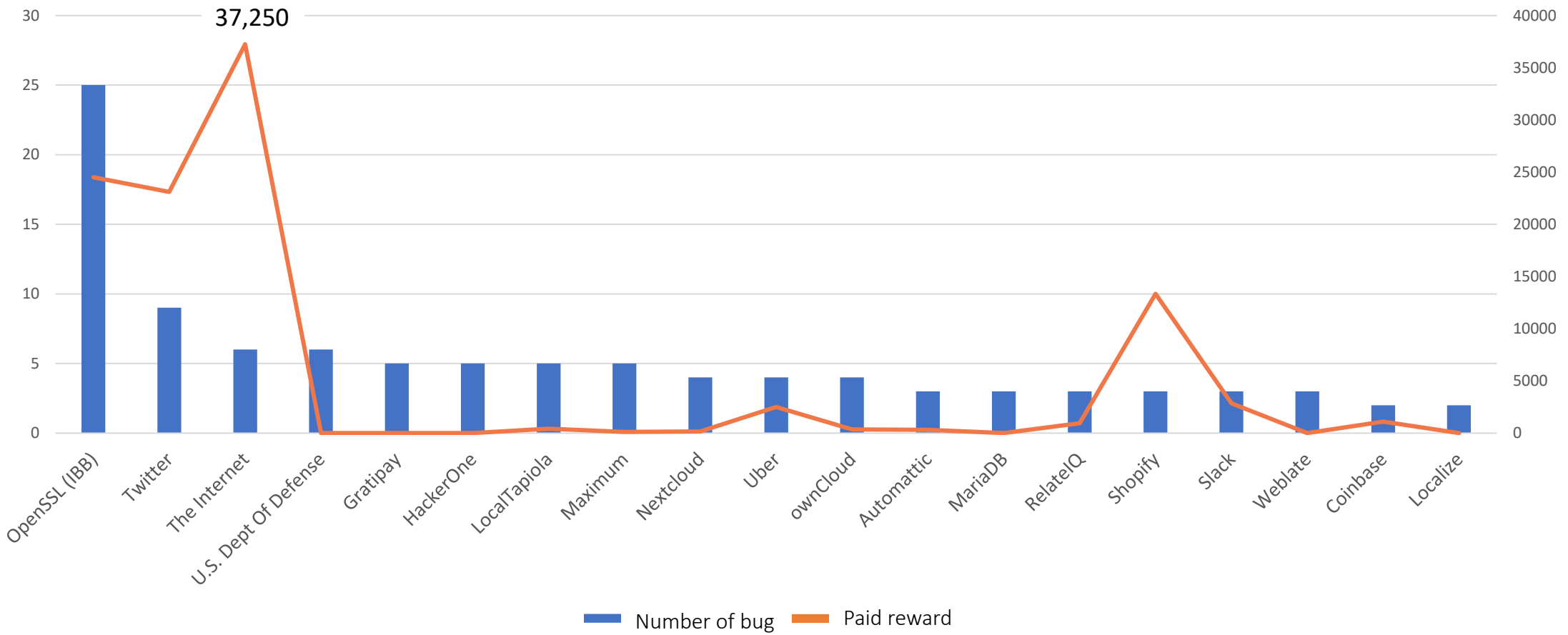
Weaknesses

Criteria	On HackerOne	Manual analysis
Weakness like '%crypto%'	180	115
Weakness like '%encrypt%' or '%auth%' or '%pass%' or '%private%' or '%ssl%'	670	167
Summary like '%crypto%' or '%encrypt%' or '%auth%' or '%pass%' or '%private%' or '%ssl%'	55	33

