Metrics:

Total lines of code: 58000
Total lines skipped (#nosec): 0

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/analytics/lib/counts.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
132             timer = time.time()
133             assert(stat.data_collector.pull_function is not None)
134             rows_added = stat.data_collector.pull_function(stat.property, start_time, end_time)
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: LOW
File: /home/groth/zulip-server-1.9.0/analytics/lib/counts.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html

```
169                 GROUP BY zerver_realm.id, %(output_table)s.subgroup
170             """ % {'output_table': output_table._meta.db_table,
171                    'property': stat.property}
172             start = time.time()
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: LOW
File: /home/groth/zulip-server-1.9.0/analytics/lib/counts.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html

```
188             GROUP BY analytics_realmcount.subgroup
189         """ % {'property': stat.property}
190         start = time.time()
```

blacklist: Standard pseudo-random generators are not suitable for security/cryptographic purposes.
Test ID: B311
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/analytics/lib/fixtures.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b311-random

```
38              for i in range(days):
39                  holidays.extend([random() < holiday_rate] * 24)
40          elif frequency == CountStat.DAY:
```

blacklist: Standard pseudo-random generators are not suitable for security/cryptographic purposes.
Test ID: B311
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/analytics/lib/fixtures.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b311-random

```
43                              [24*non_business_hours_base] * 2
44              holidays = [random() < holiday_rate for i in range(days)]
45          else:
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: LOW

File: /home/groth/zulip-server-1.9.0/analytics/tests/test_counts.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html

```
155             query = """INSERT INTO analytics_realmcount (realm_id, value, property, end_time)
156                        VALUES (%s, 1, '%s', %%%%(time_end)s)""" % (self.default_realm.id, property)
157             return CountStat(property, sql_data_collector(RealmCount, query, None), CountStat.HOUR)
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: LOW
File: /home/groth/zulip-server-1.9.0/analytics/tests/test_counts.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html

```
254             query = """INSERT INTO analytics_realmcount (realm_id, value, property, end_time)
255                        VALUES (%s, 1, '%s', %%%%(time_end)s)""" % (self.default_realm.id, 'stat3')
256             stat3 = DependentCountStat('stat3', sql_data_collector(RealmCount, query, None),
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: LOW
File: /home/groth/zulip-server-1.9.0/analytics/tests/test_counts.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html

```
288             query = """INSERT INTO analytics_realmcount (realm_id, value, property, end_time)
289                        VALUES (%s, 1, '%s', %%%%(time_end)s)""" % (self.default_realm.id, 'stat4')
290             stat4 = DependentCountStat('stat4', sql_data_collector(RealmCount, query, None),
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/analytics/views.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
165
166         assert len(set([stat.frequency for stat in stats])) == 1
167         end_times = time_range(start, end, stats[0].frequency, min_length)
```

try_except_pass: Try, Except, Pass detected.
Test ID: B110
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/analytics/views.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b110_try_except_pass.html

```
502                 row['hours_per_user'] = '%.1f' % (hours / row['dau_count'],)
503             except Exception:
504                 pass
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: LOW
File: /home/groth/zulip-server-1.9.0/analytics/views.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html

```
714                 order by string_id, up.id, client.name
715             ''' % (mobile_type,)
716
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH

File: /home/groth/zulip-server-1.9.0/scripts/lib/clean_node_cache.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
3       import os
4       import subprocess
5       import sys
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/scripts/lib/clean_node_cache.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
21          try:
22              subprocess.check_output(["/home/travis/zulip-yarn/bin/yarn", '--version'])
23          except OSError:
```

blacklist: Use of insecure MD2, MD4, MD5, or SHA1 hash function.
Test ID: B303
Severity: MEDIUM
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/scripts/lib/hash_reqs.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b303-md5

```
47          deps_str = "\n".join(deps) + "\n"
48          return hashlib.sha1(deps_str.encode('utf-8')).hexdigest()
49
```

blacklist: Use of insecure MD2, MD4, MD5, or SHA1 hash function.
Test ID: B303
Severity: MEDIUM
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/scripts/lib/node_cache.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b303-md5

```
36          YARN_LOCK_FILE_PATH = os.path.join(setup_dir, 'yarn.lock')
37          sha1sum = hashlib.sha1()
38          sha1sum.update(subprocess_text_output(['cat', PACKAGE_JSON_FILE_PATH]).encode('utf8'))
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/scripts/lib/setup_path_on_import.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b102_exec_used.html

```
16          # this file will exist in production
17          exec(open(activate_this).read(), {}, dict(__file__=activate_this))
18      sys.path.append(BASE_DIR)
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/scripts/lib/setup_venv.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
3       import shutil
4       import subprocess
5       from scripts.lib.zulip_tools import run, ENDC, WARNING, parse_lsb_release
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH

File: /home/groth/zulip-server-1.9.0/scripts/lib/setup_venv.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
234         path = os.path.join(ZULIP_PATH, 'scripts', 'lib', 'hash_reqs.py')
235         output = subprocess.check_output([path, requirements_file], universal_newlines=True)
236         sha1sum = output.split()[0]
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/scripts/lib/setup_venv.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b102_exec_used.html

```
251         activate_this = os.path.join(cached_venv_path, "bin", "activate_this.py")
252         exec(open(activate_this).read(), {}, dict(__file__=activate_this))
253         return cached_venv_path
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/scripts/lib/setup_venv.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b102_exec_used.html

```
279         activate_this = os.path.join(venv_path, "bin", "activate_this.py")
280         exec(open(activate_this).read(), {}, dict(__file__=activate_this))
281
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/scripts/lib/zulip_tools.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
11      import shutil
12      import subprocess
13      import sys
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/scripts/lib/zulip_tools.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
84          # type: (Sequence[str]) -> str
85          return subprocess.check_output(args, universal_newlines=True).strip()
86
```

start_process_with_partial_path: Starting a process with a partial executable path
Test ID: B607
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/scripts/lib/zulip_tools.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b607_start_process_with_partial_path.html

```
116                 # development environment.
117                 subprocess.check_call(["sudo", "/bin/bash", "-c",
118                                        "echo %s > %s" % (zulip_uuid, uuid_path)])
119             else:
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW

Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/scripts/lib/zulip_tools.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
116                 # development environment.
117                 subprocess.check_call(["sudo", "/bin/bash", "-c",
118                                        "echo %s > %s" % (zulip_uuid, uuid_path)])
119             else:
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/scripts/lib/zulip_tools.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
163         try:
164             subprocess.check_call(args, **kwargs)
165         except subprocess.CalledProcessError:
```

blacklist: Use of insecure MD2, MD4, MD5, or SHA1 hash function.
Test ID: B303
Severity: MEDIUM
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/scripts/lib/zulip_tools.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b303-md5

```
267         ZULIP_EMOJI_DIR = os.path.join(zulip_path, 'tools', 'setup', 'emoji')
268         sha = hashlib.sha1()
269
```

start_process_with_partial_path: Starting a process with a partial executable path
Test ID: B607
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/scripts/lib/zulip_tools.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b607_start_process_with_partial_path.html

```
302             if not dry_run:
303                 subprocess.check_call(["sudo", "rm", "-rf", directory])
304
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/scripts/lib/zulip_tools.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
302             if not dry_run:
303                 subprocess.check_call(["sudo", "rm", "-rf", directory])
304
```

blacklist: Use of insecure MD2, MD4, MD5, or SHA1 hash function.
Test ID: B303
Severity: MEDIUM
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/scripts/lib/zulip_tools.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b303-md5

```
339         # changed compared to the last execution.
340         sha1sum = hashlib.sha1()
341         for path in paths:
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404

Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/data_import/gitter.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
6       import shutil
7       import subprocess
8       import ujson
```

start_process_with_partial_path: Starting a process with a partial executable path
Test ID: B607
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/data_import/gitter.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b607_start_process_with_partial_path.html

```
274
275         subprocess.check_call(["tar", "-czf", output_dir + '.tar.gz', output_dir, '-P'])
276
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/data_import/gitter.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
274
275         subprocess.check_call(["tar", "-czf", output_dir + '.tar.gz', output_dir, '-P'])
276
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/data_import/hipchat.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
7       import shutil
8       import subprocess
9       import ujson
```

start_process_with_partial_path: Starting a process with a partial executable path
Test ID: B607
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/data_import/hipchat.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b607_start_process_with_partial_path.html

```
77
78          subprocess.check_call(['tar', '-xf', tar_file, '-C', data_dir])
79
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/data_import/hipchat.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
77
78          subprocess.check_call(['tar', '-xf', tar_file, '-C', data_dir])
79
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101

Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/data_import/hipchat.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
119                     # Hipchat sometimes doesn't export an email for deactivated users.
120                     assert not is_active
121                     email = delivery_email = "deactivated-{id}@example.com".format(id=id)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/data_import/hipchat.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
403             user_id = raw_message['receiver_id']
404             assert(user_id)
405             recipient_id = user_id_to_recipient_id[user_id]
```

start_process_with_partial_path: Starting a process with a partial executable path
Test ID: B607
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/data_import/hipchat.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b607_start_process_with_partial_path.html

```
787         logging.info('Start making tarball')
788         subprocess.check_call(["tar", "-czf", output_dir + '.tar.gz', output_dir, '-P'])
789         logging.info('Done making tarball')
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/data_import/hipchat.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
787         logging.info('Start making tarball')
788         subprocess.check_call(["tar", "-czf", output_dir + '.tar.gz', output_dir, '-P'])
789         logging.info('Done making tarball')
```

blacklist: Standard pseudo-random generators are not suitable for security/cryptographic purposes.
Test ID: B311
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/data_import/import_util.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b311-random

```
93          subscription = Subscription(
94              color=random.choice(stream_colors),
95              id=subscription_id)
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/data_import/slack.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
6       import shutil
7       import subprocess
8       import re
```

blacklist: Standard pseudo-random generators are not suitable for security/cryptographic purposes.
Test ID: B311

Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/data_import/slack.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b311-random

```
705                                     # in sync with 'exports.py' function 'import_message_data'
706             format(random.randint(0, 255), 'x'),
707             random_name(18),
```

start_process_with_partial_path: Starting a process with a partial executable path
Test ID: B607
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/data_import/slack.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b607_start_process_with_partial_path.html

```
787
788         subprocess.check_call(['unzip', '-q', slack_zip_file, '-d', slack_data_dir])
789         # with zipfile.ZipFile(slack_zip_file, 'r') as zip_ref:
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/data_import/slack.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
787
788         subprocess.check_call(['unzip', '-q', slack_zip_file, '-d', slack_data_dir])
789         # with zipfile.ZipFile(slack_zip_file, 'r') as zip_ref:
```

start_process_with_partial_path: Starting a process with a partial executable path
Test ID: B607
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/data_import/slack.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b607_start_process_with_partial_path.html

```
836         rm_tree(slack_data_dir)
837         subprocess.check_call(["tar", "-czf", output_dir + '.tar.gz', output_dir, '-P'])
838
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/data_import/slack.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
836         rm_tree(slack_data_dir)
837         subprocess.check_call(["tar", "-czf", output_dir + '.tar.gz', output_dir, '-P'])
838
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
617         property_type = Realm.property_types[name]
618         assert isinstance(value, property_type), (
619             'Cannot update %s: %s is not an instance of %s' % (
620                 name, value, property_type,))
621
622         setattr(realm, name, value)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
944             user_ids = list({recipient.type_id, sender_id})
945             assert(len(user_ids) in [1, 2])
946
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
977             message_to_user_ids = list({recipient.type_id, sender_id})
978             assert(len(message_to_user_ids) in [1, 2])
979
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
983             # of this function for different message types.
984             assert(stream_topic is not None)
985
986             subscription_rows = stream_topic.get_active_subscriptions().values(
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
1258            # Render our messages.
1259            assert message['message'].rendered_content is None
1260
1261            rendered_content = render_incoming_message(
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
1391                    message['stream'] = Stream.objects.select_related("realm").get(id=stream_id)
1392                assert message['stream'] is not None  # assert needed because stubs for django are missing
1393                if message['stream'].is_public():
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: LOW
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html

```
1537            VALUES
1538        ''' + vals
1539
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
1669        except ValidationError as e:
1670            assert isinstance(e.messages[0], str)
1671            raise JsonableError(e.messages[0])
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
1671            raise JsonableError(e.messages[0])
1672        assert recipient.type != Recipient.STREAM
1673        return {'sender': sender, 'recipient': recipient, 'op': operator}
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
1801        if not_forged_mirror_message:
1802            assert forwarder_user_profile is not None
1803            if forwarder_user_profile.id not in recipient_profile_ids:
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
2144            except ValidationError as e:
2145                assert isinstance(e.messages[0], str)
2146                raise JsonableError(e.messages[0])
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
2165        # We render messages later in the process.
2166        assert message.rendered_content is None
2167
2168        if client.name == "zephyr_mirror":
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
2252        # Verify the user is in fact a system bot
2253        assert(is_cross_realm_bot_email(sender_email) or sender_email == settings.ERROR_BOT)
```

```
2254
2255        sender = get_system_bot(sender_email)
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: LOW
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html

```
2424                zerver_subscription.recipient_id
2425            ''' % (id_list,)
2426
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
3336        notification_setting_type = UserProfile.notification_setting_types[name]
3337        assert isinstance(value, notification_setting_type), (
3338            'Cannot update %s: %s is not an instance of %s' % (
3339                name, value, notification_setting_type,))
3340
3341        setattr(user_profile, name, value)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
3363        property_type = UserProfile.property_types[setting_name]
3364        assert isinstance(setting_value, property_type)
3365        setattr(user_profile, setting_name, setting_value)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
3371        if setting_name == "default_language":
3372            assert isinstance(setting_value, str)
3373            event['language_name'] = get_language_name(setting_value)
```

django_extra_used: Use of extra potential SQL attack vector.
Test ID: B610
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b610_django_extra_used.html

```
3666            # when we drop support for the old Android app entirely.
3667            app_message_ids = UserMessage.objects.filter(
3668                user_profile=user_profile,
3669                message__id__gt=prev_pointer,
3670                message__id__lte=pointer).extra(where=[
3671                    UserMessage.where_unread(),
3672                    UserMessage.where_active_push_notification(),
3673                ]).values_list("message_id", flat=True)
```

django_extra_used: Use of extra potential SQL attack vector.
Test ID: B610
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b610_django_extra_used.html

```
3674
3675            UserMessage.objects.filter(user_profile=user_profile,
3676                                       message__id__gt=prev_pointer,
3677                                       message__id__lte=pointer).extra(where=[UserMessage.where_unread()]) \
3678                               .update(flags=F('flags').bitor(UserMessage.flags.read))
```

django_extra_used: Use of extra potential SQL attack vector.
Test ID: B610
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b610_django_extra_used.html

```
3686
3687        msgs = UserMessage.objects.filter(
3688            user_profile=user_profile
3689        ).extra(
3690            where=[UserMessage.where_unread()]
3691        )
```

django_extra_used: Use of extra potential SQL attack vector.
Test ID: B610
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b610_django_extra_used.html

```
3707
3708        all_push_message_ids = UserMessage.objects.filter(
3709            user_profile=user_profile,
3710        ).extra(
3711            where=[UserMessage.where_active_push_notification()],
3712        ).values_list("message_id", flat=True)[0:10000]
```

django_extra_used: Use of extra potential SQL attack vector.
Test ID: B610
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b610_django_extra_used.html

```
3732
3733        msgs = msgs.extra(
3734            where=[UserMessage.where_unread()]
3735        )
```

