

# 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

The screenshot shows the HackerOne Hacktivity page. At the top right, there are links for "START HACKING" and "LOG IN". The main navigation bar includes "SOLUTIONS", "PRODUCTS", "WHY HACKERONE", "COMPANY", "RESOURCES", and a pink "CONTACT US" button. The page title is "hackerone". Below the navigation, the "Hacktivity" section is titled "See the latest hacker activity on HackerOne". A search bar labeled "Search Hacktivity" is present. On the left, there are filters for "Sort" (set to "New") and "Type" (with "Disclosed" selected). A list of vulnerabilities is displayed, each with a score, author, status, severity, and bounty amount.

Score	Author	Title	Status	Severity	Bounty	Time
3	root_geek	IDOR Vulnerability in Job Preferences	Resolved	Low		disclosed about 1 hr ago
9	lu3ky-13	SQL Injection intensedebate.com	Resolved	Medium	\$350.00	disclosed 3 hrs ago
4	splint3rsec	No rate limit in email subscription	Resolved	Medium		disclosed 8 hrs ago
6	zerodivisi0n	GraphQL introspection query works through unauthenticated WebSocket	Resolved	Medium		disclosed 2 days ago
18	sh3rl0ck_	Login page vulnerable to bruteforce attacks via rate limiting bypass	Resolved	Low		disclosed 2 days ago
6	bugera	Owner can change themselves for another Role Mode but application does not have this function.	Resolved	Low		disclosed 2 days ago
		Stored XSS in [https://dashboard.doppler.com/workplace/*/logs] pages				disclosed 2 days ago

# Data extraction with python

Hackactivity  
See the latest hacker activity on HackerOne

Sort  
New

No rate limit into email change leads to email notification boombing to its victim. disclosed 3 hrs ago  
By bugera to Doppler | Resolved | Low

Access page must be reloaded to perform multiple requests disclosed 7 hrs ago

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	hackerone.com	gates	vendors~main.6e5e0b...	json	2.08 KB	2 B
200	GET	hackerone.com	current_user	vendors~main.6e5e0b...	json	2.21 KB	151 B
200	GET	hackerone.com	graphql_token.json	vendors~main.6e5e0b...	json	2.10 KB	24 B
200	POST	hackerone.com	graphql	vendors~main.6e5e0b...	json	2.10 KB	20 B
200	POST	hackerone.com	graphql	vendors~main.6e5e0b...	json	8.53 KB	64.22 KB
200	POST	hackerone.com	graphql	vendors~main.6e5e0b...	json	2.10 KB	20 B
200	POST	www.google-an...	collect?v=1&v=j87&a=1947427609&t=pageview&s=1&dl=ht	vendors~main.6e5e0b...	plain	640 B	2 B
200	POST	stats.g.doubleclick.net	collect?t=dc&aip=1&r=3&v=1&v=j87&tid=UA-49905813-1&xhr		CSP		
200	GET	hackerone.com	magnifier.bfb9b803.svg	vendors~main.6e5e0b...	svg	cached	360 B
200	GET	hackerone.com	baseline_arrow_drop_up.e3531b55.svg	vendors~main.6e5e0b...	svg	257 B (raced)	451 B
200	GET	hackerone.com	chevron-down.98409cba.svg	vendors~main.6e5e0b...	svg	cached	175 B
200	GET	hackerone.com	table-sort-desc.3d42eaa3.svg	vendors~main.6e5e0b...	svg	cached	191 B

12 requests | 65.58 KB / 20 KB transferred | Finish: 4.33 s | DOMContentLoaded: 1.24 s | load: 2.13 s

Headers Cookies Request Response Timings Stack Trace Security

Filter properties

JSON

```
data: Object { me: null, hackactivity_items: (...) }
me: null
hackactivity_items: Object { total_count: 9630, __typename: "HackactivityItemConnection", pageInfo: {...}, ... }
total_count: 9630
pageInfo: Object { endCursor: "MjU", hasNextPage: true, __typename: "PageInfo" }
endCursor: "MjU"
hasNextPage: true
__typename: "PageInfo"
edges: [ {...}, {...}, {...}, {...}, {...}, {...}, {...}, {...}, {...}, {...}, ... ]
0: Object { __typename: "HackactivityItemUnionEdge", node: {...} }
node: Object { id:
```

