to make out like a bandit

1. to get a lot of something for free
2. to make a large profit

Marriam-Webster
SINCE 1828

https://github.com/PyCQA/bandit

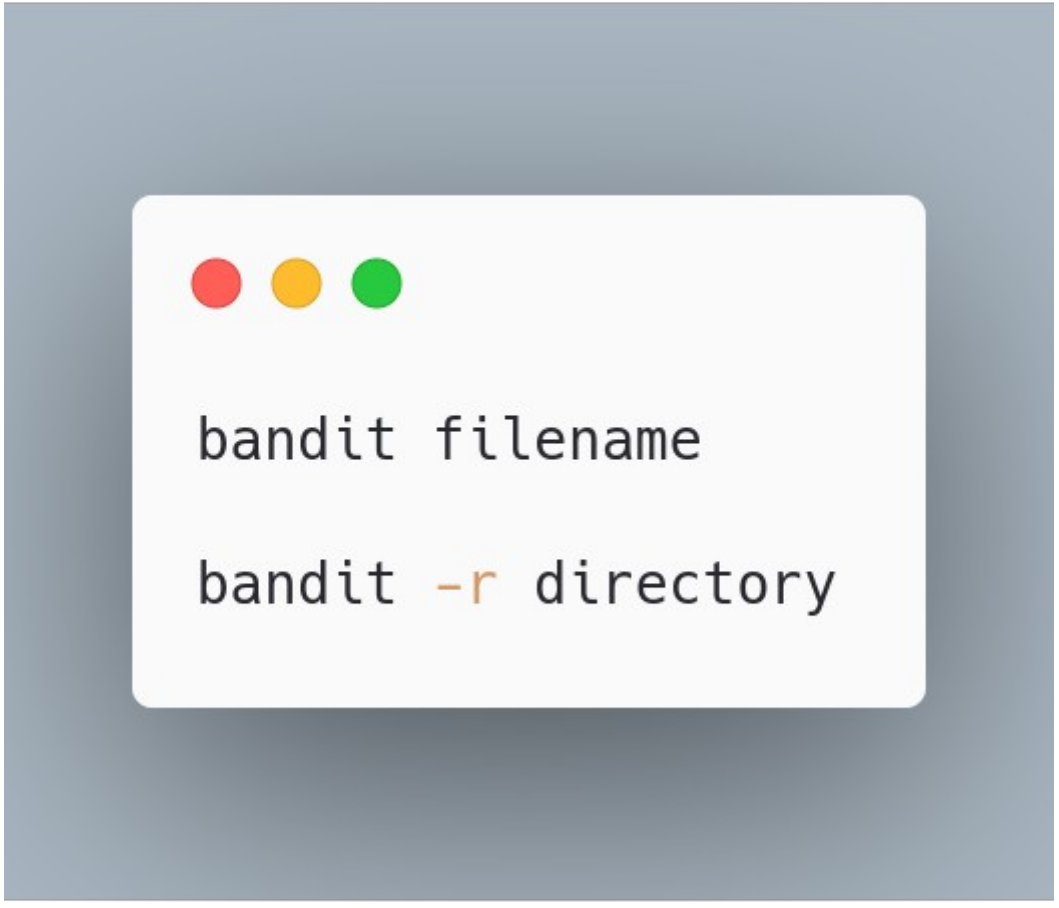
How does it work?

- parses source code
- builds abstract syntax tree (AST)
- applies checks
- generates report

How to get started?

https://github.com/pipxproject/pipx

run bandit



hibpcli


jugmac00@jugmac00-XPS-13-9370:~/Projects/hibpcli$ bandit -r hibpcli/
[main] INFO profile include tests: None
[main] INFO profile exclude tests: None
[main] INFO cli include tests: None
[main] INFO cli exclude tests: None
[main] INFO running on Python 3.6.8
Run started:2019-10-04 13:16:13.476316
Test results:
>> Issue: [B303:blacklist] Use of insecure MD2, MD4, MD5, or SHA1 hash function.
Severity: Medium Confidence: High
Location: hibpcli/password.py:23
More Info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b303-md5
22 def _generate_hash(self):
23 hash_object = hashlib.sha1(bytes(self.password, "UTF-8"))
24 hex_digest = hash_object.hexdigest().upper()
Code scanned:
Total lines of code: 54
Total lines skipped (#nosec): 0
Run metrics:
Total issues (by severity):
Undefined: 0.0
Low: 0.0
Medium: 1.0
High: 0.0
Total issues (by confidence):
Undefined: 0.0
Low: 0.0
Medium: 0.0
High: 1.0
Files skipped (0):

Zope

```
jugmac00@jugmac00-XPS-13-9370:~/Projects$ bandit -r Zope/src/OFS
[main]  INFO    profile include tests: None
[main]  INFO    profile exclude tests: None
[main]  INFO    cli include tests: None
[main]  INFO    cli exclude tests: None
[main]  INFO    running on Python 3.6.8
68 [0.. 50.. ]
Run started:2019-10-07 09:05:03.276526

Test results:
>> Issue: [B306:blacklist] Use of insecure and deprecated function (mktemp).
   Severity: Medium   Confidence: High
   Location: Zope/src/OFS/tests/testAppInitializer.py:27
   More Info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b306-mktemp-q
26
27  TEMPNAME = tempfile.mktemp()
28  TEMPPRODUCTS = os.path.join(TEMPNAME, "Products")

Code scanned:
    Total lines of code: 11419
    Total lines skipped (#nosec): 0

Run metrics:
    Total issues (by severity):
        Undefined: 0.0
        Low: 15.0
        Medium: 1.0
        High: 0.0
    Total issues (by confidence):
        Undefined: 0.0
        Low: 0.0
        Medium: 4.0
        High: 12.0
Files skipped (0):
```

automatic testing

- pre-commit
- continuous integration (e.g. travis)

even more security

- OWASP Top 10
- https://www.owasp.org

wrap up

- bandit is a static code analysis tool
- consider pipx for installing Python cli tools
- use pre-commit / ci for automatic testing
- have a look at OWASP

contact me

- Twitter: @jugmac00
- github: @jugmac00
- Web: jugmac00.github.io