django_extra_used: Use of extra potential SQL attack vector.
Test ID: B610
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b610_django_extra_used.html

```
3757                                                message_ids: List[int]) -> None:
3758        for user_message in UserMessage.objects.filter(
3759                message_id__in=message_ids,
3760                user_profile=user_profile).extra(
3761                    where=[UserMessage.where_active_push_notification()]):
3762            event = {
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
3778
3779        assert messages is not None
3780        msgs = UserMessage.objects.filter(user_profile=user_profile,
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/actions.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
4062        message.last_edit_time = timezone_now()
4063        assert message.last_edit_time is not None  # assert needed because stubs for django are missing
4064        event['edit_timestamp'] = datetime_to_timestamp(message.last_edit_time)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/addressee.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
37          except ValidationError as e:
38              assert isinstance(e.messages[0], str)
39              raise JsonableError(e.messages[0])
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/addressee.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
56                      topic: Optional[str]=None) -> None:
57              assert(msg_type in ['stream', 'private'])
58              self._msg_type = msg_type
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/addressee.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
69          def user_profiles(self) -> List[UserProfile]:
70              assert(self.is_private())
71              return self._user_profiles  # type: ignore # assertion protects us
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/addressee.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
73          def stream_name(self) -> str:
74              assert(self.is_stream())
75              assert(self._stream_name is not None)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/addressee.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
74              assert(self.is_stream())
75              assert(self._stream_name is not None)
76              return self._stream_name
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/addressee.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
78          def topic(self) -> str:
79              assert(self.is_stream())
80              assert(self._topic is not None)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/addressee.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
79              assert(self.is_stream())
80              assert(self._topic is not None)
81              return self._topic
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
51          # {code_example|end}
52          assert result['result'] == 'success'
53          assert 'newbie@zulip.com' in result['subscribed']
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
52          assert result['result'] == 'success'
53          assert 'newbie@zulip.com' in result['subscribed']
54
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
143         members = [m for m in result['members'] if m['email'] == 'newbie@zulip.com']
144         assert len(members) == 1
145         newbie = members[0]
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
145         newbie = members[0]
146         assert not newbie['is_admin']
147         assert newbie['full_name'] == 'New User'
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
146         assert not newbie['is_admin']
147         assert newbie['full_name'] == 'New User'
148
149         # {code_example|start}
150         # You may pass the `client_gravatar` query parameter as follows:
151         result = client.get_members({'client_gravatar': True})
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
154         validate_against_openapi_schema(result, '/users', 'get', '200')
155         assert result['members'][0]['avatar_url'] is None
156
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
225         streams = [s for s in result['streams'] if s['name'] == 'new stream']
226         assert streams[0]['description'] == 'New stream for testing'
227
228         # {code_example|start}
229         # You may pass in one or more of the query parameters mentioned above
230         # as keyword arguments, like so:
231         result = client.get_streams(include_public=False)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
234         validate_against_openapi_schema(result, '/streams', 'get', '200')
235         assert len(result['streams']) == 4
236
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH

File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
247         result = client.get_subscribers(stream='new stream')
248         assert result['subscribers'] == ['iago@zulip.com', 'newbie@zulip.com']
249
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
253         result = client.get_user_agent()
254         assert result.startswith('ZulipPython/')
255
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
267         streams = [s for s in result['subscriptions'] if s['name'] == 'new stream']
268         assert streams[0]['description'] == 'New stream for testing'
269
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
284         result = client.list_subscriptions()
285         assert result['result'] == 'success'
286         streams = [s for s in result['subscriptions'] if s['name'] == 'new stream']
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
286         streams = [s for s in result['subscriptions'] if s['name'] == 'new stream']
287         assert len(streams) == 0
288
289         # {code_example|start}
290         # Unsubscribe another user from the stream "new stream"
291         result = client.remove_subscriptions(
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
429         validate_against_openapi_schema(result, '/messages', 'get', '200')
430         assert len(result['messages']) <= request['num_before']
431
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
434
435         assert int(message_id)
436
437         # {code_example|start}
438         # Get the raw content of the message with ID "message_id"
439         result = client.get_raw_message(message_id)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
467         )
468         assert result['result'] == 'success'
469         assert result['raw_content'] == request['content']
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
468         assert result['result'] == 'success'
469         assert result['raw_content'] == request['content']
470
471         # {code_example|start}
472         # Send a private message
473         request = {
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
489         )
490         assert result['result'] == 'success'
491         assert result['raw_content'] == request['content']
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
490         assert result['result'] == 'success'
491         assert result['raw_content'] == request['content']
492
493         return message_id
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH

File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
522
523         assert int(message_id)
524
525         # {code_example|start}
526         # Edit a message
527         # (make sure that message_id below is set to the ID of the
528         # message you wish to update)
529         request = {
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
544         )
545         assert result['result'] == 'success'
546         assert result['raw_content'] == request['content']
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
545         assert result['result'] == 'success'
546         assert result['raw_content'] == request['content']
547
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
823         else:
824             assert result[key] == fixture[key]
825
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
833         else:
834             assert len(result) == len(fixture)
835
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/api_test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
842         else:
843             assert key in result
844
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/avatar.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
110             return upload_backend.get_avatar_url(hash_key, medium=medium)
111         assert email is not None
112         return _get_unversioned_gravatar_url(email, medium)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/avatar.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
120         # avatar_url can return None if client_gravatar=True, however here we use the default value of False
121         assert avatar is not None
122         return urllib.parse.urljoin(user_profile.realm.uri, avatar)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/bot_lib.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
80
81              assert message['type'] == 'private'
82              # Ensure that it's a comma-separated list, even though the
83              # usual 'to' field could be either a List[str] or a str.
84              recipients = ','.join(message['to']).split(',')
```

blacklist: Using xml.etree.cElementTree to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.cElementTree with the equivalent defusedxml package, or make sure defusedxml.defuse_stdlib() is called.
Test ID: B405
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/bugdown/__init__.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b405-import-xml-etree

```
18      import ujson
19      import xml.etree.cElementTree as etree
20      from xml.etree.cElementTree import Element, SubElement
```

blacklist: Using Element to parse untrusted XML data is known to be vulnerable to XML attacks. Replace Element with the equivalent defusedxml package, or make sure defusedxml.defuse_stdlib() is called.
Test ID: B405
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/bugdown/__init__.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b405-import-xml-etree

```
19      import xml.etree.cElementTree as etree
20      from xml.etree.cElementTree import Element, SubElement
21
22      from collections import deque, defaultdict
```

blacklist: Using xml.etree.cElementTree.fromstring to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.cElementTree.fromstring with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B313
Severity: MEDIUM
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/bugdown/__init__.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b313-b320-xml-bad-celementtree

```
397         try:
398             doc = etree.fromstring(''.join(head))
399         except etree.ParseError:
```

blacklist: Using xml.etree.cElementTree.fromstring to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.cElementTree.fromstring with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B313
Severity: MEDIUM
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/bugdown/__init__.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b313-b320-xml-bad-celementtree

```
1081            if rendered is not None:
1082                return etree.fromstring(rendered.encode('utf-8'))
1083            else:  # Something went wrong while rendering
```

try_except_pass: Try, Except, Pass detected.
Test ID: B110
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/bugdown/__init__.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b110_try_except_pass.html

```
1529                del md.inlinePatterns['linebreak2']
1530            except Exception:
1531                pass
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/bugdown/__init__.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
1940        if message is not None:
1941            assert message_realm is not None  # ensured above if message is not None
1942            if possible_words is None:
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/bugdown/fenced_code.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
79      import re
80      import subprocess
81      import markdown
```

blacklist: Using Element to parse untrusted XML data is known to be vulnerable to XML attacks. Replace Element with the equivalent defusedxml package, or make sure defusedxml.defuse_stdlib() is called.
Test ID: B405
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/bugdown/nested_code_blocks.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b405-import-xml-etree

```
4       import markdown
5       from xml.etree.cElementTree import Element
6
7       from zerver.lib.bugdown import walk_tree_with_family, ResultWithFamily
```

blacklist: Use of insecure MD2, MD4, MD5, or SHA1 hash function.
Test ID: B303
Severity: MEDIUM
Confidence: HIGH

File: /home/groth/zulip-server-1.9.0/zerver/lib/cache.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b303-md5

```
101         # Memcached keys should have a length of less than 256.
102         KEY_PREFIX = hashlib.sha1(KEY_PREFIX.encode('utf-8')).hexdigest()
103
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/lib/debug.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b108_hardcoded_tmp_directory.html

```
81          sock = socket.socket(socket.AF_UNIX, socket.SOCK_DGRAM)
82          path = "/tmp/tracemalloc.{}".format(os.getpid())
83          sock.bind(path)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/email_mirror.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
161         if recipient.type == Recipient.STREAM:
162             assert isinstance(display_recipient, str)
163             recipient_str = display_recipient
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/email_mirror.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
166         elif recipient.type == Recipient.PERSONAL:
167             assert not isinstance(display_recipient, str)
168             recipient_str = display_recipient[0]['email']
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/email_mirror.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
172         elif recipient.type == Recipient.HUDDLE:
173             assert not isinstance(display_recipient, str)
174             emails = [user_dict['email'] for user_dict in display_recipient]
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/email_mirror.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
211                 content = part.get_payload(decode=True)
212                 assert isinstance(content, bytes)
213                 if charsets[idx]:
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH

File: /home/groth/zulip-server-1.9.0/zerver/lib/events.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
619         elif event['type'] == "update_display_settings":
620             assert event['setting_name'] in UserProfile.property_types
621             state[event['setting_name']] = event['setting']
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/events.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
622         elif event['type'] == "update_global_notifications":
623             assert event['notification_name'] in UserProfile.notification_setting_types
624             state[event['notification_name']] = event['setting']
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
13      import ujson
14      import subprocess
15      import tempfile
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
246         # expertise on this export system.
247         assert ALL_ZULIP_TABLES == all_tables_db
248         assert NON_EXPORTED_TABLES.issubset(ALL_ZULIP_TABLES)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
247         assert ALL_ZULIP_TABLES == all_tables_db
248         assert NON_EXPORTED_TABLES.issubset(ALL_ZULIP_TABLES)
249         assert IMPLICIT_TABLES.issubset(ALL_ZULIP_TABLES)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
248         assert NON_EXPORTED_TABLES.issubset(ALL_ZULIP_TABLES)
249         assert IMPLICIT_TABLES.issubset(ALL_ZULIP_TABLES)
250         assert ATTACHMENT_TABLES.issubset(ALL_ZULIP_TABLES)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH

File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
249         assert IMPLICIT_TABLES.issubset(ALL_ZULIP_TABLES)
250         assert ATTACHMENT_TABLES.issubset(ALL_ZULIP_TABLES)
251
252         tables = set(ALL_ZULIP_TABLES)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
331                     exclude: Optional[List[Field]]=None) -> None:
332             assert table or custom_tables
333             self.table = table
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
434                 logging.info('Deleted temporary %s' % (t,))
435             assert table is not None
436             response[table] = data
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
438         elif config.use_all:
439             assert model is not None
440             query = model.objects.all()
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
448             model = config.model
449             assert parent is not None
450             assert parent.table is not None
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
449             assert parent is not None
450             assert parent.table is not None
451             assert config.parent_key is not None
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW

Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
450             assert parent.table is not None
451             assert config.parent_key is not None
452             parent_ids = [r['id'] for r in response[parent.table]]
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
455                 filter_parms.update(config.filter_args)
456             assert model is not None
457             query = model.objects.filter(**filter_parms)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
464             model = config.model
465             assert model is not None
466             # This will be a tuple of the form ('zerver_article', 'blog').
467             (child_table, field) = config.id_source
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
479         if rows is not None:
480             assert table is not None  # Hint for mypy
481             response[table] = make_raw(rows, exclude=config.exclude)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
771                 if row['id'] in exportable_user_ids:
772                     assert not row['is_mirror_dummy']
773                 else:
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
839         realm = context['realm']
840         assert config.parent is not None
841         assert config.parent.table is not None
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101

Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
840         assert config.parent is not None
841         assert config.parent.table is not None
842         user_profile_ids = set(r['id'] for r in response[config.parent.table])
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
998             message_ids = set(m['id'] for m in message_chunk)
999             assert len(message_ids.intersection(all_message_ids)) == 0
1000
1001            all_message_ids.update(message_ids)
```

start_process_with_partial_path: Starting a process with a partial executable path
Test ID: B607
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b607_start_process_with_partial_path.html

```
1161            os.makedirs(os.path.dirname(output_path), exist_ok=True)
1162            subprocess.check_call(["cp", "-a", local_path, output_path])
1163            stat = os.stat(local_path)
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
1161            os.makedirs(os.path.dirname(output_path), exist_ok=True)
1162            subprocess.check_call(["cp", "-a", local_path, output_path])
1163            stat = os.stat(local_path)
```

start_process_with_partial_path: Starting a process with a partial executable path
Test ID: B607
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b607_start_process_with_partial_path.html

```
1204                os.makedirs(str(os.path.dirname(output_path)), exist_ok=True)
1205                subprocess.check_call(["cp", "-a", str(local_path), str(output_path)])
1206                stat = os.stat(local_path)
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
1204                os.makedirs(str(os.path.dirname(output_path)), exist_ok=True)
1205                subprocess.check_call(["cp", "-a", str(local_path), str(output_path)])
1206                stat = os.stat(local_path)
```

start_process_with_partial_path: Starting a process with a partial executable path
Test ID: B607
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b607_start_process_with_partial_path.html

```
1236            os.makedirs(os.path.dirname(output_path), exist_ok=True)
1237            subprocess.check_call(["cp", "-a", local_path, output_path])
1238            record = dict(realm_id=realm.id,
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
1236            os.makedirs(os.path.dirname(output_path), exist_ok=True)
1237            subprocess.check_call(["cp", "-a", local_path, output_path])
1238            record = dict(realm_id=realm.id,
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
1287        if not settings.TEST_SUITE:
1288            assert threads >= 1
1289
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
1289
1290        assert os.path.exists("./manage.py")
1291
1292        realm_config = get_realm_config()
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b108_hardcoded_tmp_directory.html

```
1346        is_done = not in_progress
1347        in_progress_link = '/tmp/zulip-export-in-progress'
1348        done_link = '/tmp/zulip-export-most-recent'
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b108_hardcoded_tmp_directory.html

```
1347        in_progress_link = '/tmp/zulip-export-in-progress'
1348        done_link = '/tmp/zulip-export-most-recent'
1349
1350        if in_progress:
```

start_process_with_partial_path: Starting a process with a partial executable path
Test ID: B607
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b607_start_process_with_partial_path.html

```
1352        else:
1353            subprocess.check_call(['rm', '-f', in_progress_link])
1354            new_target = done_link
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
1352        else:
1353            subprocess.check_call(['rm', '-f', in_progress_link])
1354            new_target = done_link
```

start_process_with_partial_path: Starting a process with a partial executable path
Test ID: B607
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b607_start_process_with_partial_path.html

```
1355
1356        subprocess.check_call(["ln", "-nsf", source, new_target])
1357        if is_done:
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
1355
1356        subprocess.check_call(["ln", "-nsf", source, new_target])
1357        if is_done:
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
1364        def run_job(shard: str) -> int:
1365            subprocess.call(["./manage.py", 'export_usermessage_batch', '--path',
1366                             str(output_dir), '--thread', shard])
1367            return 0
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/lib/feedback.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b108_hardcoded_tmp_directory.html

```
27      def get_ticket_number() -> int:
28          num_file = '/var/tmp/.feedback-bot-ticket-number'
29          try:
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: LOW
File: /home/groth/zulip-server-1.9.0/zerver/lib/fix_unreads.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html

```
56              WHERE id IN (%s)
57          ''' % (um_id_list,)
58
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: LOW
File: /home/groth/zulip-server-1.9.0/zerver/lib/fix_unreads.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html

```
120                 )
121             ''' % (user_profile.id, recips)
122
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: LOW
File: /home/groth/zulip-server-1.9.0/zerver/lib/fix_unreads.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html

```
209                 )
210             ''' % (user_profile.id, pointer, recips)
211
```

blacklist: Standard pseudo-random generators are not suitable for security/cryptographic purposes.
Test ID: B311
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/generate_test_data.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b311-random

```
115         vals = text.split()
116         start = random.randrange(len(vals))
117         end = random.randrange(len(vals) - start) + start
```

blacklist: Standard pseudo-random generators are not suitable for security/cryptographic purposes.
Test ID: B311
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/generate_test_data.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b311-random

```
116         start = random.randrange(len(vals))
117         end = random.randrange(len(vals) - start) + start
118         vals[start] = mode + vals[start]
```

blacklist: Standard pseudo-random generators are not suitable for security/cryptographic purposes.
Test ID: B311
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/generate_test_data.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b311-random

```
125         vals = text.split()
126         start = random.randrange(len(vals))
127
```

blacklist: Standard pseudo-random generators are not suitable for security/cryptographic purposes.
Test ID: B311
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/generate_test_data.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b311-random

```
133         vals = text.split()
134         start = random.randrange(len(vals))
135
```

blacklist: Using lxml to parse untrusted XML data is known to be vulnerable to XML attacks. Replace lxml with the equivalent defusedxml package.
Test ID: B410
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/html_diff.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b410-import-lxml

```
1       import lxml
2
3       from lxml.html.diff import htmldiff
4       from typing import Optional
```

blacklist: Using htmldiff to parse untrusted XML data is known to be vulnerable to XML attacks. Replace htmldiff with the equivalent defusedxml package.
Test ID: B410
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/html_diff.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b410-import-lxml

```
2
3       from lxml.html.diff import htmldiff
4       from typing import Optional
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/i18n.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
42          seconds = list(range(firsts_end, lang_len))
43          assert len(firsts) + len(seconds) == lang_len
44          for row in zip_longest(firsts, seconds):
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/lib/import_realm.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html

```
257         sequence = idseq(model_class)
258         conn.execute("select nextval('%s') from generate_series(1,%s)" %
259                      (sequence, str(count)))
260         query = conn.fetchall()  # Each element in the result is a tuple like (5,)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/import_realm.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
292         # See comments in bulk_import_user_message_data.
293         assert('usermessage' not in related_table)
294
295         re_map_foreign_keys_internal(data[table], table, field_name, related_table, verbose, id_field,
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/import_realm.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
423         # memory errors. We don't even use ids from ID_MAP.
424         assert('usermessage' not in table)
425
426         old_id_list = current_table_ids(data, table)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/import_realm.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
1042            for row in data['zerver_usermessage']:
1043                assert(row['message'] in message_id_map)
1044
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/integrations.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
248         def __init__(self, name: str, *args: Any, **kwargs: Any) -> None:
249             assert kwargs.get("client_name") is None
250             client_name = self.DEFAULT_CLIENT_NAME.format(name=name.title())
```

blacklist: Use of insecure MD2, MD4, MD5, or SHA1 hash function.
Test ID: B303
Severity: MEDIUM
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/logging_util.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b303-md5

```
40                          tb = str(record)
41                      key = self.__class__.__name__.upper() + hashlib.sha1(tb.encode()).hexdigest()
42                      duplicate = cache.get(key) == 1
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/mdiff.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
1       import os
2       import subprocess
3       import logging
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH

File: /home/groth/zulip-server-1.9.0/zerver/lib/mdiff.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
17          command = ['node', mdiff_path, output, expected_output]
18          diff = subprocess.check_output(command).decode('utf-8')
19          return diff
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/message.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
336                 obj['last_edit_timestamp'] = datetime_to_timestamp(last_edit_time)
337                 assert edit_history is not None
338                 obj['edit_history'] = ujson.loads(edit_history)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/message.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
353
354                 assert message is not None  # Hint for mypy.
355                 # It's unfortunate that we need to have side effects on the message
356                 # in some cases.
357                 rendered_content = save_message_rendered_content(message, content)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/message.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
435             elif recipient_type in (Recipient.HUDDLE, Recipient.PERSONAL):
436                 assert not isinstance(display_recipient, str)
437                 display_type = "private"
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/message.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
616         # str is for streams.
617         assert not isinstance(display_recipient, str)
618
619         user_ids = [obj['id'] for obj in display_recipient]  # type: List[int]
```

django_extra_used: Use of extra potential SQL attack vector.
Test ID: B610
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/lib/message.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b610_django_extra_used.html

```
708     def get_starred_message_ids(user_profile: UserProfile) -> List[int]:
709         return list(UserMessage.objects.filter(
710             user_profile=user_profile,
711         ).extra(
712             where=[UserMessage.where_starred()]
713         ).order_by(
```

django_extra_used: Use of extra potential SQL attack vector.
Test ID: B610
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/lib/message.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b610_django_extra_used.html

```
720
721         user_msgs = UserMessage.objects.filter(
722             user_profile=user_profile
723         ).exclude(
724             message__recipient_id__in=excluded_recipient_ids
725         ).extra(
726             where=[UserMessage.where_unread()]
727         ).values(
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/message.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
932             # We have verified that the limit is not none before calling this function.
933             assert realm.message_visibility_limit is not None
934             first_visible_message_id = Message.objects.filter(sender__realm=realm).values('id').\
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: LOW
File: /home/groth/zulip-server-1.9.0/zerver/lib/migrate.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html