# Dataset

---



9311 Hacktivity



3160 Hackers



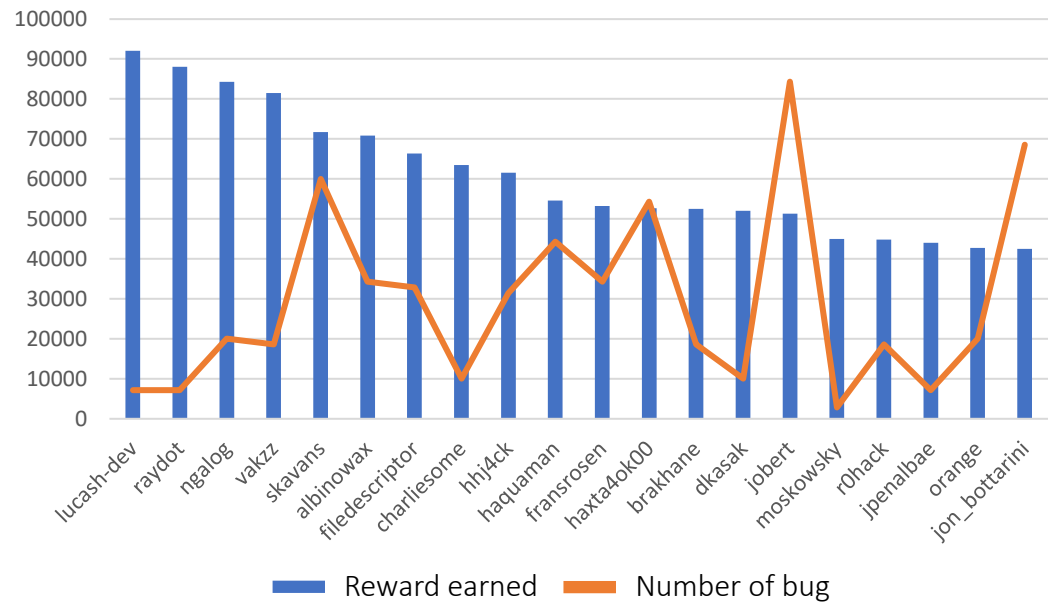
315 Companies



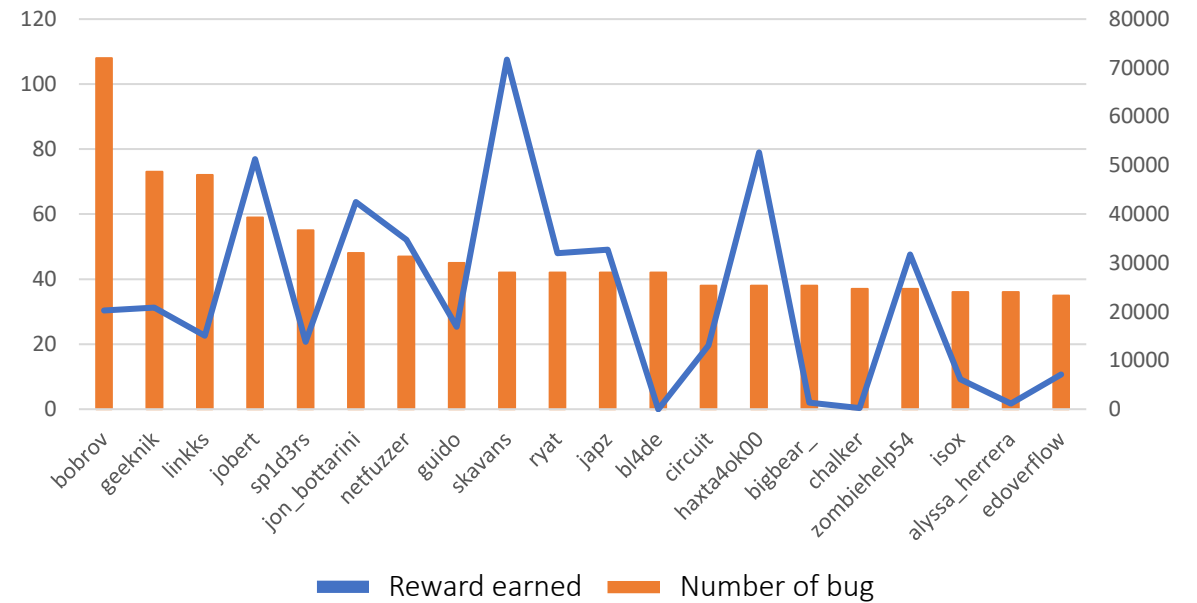
