```
Run started:2020-12-04 03:17:47.553127

Test results:
>> Issue: [B314:blacklist] Using xml.etree.ElementTree.fromstring to parse untrusted
XML data is known to be vulnerable to XML attacks. Replace
xml.etree.ElementTree.fromstring with its defusedxml equivalent function or make
sure defusedxml.defuse_stdlib() is called
   Severity: Medium   Confidence: High
   Location: liberapay.com-master/liberapay/elsewhere/_base.py:108
   More Info:
https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b313-b320-xm
l-bad-elementtree
107             elif api_format == 'xml':
108                 self.api_parser = lambda r: ET.fromstring(r.content)
109             elif api_format:

--------------------------------------------------
>> Issue: [B303:blacklist] Use of insecure MD2, MD4, MD5, or SHA1 hash function.
   Severity: Medium   Confidence: High
   Location: liberapay.com-master/liberapay/elsewhere/_base.py:265
   More Info:
https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b303-md5
264                     bs = r.email.strip().lower().encode('utf8')
265                     gravatar_id = hashlib.md5(bs).hexdigest()
266                 if gravatar_id:

--------------------------------------------------
>> Issue: [B303:blacklist] Use of insecure MD2, MD4, MD5, or SHA1 hash function.
   Severity: Medium   Confidence: High
   Location: liberapay.com-master/liberapay/i18n/extract.py:13
   More Info:
https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b303-md5
12              if isinstance(msg, tuple) and msg[0] == '':
13                  unused = "<unused singular (hash=%s)>" %
md5(msg[1].encode('utf8')).hexdigest()
14                  msg = (unused, msg[1], msg[2])

--------------------------------------------------
>> Issue: [B307:blacklist] Use of possibly insecure function - consider using safer
ast.literal_eval.
   Severity: Medium   Confidence: High
   Location: liberapay.com-master/liberapay/i18n/plural_rules.py:25
   More Info:
https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b307-eval
24          rule = or_re.sub(' or ', rule)
25          return eval('lambda n: ' + rule, {'__builtins__': {}})

--------------------------------------------------
>> Issue: [B608:hardcoded_sql_expressions] Possible SQL injection vector through
string-based query construction.
```

```
   Severity: Medium   Confidence: Low
   Location: liberapay.com-master/liberapay/models/repository.py:70
   More Info:
https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html
69                      RETURNING repositories
70              """.format(cols, placeholders, on_conflict_set), vals))
71          return r

--------------------------------------------------
>> Issue: [B307:blacklist] Use of possibly insecure function - consider using safer
ast.literal_eval.
   Severity: Medium   Confidence: High
   Location: liberapay.com-master/liberapay/renderers/csv_dump.py:10
   More Info:
https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b307-eval
9           def render_content(self, context):
10              rows = eval(self.compiled, globals(), context)
11              if not rows:

--------------------------------------------------
>> Issue: [B314:blacklist] Using xml.etree.ElementTree.fromstring to parse untrusted
XML data is known to be vulnerable to XML attacks. Replace
xml.etree.ElementTree.fromstring with its defusedxml equivalent function or make
sure defusedxml.defuse_stdlib() is called
   Severity: Medium   Confidence: High
   Location: liberapay.com-master/liberapay/testing/elsewhere.py:126
   More Info:
https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b313-b320-
xml-bad-elementtree
125
126     openstreetmap = lambda: ET.fromstring("""
127      <!-- copied from http://wiki.openstreetmap.org/wiki/API_v0.6 -->
128      <osm version="0.6" generator="OpenStreetMap server">
129        <user id="12023" display_name="jbpbis"
account_created="2007-08-16T01:35:56Z">
130          <description></description>
131          <contributor-terms agreed="false"/>
132          <img
href="http://www.gravatar.com/avatar/c8c86cd15f60ecca66ce2b10cb6b9a00.jpg?s=256&amp;
d=http%3A%2F%2Fwww.openstreetmap.org%2Fassets%2Fusers%2Fimages%2Flarge-39c3a9dc4e778
311af6b70ddcf447b58.png"/>
133          <roles>
134          </roles>
135          <changesets count="1"/>
136          <traces count="0"/>
137          <blocks>
138            <received count="0" active="0"/>
139          </blocks>
140        </user>
141      </osm>
```

```
142     """)
143
```

```
--------------------------------------------------
>> Issue: [B506:yaml_load] Use of unsafe yaml load. Allows instantiation of
arbitrary objects. Consider yaml.safe_load().