```
29              END$$;
30              ''' % (index_name, index_name, table_name, column_string, where_clause)
31          return stmt
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: LOW
File: /home/groth/zulip-server-1.9.0/zerver/lib/migrate.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html

```
44              WHERE id >= %%s AND id < %%s
45          ''' % (table, ', '.join(cols), ', '.join(['%s'] * len(cols)))
46
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/lib/migrate.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html

```
46
47          cursor.execute("SELECT MIN(id), MAX(id) FROM %s" % (table,))
48          (min_id, max_id) = cursor.fetchall()[0]
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/lib/migrate.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html

```
67              if min_id > max_id:
68                  cursor.execute("SELECT MAX(id) FROM %s" % (table,))
69                  max_id = cursor.fetchall()[0][0]
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/mobile_auth_otp.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
16          the bitwise xor of the two hex strings."""
17          assert len(bytes_a) == len(bytes_b)
18          return ''.join(["%x" % (int(x, 16) ^ int(y, 16))
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/mobile_auth_otp.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
29      def otp_encrypt_api_key(api_key: str, otp: str) -> str:
30          assert len(otp) == UserProfile.API_KEY_LENGTH * 2
31          hex_encoded_api_key = ascii_to_hex(api_key)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/mobile_auth_otp.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
31          hex_encoded_api_key = ascii_to_hex(api_key)
32          assert len(hex_encoded_api_key) == UserProfile.API_KEY_LENGTH * 2
33          return xor_hex_strings(hex_encoded_api_key, otp)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/mobile_auth_otp.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
35      def otp_decrypt_api_key(otp_encrypted_api_key: str, otp: str) -> str:
36          assert len(otp) == UserProfile.API_KEY_LENGTH * 2
37          assert len(otp_encrypted_api_key) == UserProfile.API_KEY_LENGTH * 2
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/mobile_auth_otp.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
36          assert len(otp) == UserProfile.API_KEY_LENGTH * 2
37          assert len(otp_encrypted_api_key) == UserProfile.API_KEY_LENGTH * 2
38          hex_encoded_api_key = xor_hex_strings(otp_encrypted_api_key, otp)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/mobile_auth_otp.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
42          try:
43              assert len(otp) == UserProfile.API_KEY_LENGTH * 2
44              [int(c, 16) for c in otp]
```

blacklist: Using CSSSelector to parse untrusted XML data is known to be vulnerable to XML attacks. Replace CSSSelector with the equivalent defusedxml package.
Test ID: B410
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/notifications.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b410-import-lxml

```
31      from email.utils import formataddr
32      from lxml.cssselect import CSSSelector
33      import lxml.html
```

blacklist: Using lxml.html to parse untrusted XML data is known to be vulnerable to XML attacks. Replace lxml.html with the equivalent defusedxml package.
Test ID: B410
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/notifications.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b410-import-lxml

```
32      from lxml.cssselect import CSSSelector
33      import lxml.html
34      import re
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/notifications.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
34      import re
35      import subprocess
36      import ujson
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/notifications.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
101             # we assert that it does not.
102             assert match is not None
103             emoji_code = match.group('emoji_code')
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/notifications.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
164
165             assert message.rendered_content is not None
166             html = message.rendered_content
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH

File: /home/groth/zulip-server-1.9.0/zerver/lib/notifications.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
183                 disp_recipient = get_display_recipient(message.recipient)
184                 assert not isinstance(disp_recipient, str)
185                 other_recipients = [r['full_name'] for r in disp_recipient
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/notifications.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
321             # Make sure that this is a list of strings, not a string.
322             assert not isinstance(display_recipient, str)
323             other_recipients = [r['full_name'] for r in display_recipient
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/notifications.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
531                 # A body width of 0 means do not try to wrap the text for us.
532                 p = subprocess.Popen(
533                     [command, "--body-width=0"], stdout=subprocess.PIPE,
534                     stdin=subprocess.PIPE, stderr=subprocess.STDOUT)
535                 break
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/openapi.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
53                  self.reload()
54              assert(self.data)
55              return self.data
```

blacklist: Using lxml.html to parse untrusted XML data is known to be vulnerable to XML attacks. Replace lxml.html with the equivalent defusedxml package.
Test ID: B410
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/push_notifications.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b410-import-lxml

```
6       import logging
7       import lxml.html as LH
8       import os
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/send_email.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
40          # Callers should pass exactly one of to_user_id and to_email.
41          assert (to_user_id is None) ^ (to_email is None)
42          if to_user_id is not None:
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/send_email.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
121
122         assert (to_user_id is None) ^ (to_email is None)
123         if to_user_id is not None:
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/send_email.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
125             # expresses that fact
126             assert(UserProfile.objects.filter(id=to_user_id, realm=realm).exists())
127             to_field = {'user_id': to_user_id}  # type: Dict[str, Any]
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/soft_deactivation.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
99          """
100         assert user_profile.last_active_message_id is not None
101         all_stream_subs = list(Subscription.objects.select_related('recipient').filter(
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/soft_deactivation.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
123             if stream_subscription_logs[-1].event_type == RealmAuditLog.SUBSCRIPTION_DEACTIVATED:
124                 assert stream_subscription_logs[-1].event_last_message_id is not None
125                 if stream_subscription_logs[-1].event_last_message_id <= user_profile.last_active_message_id:
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: LOW
File: /home/groth/zulip-server-1.9.0/zerver/lib/stream_recipient.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html

```
46                      zerver_stream.id in (%s)
47                  ''' % (Recipient.STREAM, id_list)
48              self._process_query(query)
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: LOW
File: /home/groth/zulip-server-1.9.0/zerver/lib/stream_recipient.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html

```
72                      zerver_recipient.id in (%s)
73                  ''' % (Recipient.STREAM, id_list)
74
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/streams.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
18          # all callers should have the require_realm_admin decorator.
19          assert(user_profile.is_realm_admin)
20
21          error = _("Invalid stream id")
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/streams.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
219             # caller, but it makes sense to verify anyway.
220             assert stream_name == stream_name.strip()
221             check_stream_name(stream_name)
```

hardcoded_password_funcarg: Possible hardcoded password: '[a-z0-9_]{24}'
Test ID: B106
Severity: LOW
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/lib/test_classes.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b106_hardcoded_password_funcarg.html

```
111         DEFAULT_REALM = Realm.objects.get(string_id='zulip')
112         TOKENIZED_NOREPLY_REGEX = settings.TOKENIZED_NOREPLY_EMAIL_ADDRESS.format(token="[a-z0-9_]{24}")
113
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/test_classes.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
439
440             assert(len(to_emails) >= 2)
441
442             (sending_client, _) = Client.objects.get_or_create(name="test suite")
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/test_classes.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
771         def setUp(self) -> None:
772             assert self.migrate_from and self.migrate_to, \
773                 "TestCase '{}' must define migrate_from and migrate_to properties".format(type(self).__name__)
774             migrate_from = [(self.app, self.migrate_from)]  # type: List[Tuple[str, str]]
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/test_fixtures.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
5       import hashlib
6       import subprocess
```

```
7       import sys
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/test_fixtures.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
53              run_db_migrations('test')
54          subprocess.check_call(generate_fixtures_command)
55
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/lib/test_fixtures.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b608_hardcoded_sql_expressions.html

```
61              with connection.cursor() as cursor:
62                  cursor.execute("SELECT 1 from pg_database WHERE datname='{}';".format(database_name))
63                  return_value = bool(cursor.fetchone())
```

blacklist: Use of insecure MD2, MD4, MD5, or SHA1 hash function.
Test ID: B303
Severity: MEDIUM
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/test_fixtures.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b303-md5