5,342,500

# Top 20 hackers

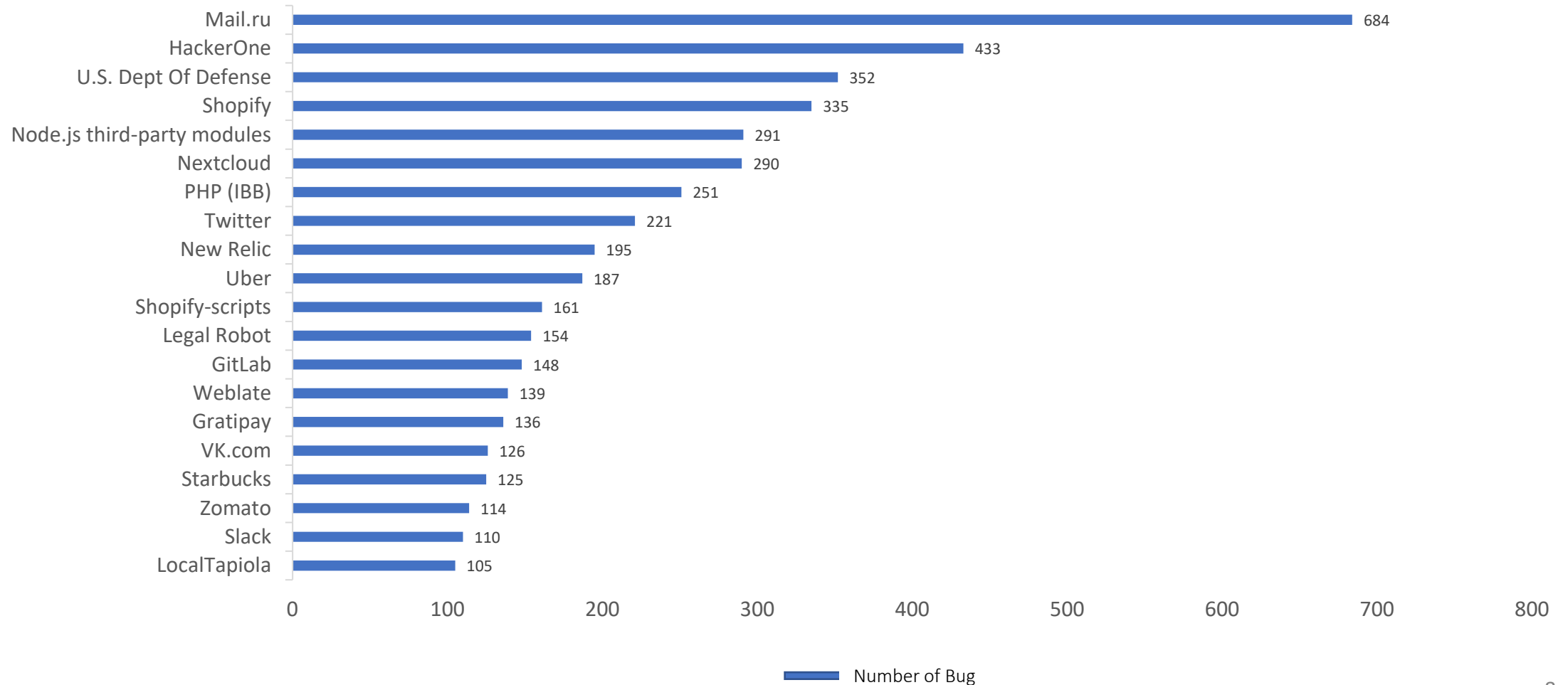
Top hackers based on the total money earned