   Severity: Medium   Confidence: High
   Location: liberapay.com-master/liberapay/testing/vcr.py:39
   More Info: https://bandit.readthedocs.io/en/latest/plugins/b506_yaml_load.html
38          def deserialize(cassette_str):
39              return yaml.load(cassette_str, Loader=yaml.Loader)
40
```

```
--------------------------------------------------
>> Issue: [B608:hardcoded_sql_expressions] Possible SQL injection vector through
string-based query construction.
   Severity: Medium   Confidence: Low
   Location: liberapay.com-master/liberapay/utils/fake_data.py:35
   More Info:
https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html
34              INSERT INTO {} ({}) VALUES ({}) RETURNING {}
35          """.format(tablename, cols, placeholders, returning), vals)
36
```

```
--------------------------------------------------
>> Issue: [B303:blacklist] Use of insecure MD2, MD4, MD5, or SHA1 hash function.
   Severity: Medium   Confidence: High
   Location: liberapay.com-master/liberapay/utils/http_caching.py:58
   More Info:
https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b303-md5
57          with open(path, 'rb') as f:
58              h = b64encode_s(md5(f.read()).digest())
59          ETAGS[path] = h
```

```
--------------------------------------------------

Code scanned:
        Total lines of code: 26791
        Total lines skipped (#nosec): 0

Run metrics:
        Total issues (by severity):
                Undefined: 0
                Low: 1983
                Medium: 10
                High: 0
        Total issues (by confidence):
                Undefined: 0
                Low: 2
                Medium: 26
```

```
                High: 1965
Files skipped (19):
        liberapay.com-master/cli/run.py (syntax error while parsing AST from file)
        liberapay.com-master/liberapay/billing/payday.py (syntax error while parsing
AST from file)
        liberapay.com-master/liberapay/constants.py (syntax error while parsing AST
from file)
        liberapay.com-master/liberapay/cron.py (syntax error while parsing AST from
file)
        liberapay.com-master/liberapay/exceptions.py (syntax error while parsing AST
from file)
        liberapay.com-master/liberapay/models/__init__.py (syntax error while
parsing AST from file)
        liberapay.com-master/liberapay/models/account_elsewhere.py (syntax error
while parsing AST from file)
        liberapay.com-master/liberapay/models/participant.py (syntax error while
parsing AST from file)
        liberapay.com-master/liberapay/models/tip.py (syntax error while parsing AST
from file)
        liberapay.com-master/liberapay/payin/common.py (syntax error while parsing
AST from file)
        liberapay.com-master/liberapay/payin/cron.py (syntax error while parsing AST
from file)
        liberapay.com-master/liberapay/payin/prospect.py (syntax error while parsing
AST from file)
        liberapay.com-master/liberapay/payin/stripe.py (syntax error while parsing
AST from file)
        liberapay.com-master/liberapay/security/crypto.py (syntax error while
parsing AST from file)
        liberapay.com-master/liberapay/security/csrf.py (syntax error while parsing
AST from file)
        liberapay.com-master/liberapay/testing/__init__.py (syntax error while
parsing AST from file)
        liberapay.com-master/liberapay/utils/emails.py (syntax error while parsing
AST from file)
        liberapay.com-master/tests/py/test_schedule.py (syntax error while parsing
AST from file)
        liberapay.com-master/tests/py/test_settings.py (syntax error while parsing
AST from file)
```