```
130         """
131         target_hash_content = hashlib.sha1(target_content.encode('utf8')).hexdigest()
132
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
374
375             assert len(pattern_cnt) > 100
376             untested_patterns = set([p for p in pattern_cnt if pattern_cnt[p] == 0])
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/test_helpers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
451     def load_subdomain_token(response: HttpResponse) -> Dict[str, Any]:
452         assert isinstance(response, HttpResponseRedirect)
453         token = response.url.rsplit('/', 1)[1]
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/test_runner.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
28      import os
29      import subprocess
```

```
30      import sys
```

blacklist: Standard pseudo-random generators are not suitable for security/cryptographic purposes.
Test ID: B311
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/test_runner.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b311-random

```
378             template_rendered.connect(self.on_template_rendered)
379             self.database_id = random.randint(1, 10000)
380
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/tex.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
3       import os
4       import subprocess
5       from django.conf import settings
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/tex.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
28              command.extend(['--', '--display-mode'])
29          katex = subprocess.Popen(command,
30                                   stdin=subprocess.PIPE,
31                                   stdout=subprocess.PIPE,
32                                   stderr=subprocess.PIPE)
33          stdout = katex.communicate(input=tex.encode())[0]
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/tex.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
35              # stdout contains a newline at the end
36              assert stdout is not None
37              return stdout.decode('utf-8').strip()
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/timeout.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
54                  # Attempt to raise a TimeoutExpired in the thread represented by 'self'.
55                  assert self.ident is not None  # Thread should be running; c_long expects int
56                  tid = ctypes.c_long(self.ident)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/timeout.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
88              six.reraise(thread.exc_info[0], thread.exc_info[1], thread.exc_info[2])
89          assert thread.result is not None  # assured if above did not reraise
90          return thread.result
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/upload.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
249         uploaded_file_name = user_file.name
250         assert isinstance(uploaded_file_name, str)
251
252         content_type = request.GET.get('mimetype')
```

blacklist: Standard pseudo-random generators are not suitable for security/cryptographic purposes.
Test ID: B311
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/upload.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b311-random

```
515                 str(user_profile.realm_id),
516                 format(random.randint(0, 255), 'x'),
517                 random_name(18),
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/user_agent.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
8           match = re.match("^(?P<name>[^/ ]*[^0-9/(]*)(/(?P<version>[^/ ]*))?([ /].*)?$", user_agent)
9           assert match is not None
10          return match.groupdict()
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/users.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
93          if base_query is None:
94              assert realm is not None
95              query = UserProfile.objects.filter(realm=realm, is_active=True)
```

django_extra_used: Use of extra potential SQL attack vector.
Test ID: B610
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/lib/users.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b610_django_extra_used.html

```
119             where_clause = "UPPER(zerver_userprofile.email::text) IN (%s)" % (upper_list,)
120             return query.select_related("realm").extra(
121                 where=[where_clause],
122                 params=emails)
123
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH

File: /home/groth/zulip-server-1.9.0/zerver/lib/utils.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
143
144         assert db_chunk_size >= 2
145         assert chunk_size >= 2
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/utils.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
144         assert db_chunk_size >= 2
145         assert chunk_size >= 2
146
147         if id_collector is not None:
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/utils.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
147         if id_collector is not None:
148             assert(len(id_collector) == 0)
149         else:
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/utils.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
155             while True:
156                 assert db_chunk_size is not None  # Hint for mypy, but also workaround for mypy bug #3442.
157                 rows = list(q.filter(id__gt=min_id)[0:db_chunk_size])
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/utils.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
173             tup_ids = set([tup[0] for tup in tup_chunk])
174             assert len(tup_ids) == len(tup_chunk)
175             assert len(tup_ids.intersection(id_collector)) == 0
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/utils.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
174             assert len(tup_ids) == len(tup_chunk)
175             assert len(tup_ids.intersection(id_collector)) == 0
176             id_collector.update(tup_ids)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW

Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/lib/webhooks/common.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
60          if stream is None:
61              assert user_profile.bot_owner is not None
62              check_send_private_message(user_profile, request.client,
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/logging_handlers.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
5       import os
6       import subprocess
7       import traceback
```

start_process_with_partial_path: Starting a process with a partial executable path
Test ID: B607
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/logging_handlers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b607_start_process_with_partial_path.html

```
21          try:  # nocoverage
22              return subprocess.check_output(
23                  ['git',
24                   '--git-dir', os.path.join(os.path.dirname(__file__), '../.git'),
25                   'describe', '--tags', '--always', '--dirty', '--long'],
26                  stderr=subprocess.PIPE,
27              ).strip().decode('utf-8')
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/logging_handlers.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
21          try:  # nocoverage
22              return subprocess.check_output(
23                  ['git',
24                   '--git-dir', os.path.join(os.path.dirname(__file__), '../.git'),
25                   'describe', '--tags', '--always', '--dirty', '--long'],
26                  stderr=subprocess.PIPE,
27              ).strip().decode('utf-8')
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/add_users_to_streams.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
24              realm = self.get_realm(options)
25              assert realm is not None  # Should be ensured by parser
26
27              user_profiles = self.get_users(options, realm)
```

blacklist: Consider possible security implications associated with CalledProcessError module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/compilemessages.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
6       import ujson
7       from subprocess import CalledProcessError, check_output
8       from typing import Any, Dict, List
```

start_process_with_partial_path: Starting a process with a partial executable path
Test ID: B607
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/compilemessages.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b607_start_process_with_partial_path.html

```
82          def get_locales(self) -> List[str]:
83              tracked_files = check_output(['git', 'ls-files', 'static/locale'])
84              tracked_files = tracked_files.decode().split()
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/compilemessages.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
82          def get_locales(self) -> List[str]:
83              tracked_files = check_output(['git', 'ls-files', 'static/locale'])
84              tracked_files = tracked_files.decode().split()
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/convert_gitter_data.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
3       import os
4       import subprocess
5       import tempfile
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/convert_gitter_data.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b108_hardcoded_tmp_directory.html

```
35              if output_dir is None:
36                  output_dir = tempfile.mkdtemp(prefix="/tmp/converted-gitter-data-")
37              else:
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/convert_hipchat_data.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
2       import os
3       import subprocess
4       import tempfile
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/convert_slack_data.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
3       import os
4       import subprocess
5       import tempfile
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/convert_slack_data.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b108_hardcoded_tmp_directory.html

```
38              if output_dir is None:
39                  output_dir = tempfile.mkdtemp(prefix="/tmp/converted-slack-data-")
40              else:
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/create_default_stream_groups.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
43              realm = self.get_realm(options)
44              assert realm is not None  # Should be ensured by parser
45
46              streams = []
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/create_stream.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
22              realm = self.get_realm(options)
23              assert realm is not None  # Should be ensured by parser
24
25              encoding = sys.getfilesystemencoding()
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/create_user.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
56              realm = self.get_realm(options)
57              assert realm is not None  # Should be ensured by parser
58
59              try:
```

blacklist: The input method in Python 2 will read from standard input, evaluate and run the resulting string as python source code. This is similar, though in many ways worse, then using eval. On Python 2, use raw_input instead, input is safe in Python 3.
Test ID: B322
Severity: HIGH
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/create_user.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b322-input

```
71                      while True:
72                          email = input("Email: ")
73                          try:
```

blacklist: The input method in Python 2 will read from standard input, evaluate and run the resulting string as python source code. This is similar, though in many ways worse, then using eval. On Python 2, use raw_input instead, input is safe in Python 3.
Test ID: B322

Severity: HIGH
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/create_user.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b322-input

```
77                              print("Invalid email address.", file=sys.stderr)
78                      full_name = input("Full name: ")
79
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/deactivate_realm.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
15              realm = self.get_realm(options)
16              assert realm is not None  # Should be ensured by parser
17
18              if realm.deactivated:
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/deliver_email.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b108_hardcoded_tmp_directory.html

```
44
45              with lockfile("/tmp/zulip_email_deliver.lockfile"):
46                  while True:
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/deliver_scheduled_messages.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b108_hardcoded_tmp_directory.html

```
60
61              with lockfile("/tmp/zulip_scheduled_message_deliverer.lockfile"):
62                  while True:
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/export.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
3       import shutil
4       import subprocess
5       import tempfile
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
103             realm = self.get_realm(options)
104             assert realm is not None  # Should be ensured by parser
105
106             output_dir = options["output_dir"]
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b108_hardcoded_tmp_directory.html

```
107             if output_dir is None:
108                 output_dir = tempfile.mkdtemp(prefix="/tmp/zulip-export-")
109             else:
```

start_process_with_partial_path: Starting a process with a partial executable path
Test ID: B607
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b607_start_process_with_partial_path.html