Top hacker based on the total bug report



# Top 20 companies





# Analyzing cryptographic vulnerability

---

# Weaknesses

There are 121 unique weaknesses

The screenshot shows the Hackerone interface. At the top, there is a navigation bar with the Hackerone logo and links for SOLUTIONS, PRODUCTS, WHY HACKERONE, COMPANY, RESOURCES, and a CONTACT US button. The main content area displays a report by Omar Espino (omespino) with a reputation of 234, rank of -, signal of 0.09, 60th percentile, impact of 22.50, and 94th percentile. The report title is "#288966 POODLE SSLv3 bug on multiple twitter smtp servers (mx3.twitter.com, 199.59.148.204, 199.16.156.108 and 199.59.148.204)". The report details include: State: Resolved (Closed); Disclosed: February 22, 2018 1:11am +0100; Reported To: Twitter; Reported at: November 9, 2017 10:44pm +0100; Asset: \*.twitter.com (Domain); CVE ID: (empty); Weakness: Cryptographic Issues - Generic; Bounty: \$280. A red arrow points to the Weakness field. The report also shows a severity of "No Rating (---)", participants, and visibility set to "Disclosed (Full)". A timeline at the bottom shows the report was submitted to Twitter on Nov 9th (3 years ago).

**hackerone** SOLUTIONS ▾ PRODUCTS ▾ WHY HACKERONE ▾ COMPANY ▾ RESOURCES ▾ CONTACT US

**Omar Espino (omespino)** 234 Reputation - Rank 0.09 Signal 60th Percentile 22.50 Impact 94th Percentile

#288966 **POODLE SSLv3 bug on multiple twitter smtp servers (mx3.twitter.com, 199.59.148.204, 199.16.156.108 and 199.59.148.204)** Share:

State **Resolved (Closed)** Severity No Rating (---)

Disclosed **February 22, 2018 1:11am +0100** Participants

Reported To **Twitter** Visibility **Disclosed (Full)**

Reported at **November 9, 2017 10:44pm +0100**

Asset **\*.twitter.com (Domain)**

CVE ID

**Weakness** Cryptographic Issues - Generic

Bounty **\$280**

[Collapse](#)

