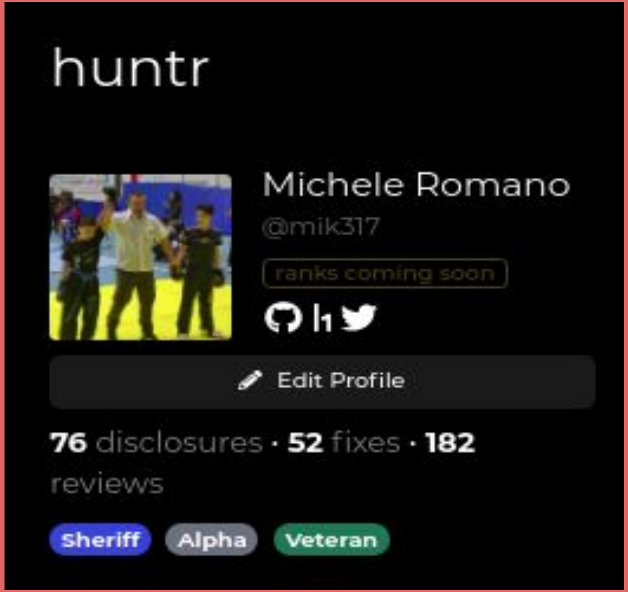
Open Source BB - Methodology, tools and resources

Author: Michele Romano aka Mik317 (ex Huntr Sheriff && Veteran Huntr)

WHOAMI

- Michele Romano aka Mik317 (mik317_)
- Bug Hunter acknowledged by more than 100 companies && Top 0x3 All-Time Huntr && Top 100 All-Time H1
- Open source Huntr with more than 300 contributions (fixes, disclosures and reviews)



huntr

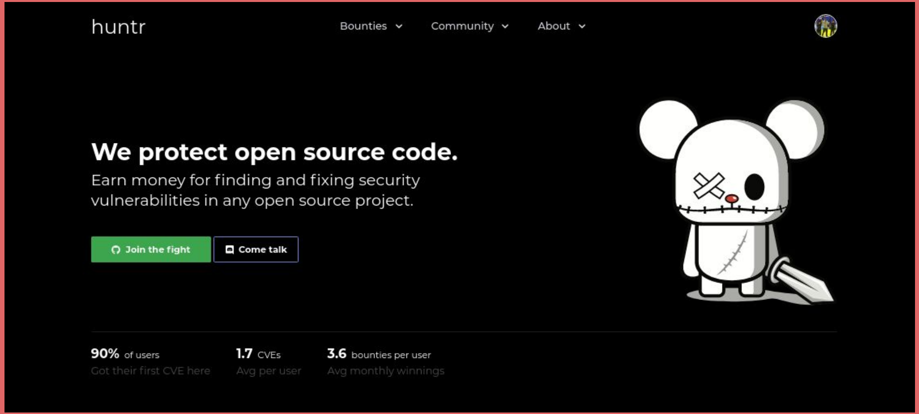
Michele Romano
@mik317
ranks coming soon

76 disclosures · 52 fixes · 182 reviews

HUNTR

- Platform for protecting Open Source @ https://huntr.dev/
- Scope == All the Open Source projects*
- You can both fix and disclose
- No more “Security through obscurity”

*: The maintainers of the repo have to accept your fix!



We protect open source code.

Earn money for finding and fixing security vulnerabilities in any open source project.

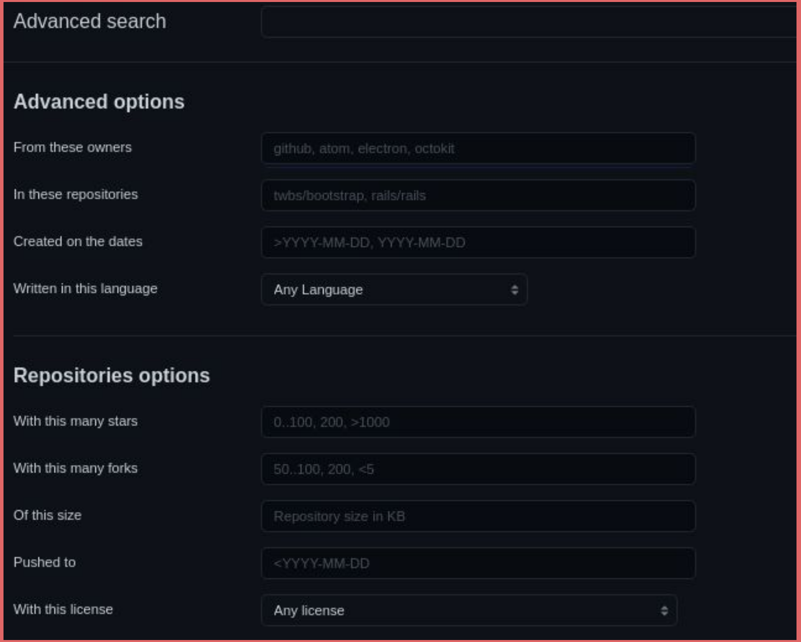
90% of users
Got their first CVE here

1.7 CVEs
Avg per user

3.6 bounties per user
Avg monthly winnings

Methodology

- Always starts with **recon**
- Useful tools:
  - Google dorks
  - GHDB
  - Advanced search @ Github
  - Advanced search @ “registry name”
  - Merge-chance
  - Grep.app and regexes
  - Debuggers and breakpoints
  - Dependency check