Crypto bug types

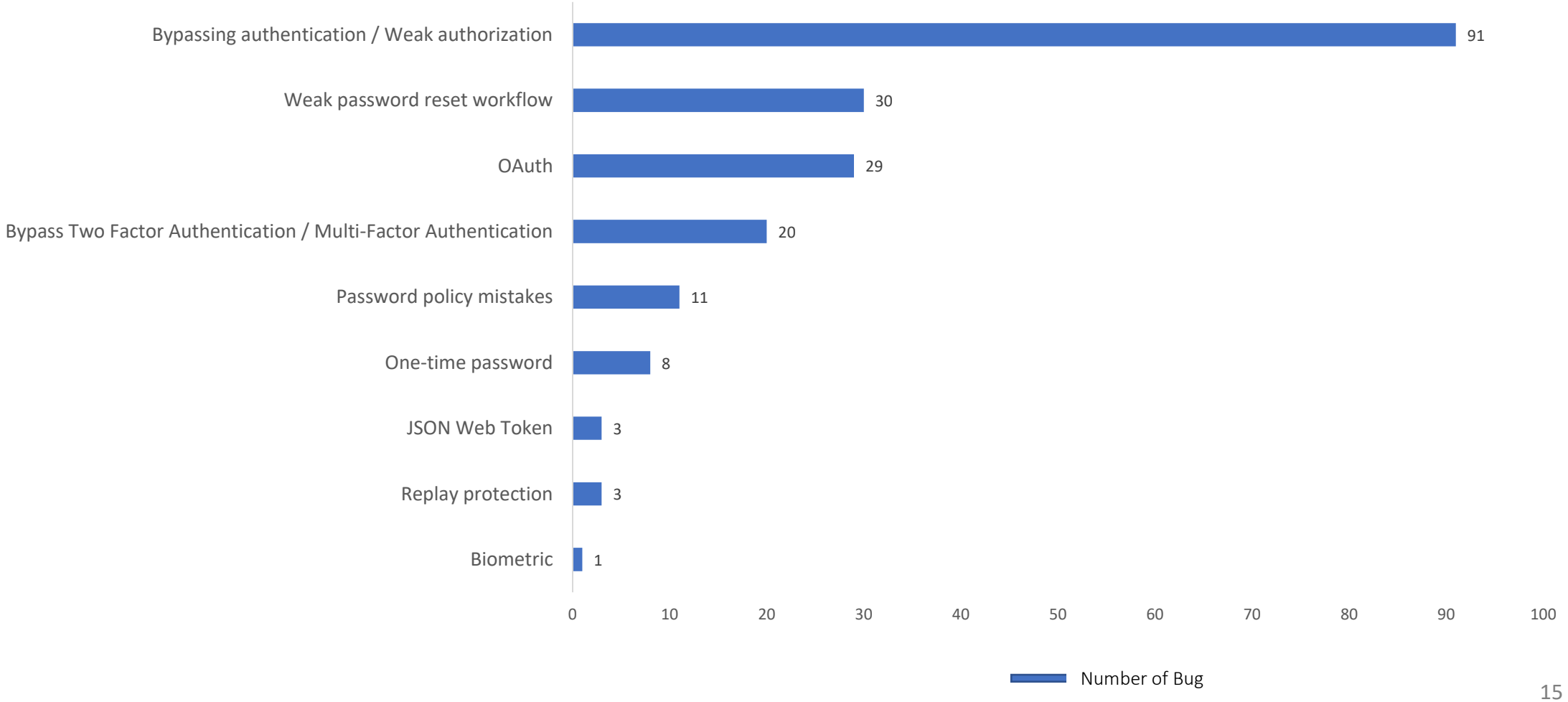


Companies’ crypto bugs

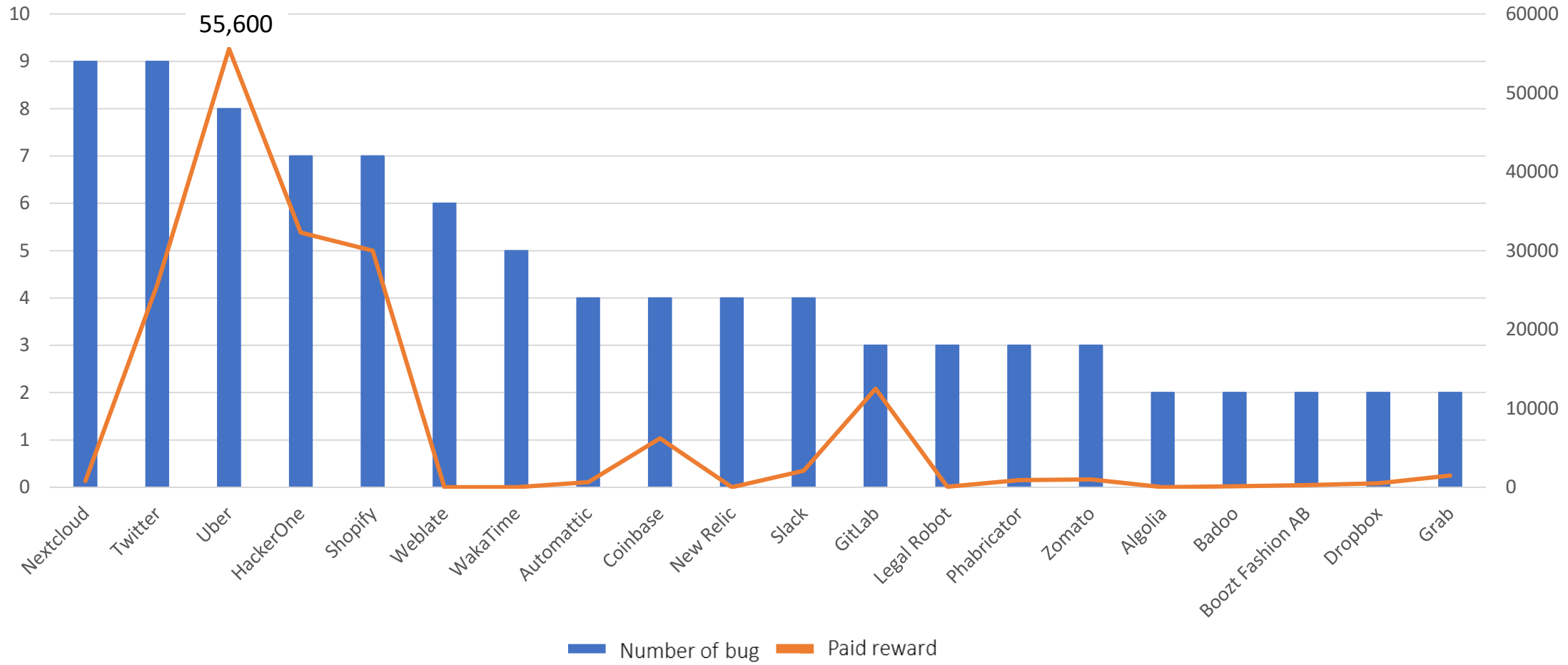


Authentication bugs types

Authentication bug types

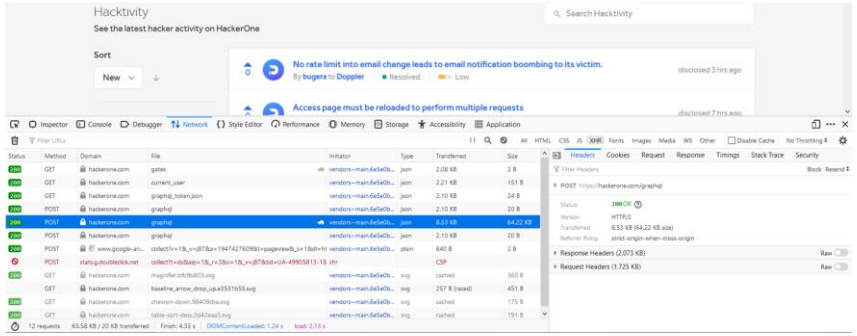


Companies’ authentication bugs



Summary

Data extraction



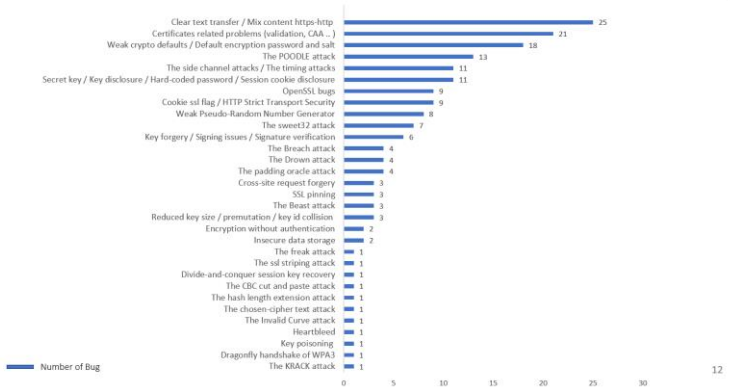
5

Weaknesses

Criteria	On HackerOne	Manual analysis
Weakness like '%crypto%'	180	115
Weakness like '%encrypt%' or '%auth%' or '%pass%' or '%private%' or '%ssl%'	670	167
Summary like '%crypto%' or '%encrypt%' or '%auth%' or '%pass%' or '%private%' or '%ssl%'	55	33

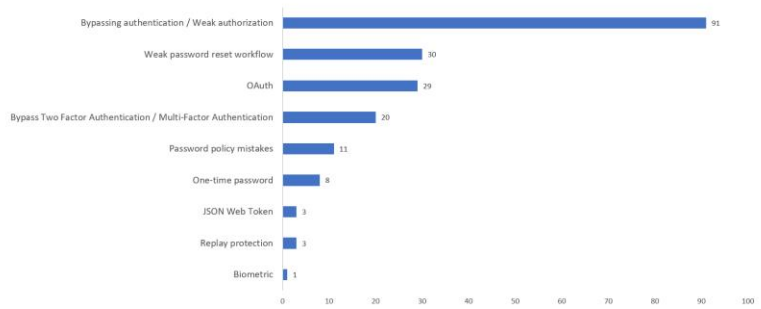
11

Crypto bug types



12

Authentication bug types



15