**TIMELINE**

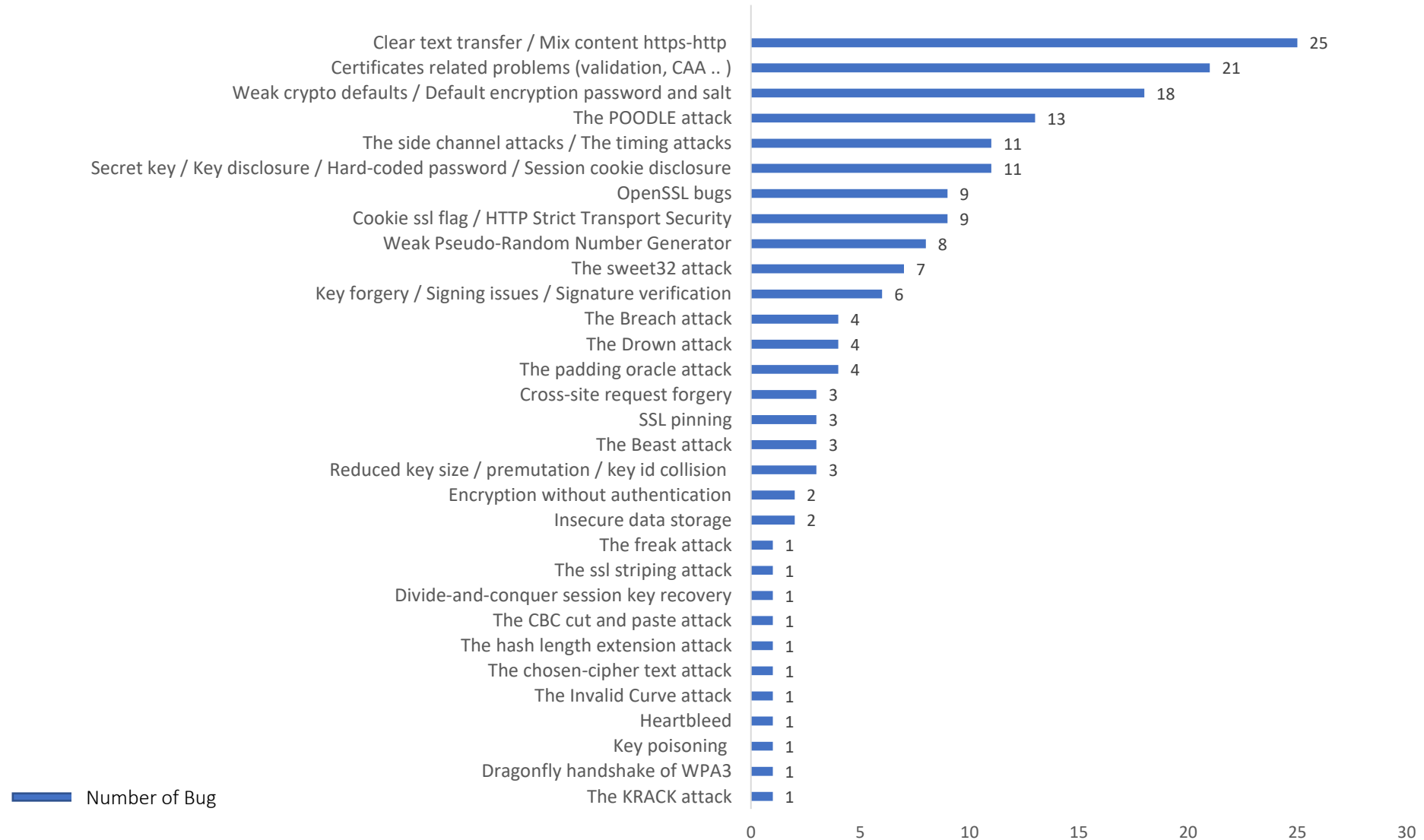
**omespino** submitted a report to **Twitter**. Nov 9th (3 years ago)