Advanced search

Advanced options

From these owners	github, atom, electron, octokit
In these repositories	twbs/bootstrap, rails/rails
Created on the dates	>YYYY-MM-DD, YYYY-MM-DD
Written in this language	Any Language

Repositories options

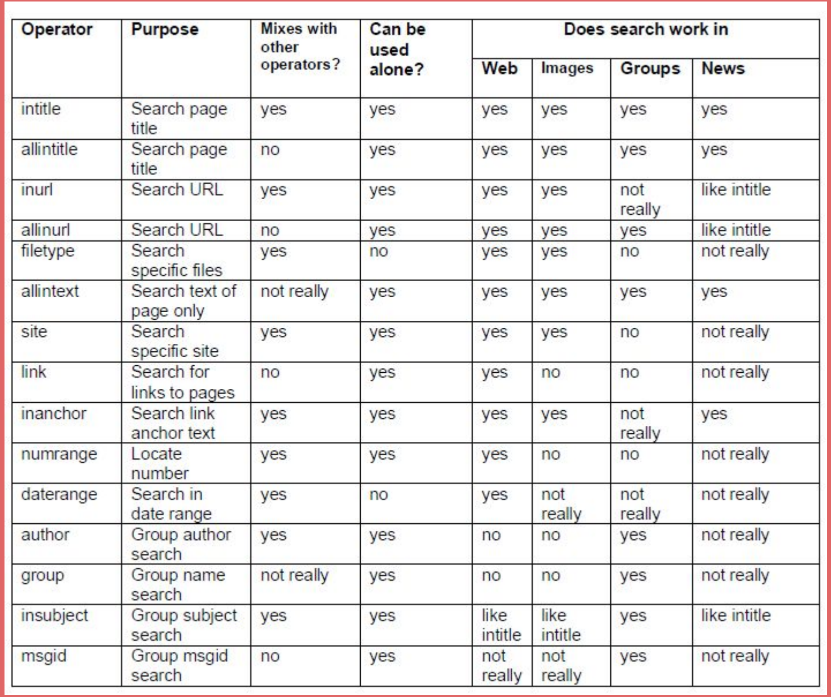
With this many stars	0..100, 200, >1000
With this many forks	50..100, 200, <5
Of this size	Repository size in KB
Pushed to	<YYYY-MM-DD
With this license	Any license

Google Dorks

- Allow you to make queries to return just the content you really need
- Useful to find pieces of vulnerable code and packages
- Do practice with https://www.exploit-db.com/google-hacking-database

TO REMEMBER:

- site:example.com
- filetype:extension
- OR operator
- Remove results with word “xyz” (-xyz)
- Find results with exact word (“xyz”)
- Wildcard operator (*)



Operator	Purpose	Mixes with other operators?	Can be used alone?	Does search work in			
				Web	Images	Groups	News
intitle	Search page title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	Search specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

Github Advanced Search && Registry AS

- Located @ https://github.com/search/advanced
- Filter results in order to find vulnerable code, filtering for profile/company, language used, filenames and paths

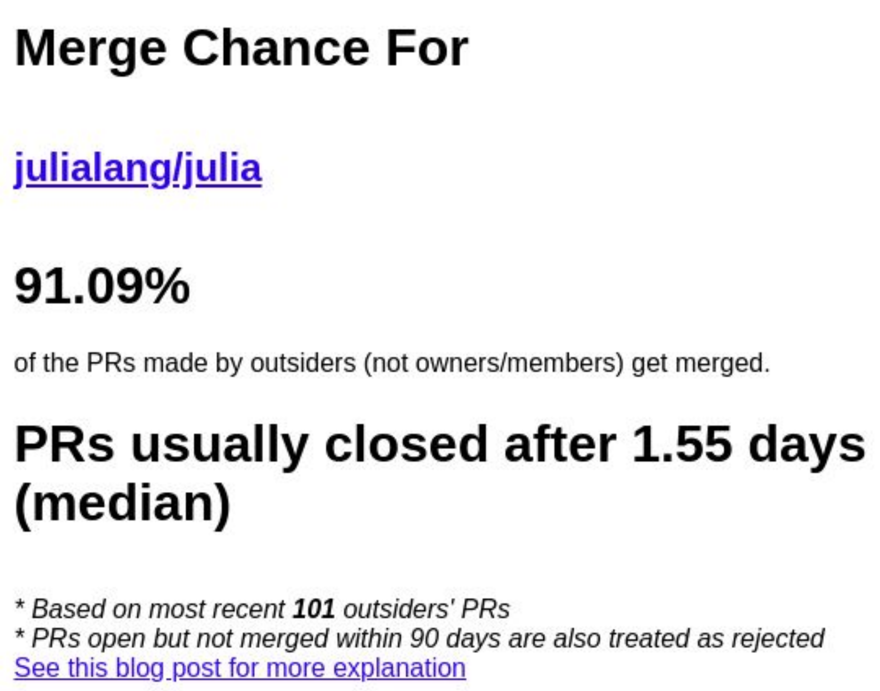
- Different from registry to registry
- Filter for name, author, code language, update status and download

