Metrics:

Total lines of code: 880462
Total lines skipped (#nosec): 7

hardcoded_bind_all_interfaces: Possible binding to all interfaces.
Test ID: B104
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-605
File: ./.venv/lib/python3.9/site-packages/anyio/_core/_sockets.py
Line number: 490
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b104_hardcoded_bind_all_interfaces.html

```
489         else:
490             local_address = ("0.0.0.0", 0)
491
```

django_extra_used: Use of extra potential SQL attack vector.
Test ID: B610
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-89
File: ./.venv/lib/python3.9/site-packages/anyio/streams/tls.py
Line number: 247
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b610_django_extra_used.html

```
246         async def send_eof(self) -> None:
247             tls_version = self.extra(TLSAttribute.tls_version)
248             match = re.match(r"TLSv(\d+)(?:\.(\d+))?", tls_version)
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/anyio/to_interpreter.py
Line number: 123
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
122                 if fmt == FMT_PICKLED:
123                     res = pickle.loads(res)
124
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/anyio/to_process.py
Line number: 86
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
85
86              retval = pickle.loads(pickled_response)
87              if status == b"EXCEPTION":
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/anyio/to_process.py
Line number: 210
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
209             try:
210                 command, *args = pickle.load(stdin.buffer)
211             except EOFError:
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78

File: ./.venv/lib/python3.9/site-packages/attr/_make.py
Line number: 227
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
226         bytecode = compile(script, filename, "exec")
227         eval(bytecode, globs, locs)
228
```

---

blacklist: Use of insecure MD2, MD4, MD5, or SHA1 hash function.
Test ID: B303
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/authlib/jose/rfc7518/jwe_algs.py
Line number: 329
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b303-md5

```
328             "RSAES OAEP using default parameters",
329             padding.OAEP(padding.MGF1(hashes.SHA1()), hashes.SHA1(), None),
330         ),
```

---

blacklist: Use of insecure MD2, MD4, MD5, or SHA1 hash function.
Test ID: B303
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/authlib/jose/rfc7518/jwe_algs.py
Line number: 329
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b303-md5

```
328             "RSAES OAEP using default parameters",
329             padding.OAEP(padding.MGF1(hashes.SHA1()), hashes.SHA1(), None),
330         ),
```

---

hashlib: Use of weak SHA1 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/authlib/oauth1/rfc5849/client_auth.py
Line number: 150
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
149             if body and headers.get("Content-Type") != CONTENT_TYPE_FORM_URLENCODED:
150                 oauth_body_hash = base64.b64encode(hashlib.sha1(body).digest())
151                 oauth_params.append(("oauth_body_hash", oauth_body_hash.decode("utf-8")))
```

---

blacklist: Use of insecure MD2, MD4, MD5, or SHA1 hash function.
Test ID: B303
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/authlib/oauth1/rfc5849/rsa.py
Line number: 15
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b303-md5

```
14          )
15          return key.sign(msg, padding.PKCS1v15(), hashes.SHA1())
16
```

---

blacklist: Use of insecure MD2, MD4, MD5, or SHA1 hash function.
Test ID: B303
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/authlib/oauth1/rfc5849/rsa.py
Line number: 21
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b303-md5

```
20          try:
21              key.verify(sig, msg, padding.PKCS1v15(), hashes.SHA1())
22              return True
```

---

trojansource: A Python source file contains bidirectional control characters ('\u202e').
Test ID: B613
Severity: HIGH

Confidence: MEDIUM
CWE: CWE-838
File: ./.venv/lib/python3.9/site-packages/bandit/plugins/trojansource.py
Line number: 22
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b613_trojansource.html

```
21          3          access_level = "user"
22          4      if access_level != 'none' and access_level != 'user': # Check if admin
23          5          print("You are an admin.\n")
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/boltons/fileutils.py
Line number: 703
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
702     if __name__ == '__main__':
703         with atomic_save('/tmp/final.txt') as f:
704             f.write('rofl')
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/boltons/funcutils.py
Line number: 1035
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
1034                code = compile(src, filename, 'single')
1035                exec(code, execdict)
1036            except Exception:
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/boltons/namedutils.py
Line number: 64
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
63          def exec_(code, global_env):
64              exec("exec code in global_env")
65      except NameError:
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/boltons/namedutils.py
Line number: 68
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
67          def exec_(code, global_env):
68              exec(code, global_env)
69
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/cffi/recompiler.py
Line number: 78
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
77          def as_python_expr(self):
78              flags = eval(self.flags, G_FLAGS)
79              fields_expr = [c_field.as_field_python_expr()
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/cffi/setuptools_ext.py
Line number: 26
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
25          code = compile(src, filename, 'exec')
26          exec(code, glob, glob)
27
```

subprocess_popen_with_shell_equals_true: subprocess call with shell=True identified, security issue.
Test ID: B602
Severity: HIGH
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/click/_termui_impl.py
Line number: 429
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b602_subprocess_popen_with_shell_equals_true.html