**Summary:** POODLE SSLv3 bug on multiple twitter smtp servers

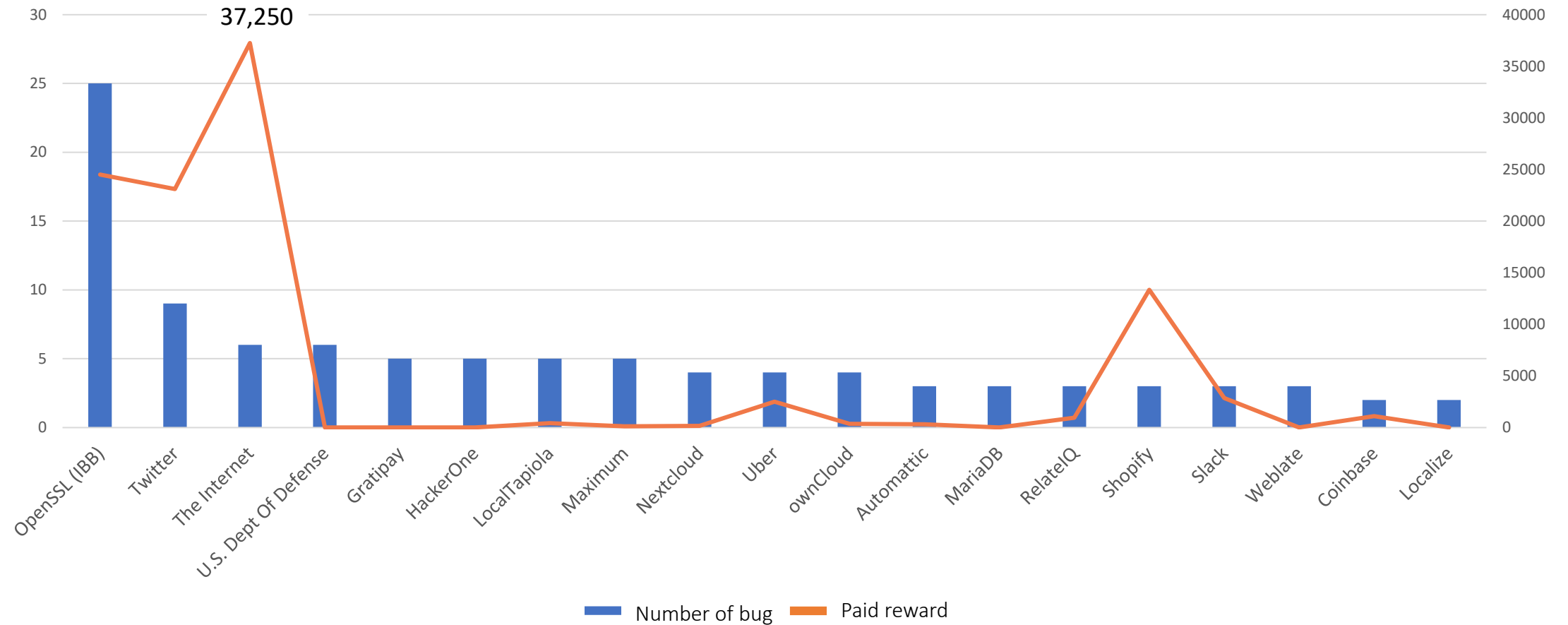
# Weaknesses

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



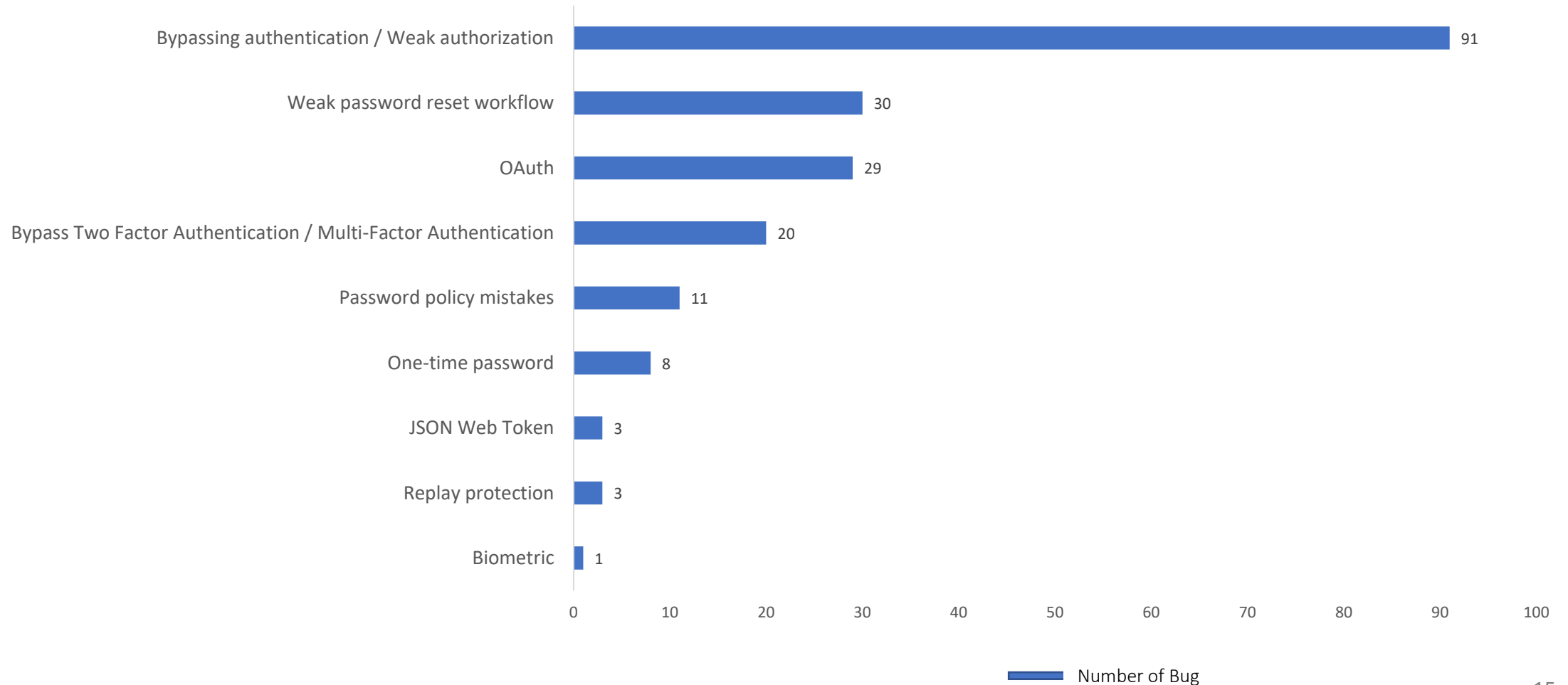