```
125             os.chdir(os.path.dirname(output_dir))
126             subprocess.check_call(["tar", "-czf", tarball_path, os.path.basename(output_dir)])
127             print("Tarball written to %s" % (tarball_path,))
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/export.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
125             os.chdir(os.path.dirname(output_dir))
126             subprocess.check_call(["tar", "-czf", tarball_path, os.path.basename(output_dir)])
127             print("Tarball written to %s" % (tarball_path,))
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/export_single_user.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
3       import shutil
4       import subprocess
5       import tempfile
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/export_single_user.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b108_hardcoded_tmp_directory.html

```
36              if output_dir is None:
37                  output_dir = tempfile.mkdtemp(prefix="/tmp/zulip-export-")
38              if os.path.exists(output_dir):
```

start_process_with_partial_path: Starting a process with a partial executable path
Test ID: B607
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/export_single_user.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b607_start_process_with_partial_path.html

```
44              tarball_path = output_dir.rstrip('/') + '.tar.gz'
45              subprocess.check_call(["tar", "--strip-components=1", "-czf", tarball_path, output_dir])
46              print("Tarball written to %s" % (tarball_path,))
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/export_single_user.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
44              tarball_path = output_dir.rstrip('/') + '.tar.gz'
45              subprocess.check_call(["tar", "--strip-components=1", "-czf", tarball_path, output_dir])
46              print("Tarball written to %s" % (tarball_path,))
```

try_except_continue: Try, Except, Continue detected.
Test ID: B112
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/export_usermessage_batch.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b112_try_except_continue.html

```
35                      shutil.move(partial_path, locked_path)
36                  except Exception:
37                      # Already claimed by another process
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/generate_invite_links.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
27              realm = self.get_realm(options)
28              assert realm is not None  # Should be ensured by parser
29
30              if not options['emails']:
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/generate_multiuse_invite_link.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
31              realm = self.get_realm(options)
32              assert realm is not None  # Should be ensured by parser
33
34              streams = []  # type: List[Stream]
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/import.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
3       import os
4       import subprocess
5       import tarfile
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/import.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
43              call_command('flush', verbosity=0, interactive=False)
44              subprocess.check_call([os.path.join(settings.DEPLOY_ROOT, "scripts/setup/flush-memcached")])
45
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/merge_streams.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
32              realm = self.get_realm(options)
33              assert realm is not None  # Should be ensured by parser
34              stream_to_keep = get_stream(options["stream_to_keep"], realm)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/process_queue.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
58                      td.start()
59                  assert len(queues) == cnt
60                  logger.info('%d queue worker threads were launched' % (cnt,))
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/reactivate_realm.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
15              realm = self.get_realm(options)
16              assert realm is not None  # Should be ensured by parser
17              if not realm.deactivated:
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/realm_domain.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
32              realm = self.get_realm(options)
33              assert realm is not None  # Should be ensured by parser
34              if options["op"] == "show":
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/realm_filters.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
38              realm = self.get_realm(options)
39              assert realm is not None  # Should be ensured by parser
40              if options["op"] == "show":
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/register_server.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
4       import requests
5       import subprocess
6       from typing import Any
```

start_process_with_partial_path: Starting a process with a partial executable path
Test ID: B607
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/register_server.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b607_start_process_with_partial_path.html

```
88                      print("Success! Updating %s with the new key..." % (SECRETS_FILENAME,))
89                      subprocess.check_call(["crudini", '--set', SECRETS_FILENAME, "secrets", "zulip_org_key",
90                                            request["new_org_key"]])
91                  print("Mobile Push Notification Service registration successfully updated!")
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/register_server.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
88                      print("Success! Updating %s with the new key..." % (SECRETS_FILENAME,))
89                      subprocess.check_call(["crudini", '--set', SECRETS_FILENAME, "secrets", "zulip_org_key",
90                                            request["new_org_key"]])
91                  print("Mobile Push Notification Service registration successfully updated!")
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/remove_users_from_stream.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
24              realm = self.get_realm(options)
25              assert realm is not None  # Should be ensured by parser
26              user_profiles = self.get_users(options, realm)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/rename_stream.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
22              realm = self.get_realm(options)
23              assert realm is not None  # Should be ensured by parser
24              old_name = options['old_name']
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/scrub_realm.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
15              realm = self.get_realm(options)
16              assert realm is not None  # Should be ensured by parser
17              if not realm.deactivated:
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/set_default_streams.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
43              realm = self.get_realm(options)
44              assert realm is not None  # Should be ensured by parser
```

```
45
46              stream_dict = {
```

django_extra_used: Use of extra potential SQL attack vector.
Test ID: B610
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/management/commands/show_unreads.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b610_django_extra_used.html

```
11      def get_unread_messages(user_profile: UserProfile) -> List[Dict[str, Any]]:
12          user_msgs = UserMessage.objects.filter(
13              user_profile=user_profile,
14              message__recipient__type=Recipient.STREAM
15          ).extra(
16              where=[UserMessage.where_unread()]
17          ).values(
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/middleware.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
99                          error_content_iter: Optional[Iterable[AnyStr]]=None) -> None:
100         assert error_content is None or error_content_iter is None
101         if error_content is not None:
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/middleware.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b108_hardcoded_tmp_directory.html

```
208             log_data["prof"].disable()
209             profile_path = "/tmp/profile.data.%s.%s" % (path.split("/")[-1], int(time_delta * 1000),)
210             log_data["prof"].dump_stats(profile_path)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/middleware.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
213         if 400 <= status_code < 500 and status_code not in [401, 404, 405]:
214             assert error_content_iter is not None
215             error_content_list = list(error_content_iter)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/models.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
71          '''
72          assert(user_ids)
73          value_list = ', '.join(str(int(user_id)) for user_id in user_ids)
```

django_extra_used: Use of extra potential SQL attack vector.
Test ID: B610
Severity: MEDIUM
Confidence: MEDIUM

File: /home/groth/zulip-server-1.9.0/zerver/models.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b610_django_extra_used.html

```
74          clause = '%s in (%s)' % (field, value_list)
75          query = query.extra(
76              where=[clause]
77          )
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/models.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
118         if recipient_type == Recipient.STREAM:
119             assert recipient_type_id is not None
120             stream = Stream.objects.get(id=recipient_type_id)
```

django_extra_used: Use of extra potential SQL attack vector.
Test ID: B610
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/models.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b610_django_extra_used.html

```
1239            where_clause = "UPPER(zerver_stream.name::text) IN (%s)" % (upper_list,)
1240            return get_active_streams(realm.id).select_related("realm").extra(
1241                where=[where_clause],
1242                params=stream_names)
1243
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/models.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
1271    def get_huddle_user_ids(recipient: Recipient) -> List[int]:
1272        assert(recipient.type == Recipient.HUDDLE)
1273
1274        return Subscription.objects.filter(
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/models.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
1782            return get_system_bot(email)
1783        assert realm is not None
1784        return get_user(email, realm)
```

django_mark_safe: Potential XSS on mark_safe function.
Test ID: B703
Severity: MEDIUM
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/templatetags/app_filters.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b703_django_mark_safe.html

```
158
159         return mark_safe(rendered_html)
```

blacklist: Use of mark_safe() may expose cross-site scripting vulnerabilities and should be reviewed.
Test ID: B308
Severity: MEDIUM
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/templatetags/app_filters.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b308-mark-safe

```
158
159         return mark_safe(rendered_html)
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/tornado/autoreload.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
63      import types
64      import subprocess
65      import weakref
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/tornado/autoreload.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
215         if not _has_execv:
216             subprocess.Popen([sys.executable] + sys.argv)
217             sys.exit(0)
```

start_process_with_no_shell: Starting a process without a shell.
Test ID: B606
Severity: LOW
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/tornado/autoreload.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b606_start_process_with_no_shell.html

```
219             try:
220                 os.execv(sys.executable, [sys.executable] + sys.argv)
221             except OSError:
```

start_process_with_no_shell: Starting a process without a shell.
Test ID: B606
Severity: LOW
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/tornado/autoreload.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b606_start_process_with_no_shell.html

```
232                 # this error specifically.
233                 os.spawnv(os.P_NOWAIT, sys.executable,
234                           [sys.executable] + sys.argv)
235                 # At this point the IOLoop has been closed and finally
```

blacklist: Standard pseudo-random generators are not suitable for security/cryptographic purposes.
Test ID: B311
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/tornado/event_queue.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_calls.html#b311-random

```
200             ioloop = tornado.ioloop.IOLoop.instance()
201             interval = HEARTBEAT_MIN_FREQ_SECS + random.randint(0, 10)
202             if self.client_type_name != 'API: heartbeat test':
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/tornado/event_queue.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
339     def clear_client_event_queues_for_testing() -> None:
340         assert(settings.TEST_SUITE)
341         clients.clear()
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/tornado/event_queue.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b108_hardcoded_tmp_directory.html

```
425             if last:
426                 return "/var/tmp/event_queues.json.last"
427             return settings.JSON_PERSISTENT_QUEUE_FILENAME_PATTERN % ('',)
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/tornado/event_queue.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b108_hardcoded_tmp_directory.html