Registry	**Language**	**Located @**
NPM	NodeJS, JS, TS and ECMA	https://www.npmjs.com
Pypi	Python	https://pypi.org
Maven	Mostly Java	https://search.maven.org/
Packagist	PHP	https://packagist.org/

Merge-Chance

- Located @ https://merge-chance.info
- Makes easier understanding if your PR will be accepted or not (from this depends your **payout**)
- Could be automated (I would have done if I wasn't a lazy person)
- Returns even an average of days you'll have to wait

Pro tip: Use this before actually spending much time hunting on a repo you didn't check. Definitely don't work on **archived** projects



Merge Chance For

julialang/julia

91.09%

of the PRs made by outsiders (not owners/members) get merged.

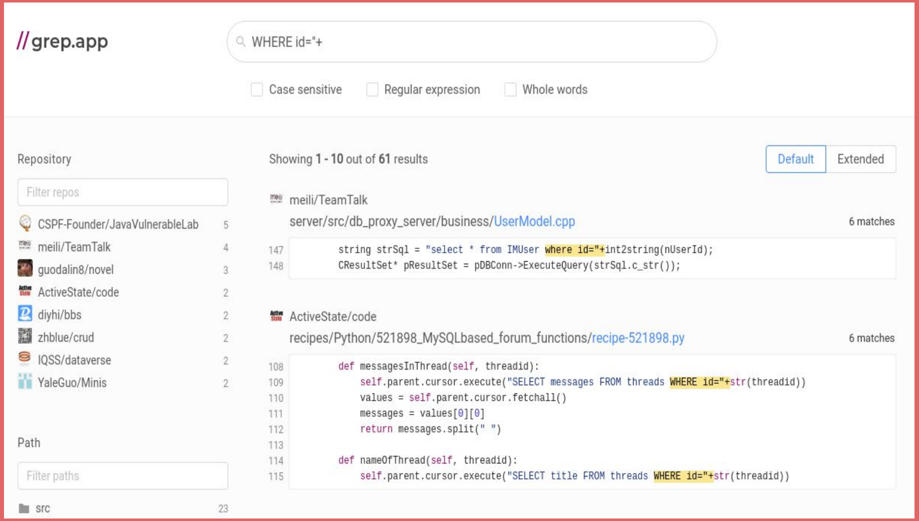
PRs usually closed after 1.55 days (median)

** Based on most recent **101** outsiders' PRs*
** PRs open but not merged within 90 days are also treated as rejected*
See this blog post for more explanation

Grep.app

- Located @ https://grep.app/
- Allows you to search for vulnerable **code snippets** and filter the results
- You can search for exact words or just use **regexes**

You can learn regex through https://regexone.com. This will speed up the entire process and give more good results



WHERE id="+

□ Case sensitive □ Regular expression □ Whole words

Showing **1 - 10** out of **61** results

Repository	
CSPF-Founder/JavaVulnerableLab	5
meili/TeamTalk	4
guodalin8/novel	3
ActiveState/code	2
diyhi/bbs	2
zhblue/crud	2
IQSS/dataverse	2
YaleGuo/Minis	2

Path	
src	23

meili/TeamTalk

server/src/db_proxy_server/business/UserModel.cpp — 6 matches

```
        string strSql = "select * from IMUser where id="+int2string(nUserId);
        CResultSet* pResultSet = pDBConn->ExecuteQuery(strSql.c_str());
```

ActiveState/code

recipes/Python/521898_MySQLbased_forum_functions/recipe-521898.py — 6 matches

```
        def messagesInThread(self, threadid):
            self.parent.cursor.execute("SELECT messages FROM threads WHERE id="+str(threadid))
            values = self.parent.cursor.fetchall()
            messages = values[0][0]
            return messages.split(" ")

        def nameOfThread(self, threadid):
            self.parent.cursor.execute("SELECT title FROM threads WHERE id="+str(threadid))
```