# Companies' crypto bugs



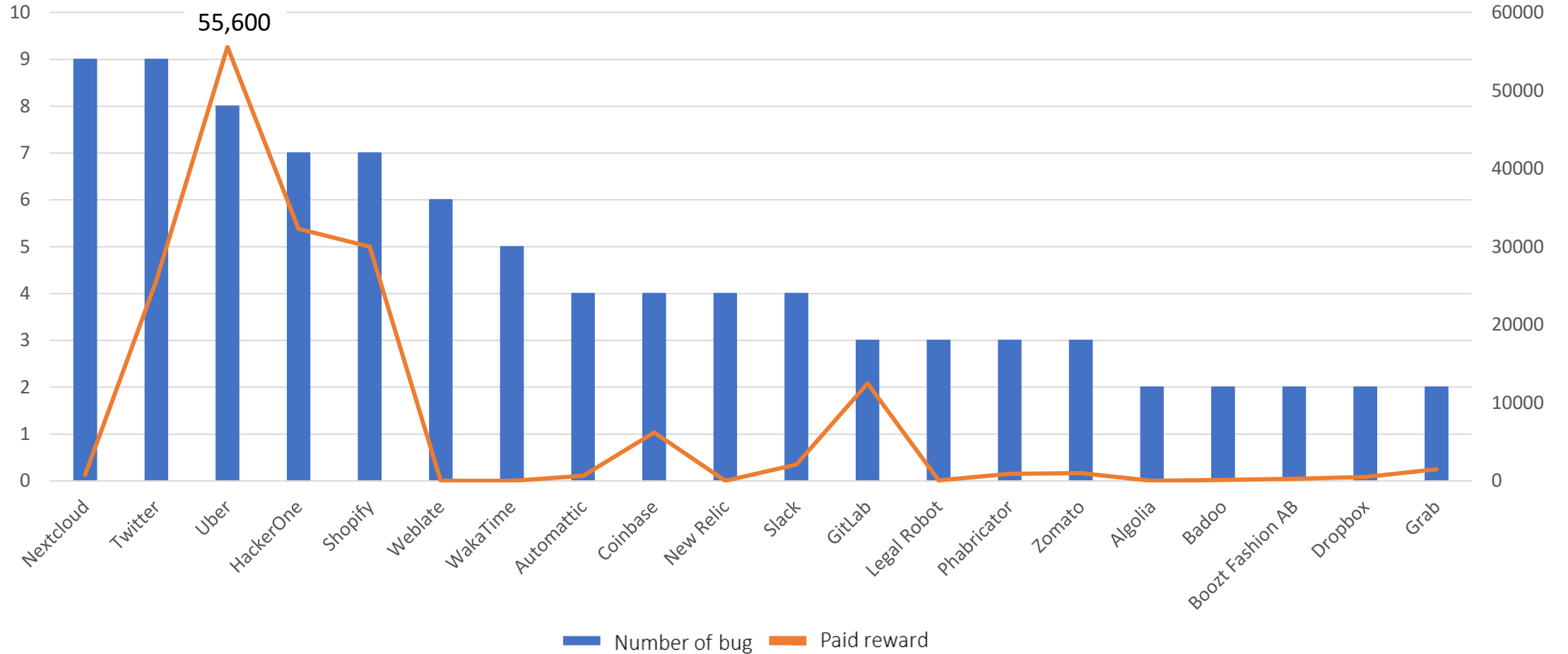
# Authentication bugs types

---

# Authentication bug types



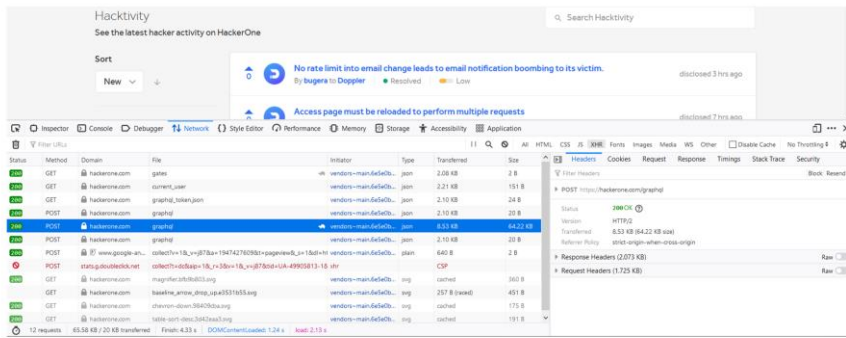
# Companies' authentication bugs





# Summary

## Data