```
428         if last:
429             return "/var/tmp/event_queues.%d.last.json" % (port,)
430         return settings.JSON_PERSISTENT_QUEUE_FILENAME_PATTERN % ('.' + str(port),)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/tornado/event_queue.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
655                 continue
656             assert 'flags' in event
657
658             flags = event.get('flags')
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/tornado/socket.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
64      def deregister_connection(conn: 'SocketConnection') -> None:
65          assert conn.client_id is not None
66          del connections[conn.client_id]
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/auth.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
641         except ZulipLDAPConfigurationError as e:
642             assert len(e.args) > 1
643             return redirect_to_misconfigured_ldap_notice(e.args[1])
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/email_log.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
58          result = client.post('/accounts/password/reset/', {'email': registered_email}, **host_kwargs)
59          assert result.status_code == 302
60
61          # Confirm account email
62          result = client.post('/accounts/home/', {'email': unregistered_email_1}, **host_kwargs)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/email_log.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
62          result = client.post('/accounts/home/', {'email': unregistered_email_1}, **host_kwargs)
63          assert result.status_code == 302
64
65          # Find account email
66          result = client.post('/accounts/find/', {'emails': registered_email}, **host_kwargs)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/email_log.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
66          result = client.post('/accounts/find/', {'emails': registered_email}, **host_kwargs)
67          assert result.status_code == 302
68
69          # New login email
70          logged_in = client.login(dev_auth_username=registered_email, realm=realm)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/email_log.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
70          logged_in = client.login(dev_auth_username=registered_email, realm=realm)
71          assert logged_in
72
73          # New user invite and reminder emails
74          result = client.post("/json/invites",
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/email_log.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
76                              **host_kwargs)
77          assert result.status_code == 200
78
79          # Verification for new email
80          result = client.patch('/json/settings',
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101

Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/email_log.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
82                                **host_kwargs)
83          assert result.status_code == 200
84
85          # Email change successful
86          key = Confirmation.objects.filter(type=Confirmation.EMAIL_CHANGE).latest('id').confirmation_key
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/email_log.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
89          result = client.get(url)
90          assert result.status_code == 200
91
92          # Reset the email value so we can run this again
93          user_profile.email = registered_email
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/messages.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
211                 # a Zephyr realm are private, so that doesn't happen.
212                 assert(not stream.is_public())
213
214                 m = re.search(r'^(?:un)*(.+?)(?:\.d)*$', stream.name, re.IGNORECASE)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/messages.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
216                 # stream name, this will always match
217                 assert(m is not None)
218                 base_stream_name = m.group(1)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/messages.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
236                 # Since the regex has a `.*` in it, this will always match
237                 assert(m is not None)
238                 base_topic = m.group(1)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/messages.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
591         else:
592             assert(need_message)
```

```
593             query = select([column("id").label("message_id")],
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/messages.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
1284        if len(message_history) > 0:
1285            assert(datetime_to_timestamp(message.last_edit_time) ==
1286                   message_history[0]['timestamp'])
1287
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/realm_icon.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
53          # hacks to prevent us from having to jump through decode/encode hoops.
54          assert '?' in url
55          url += '&' + request.META['QUERY_STRING']
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/registration.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
203                 setup_realm_internal_bots(realm)
204             assert(realm is not None)
205
206             full_name = form.cleaned_data['full_name']
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/report.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
20
21      import subprocess
22      import os
```

start_process_with_partial_path: Starting a process with a partial executable path
Test ID: B607
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/report.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b607_start_process_with_partial_path.html

```
111         try:
112             version = subprocess.check_output(["git", "log", "HEAD^..HEAD", "--oneline"],
113                                               universal_newlines=True)  # type: Optional[str]
114         except Exception:
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/report.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
111         try:
112             version = subprocess.check_output(["git", "log", "HEAD^..HEAD", "--oneline"],
113                                               universal_newlines=True)  # type: Optional[str]
114         except Exception:
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/users.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
74          if target.is_bot:
75              assert target.bot_type is not None
76              check_bot_creation_policy(user_profile, target.bot_type)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/users.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
145         # hacks to prevent us from having to jump through decode/encode hoops.
146         assert url is not None
147         assert '?' in url
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/users.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
146         assert url is not None
147         assert '?' in url
148         url += '&' + request.META['QUERY_STRING']
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/users.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
206             check_valid_interface_type(service_interface)
207             assert service_interface is not None
208             do_update_outgoing_webhook_service(bot, service_interface, service_payload_url)
```

hardcoded_password_funcarg: Possible hardcoded password: ''
Test ID: B106
Severity: LOW
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zerver/views/users.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b106_hardcoded_password_funcarg.html

```
318
319         bot_profile = do_create_user(email=email, password='',
320                                      realm=user_profile.realm, full_name=full_name,
321                                      short_name=short_name,
322                                      bot_type=bot_type,
323                                      bot_owner=user_profile,
324                                      avatar_source=avatar_source,
325                                      default_sending_stream=default_sending_stream,
326                                      default_events_register_stream=default_events_register_stream,
327                                      default_all_public_streams=default_all_public_streams)
328         if len(request.FILES) == 1:
```

blacklist: Consider possible security implications associated with subprocess module.
Test ID: B404
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/zephyr.py
More info: https://bandit.readthedocs.io/en/latest/blacklists/blacklist_imports.html#b404-import-subprocess

```
15      import logging
16      import subprocess
17      import ujson
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/zephyr.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
40                  user = kerberos_alter_egos[user]
41              assert(user == user_profile.email.split("@")[0])
42              ccache = make_ccache(parsed_cred)
```

start_process_with_partial_path: Starting a process with a partial executable path
Test ID: B607
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/zephyr.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b607_start_process_with_partial_path.html

```
48              api_key = get_api_key(user_profile)
49              subprocess.check_call(["ssh", settings.PERSONAL_ZMIRROR_SERVER, "--",
50                                     "/home/zulip/python-zulip-api/zulip/integrations/zephyr/process_ccache",
51                                     force_str(user),
52                                     force_str(api_key),
53                                     force_str(base64.b64encode(ccache))])
54          except Exception:
```

subprocess_without_shell_equals_true: subprocess call - check for execution of untrusted input.
Test ID: B603
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/views/zephyr.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b603_subprocess_without_shell_equals_true.html

```
48              api_key = get_api_key(user_profile)
49              subprocess.check_call(["ssh", settings.PERSONAL_ZMIRROR_SERVER, "--",
50                                     "/home/zulip/python-zulip-api/zulip/integrations/zephyr/process_ccache",
51                                     force_str(user),
52                                     force_str(api_key),
53                                     force_str(base64.b64encode(ccache))])
54          except Exception:
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/webhooks/appfollow/view.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
19          app_name_search = re.search(r'\A(.+)', message)
20          assert app_name_search is not None
21          app_name = app_name_search.group(0)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101

Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/webhooks/bitbucket2/view.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
100     def get_subject(payload: Dict[str, Any]) -> str:
101         assert(payload['repository'] is not None)
102         return BITBUCKET_SUBJECT_TEMPLATE.format(repository_name=get_repository_name(payload['repository']))
```

try_except_pass: Try, Except, Pass detected.
Test ID: B110
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/worker/queue_processors.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b110_try_except_pass.html

```
100                 os.kill(os.getpid(), signal.SIGUSR1)
101         except Exception:
102             pass
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zerver/worker/queue_processors.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
567                         )
568                         assert message['content'] is not None
569                     bot_handler.handle_message(
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zproject/backends.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
164                 # These are kwargs only for readability; they should never be None
165                 assert username is not None
166                 assert realm is not None
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zproject/backends.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
165                 assert username is not None
166                 assert realm is not None
167                 return common_get_active_user(username, realm, return_data)
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zproject/backends.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
250                         return_data: Optional[Dict[str, Any]]=None) -> Optional[UserProfile]:
251             assert remote_user is not None
252             if realm is None:
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101

Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zproject/backends.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
416                         return_data: Optional[Dict[str, Any]]=None) -> Optional[UserProfile]:
417             assert dev_auth_username is not None
418             if realm is None:
```

assert_used: Use of assert detected. The enclosed code will be removed when compiling to optimised byte code.
Test ID: B101
Severity: LOW
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zproject/backends.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b101_assert_used.html

```
540         # being incorrectly authenticated.
541         assert return_data.get('valid_attestation') is True
542
543         strategy = backend.strategy  # type: ignore # This comes from Python Social Auth.
```

jinja2_autoescape_false: By default, jinja2 sets autoescape to False. Consider using autoescape=True or use the select_autoescape function to mitigate XSS vulnerabilities.
Test ID: B701
Severity: HIGH
Confidence: HIGH
File: /home/groth/zulip-server-1.9.0/zproject/jinja2/__init__.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b701_jinja2_autoescape_false.html

```
15      def environment(**options: Any) -> Environment:
16          env = Environment(**options)
17          env.globals.update({
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
File: /home/groth/zulip-server-1.9.0/zproject/settings.py
More info: https://bandit.readthedocs.io/en/latest/plugins/b108_hardcoded_tmp_directory.html

```
1065
1066    ZULIP_WORKER_TEST_FILE = '/tmp/zulip-worker-test-file'
1067
1068
1069    if IS_WORKER:
```