extraction



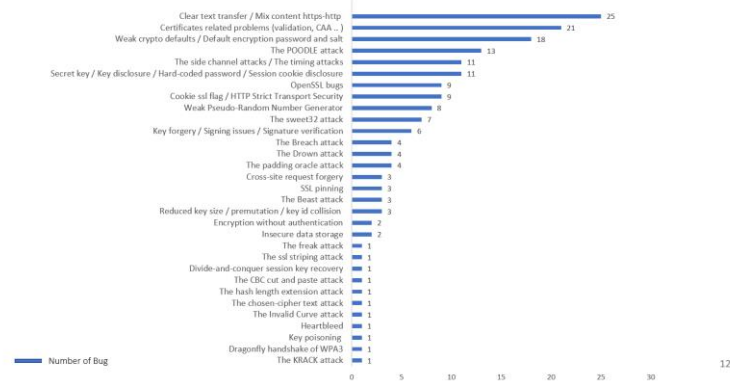
5

## 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

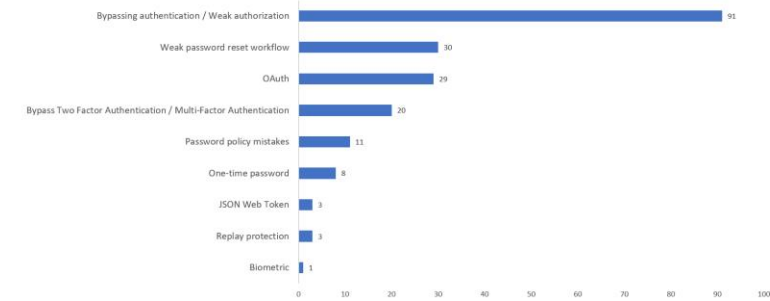
11

## Crypto bug types



12

## Authentication bug types



15