```
428             [cmd_absolute],
429             shell=True,
430             stdin=subprocess.PIPE,
431             env=env,
432             errors="replace",
433             text=True,
434         )
435         assert c.stdin is not None
436         try:
437             for text in generator:
```

subprocess_popen_with_shell_equals_true: subprocess call with shell=True identified, security issue.
Test ID: B602
Severity: HIGH
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/click/_termui_impl.py
Line number: 552
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b602_subprocess_popen_with_shell_equals_true.html

```
551             try:
552                 c = subprocess.Popen(f'{editor} "{filename}"', env=environ, shell=True)
553                 exit_code = c.wait()
```

blacklist: Use of insecure MD2, MD4, MD5, or SHA1 hash function.
Test ID: B303
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/cryptography/hazmat/_oid.py
Line number: 128
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b303-md5

```
127     _SIG_OIDS_TO_HASH: dict[ObjectIdentifier, hashes.HashAlgorithm | None] = {
128         SignatureAlgorithmOID.RSA_WITH_MD5: hashes.MD5(),
129         SignatureAlgorithmOID.RSA_WITH_SHA1: hashes.SHA1(),
```

blacklist: Use of insecure MD2, MD4, MD5, or SHA1 hash function.
Test ID: B303
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/cryptography/hazmat/_oid.py
Line number: 129
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b303-md5

```
128         SignatureAlgorithmOID.RSA_WITH_MD5: hashes.MD5(),
129         SignatureAlgorithmOID.RSA_WITH_SHA1: hashes.SHA1(),
130         SignatureAlgorithmOID._RSA_WITH_SHA1: hashes.SHA1(),
```

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

Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/cryptography/hazmat/_oid.py
Line number: 130
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b303-md5

```
129         SignatureAlgorithmOID.RSA_WITH_SHA1: hashes.SHA1(),
130         SignatureAlgorithmOID._RSA_WITH_SHA1: hashes.SHA1(),
131         SignatureAlgorithmOID.RSA_WITH_SHA224: hashes.SHA224(),
```

blacklist: Use of insecure MD2, MD4, MD5, or SHA1 hash function.
Test ID: B303
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/cryptography/hazmat/_oid.py
Line number: 139
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b303-md5

```
138         SignatureAlgorithmOID.RSA_WITH_SHA3_512: hashes.SHA3_512(),
139         SignatureAlgorithmOID.ECDSA_WITH_SHA1: hashes.SHA1(),
140         SignatureAlgorithmOID.ECDSA_WITH_SHA224: hashes.SHA224(),
```

blacklist: Use of insecure MD2, MD4, MD5, or SHA1 hash function.
Test ID: B303
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/cryptography/hazmat/_oid.py
Line number: 148
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b303-md5

```
147         SignatureAlgorithmOID.ECDSA_WITH_SHA3_512: hashes.SHA3_512(),
148         SignatureAlgorithmOID.DSA_WITH_SHA1: hashes.SHA1(),
149         SignatureAlgorithmOID.DSA_WITH_SHA224: hashes.SHA224(),
```

blacklist: Use of insecure cipher mode cryptography.hazmat.primitives.ciphers.modes.ECB.
Test ID: B305
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/cryptography/hazmat/primitives/keywrap.py
Line number: 21
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b304-b305-ciphers-and-modes

```
20          # RFC 3394 Key Wrap - 2.2.1 (index method)
21          encryptor = Cipher(AES(wrapping_key), ECB()).encryptor()
22          n = len(r)
```

blacklist: Use of insecure cipher mode cryptography.hazmat.primitives.ciphers.modes.ECB.
Test ID: B305
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/cryptography/hazmat/primitives/keywrap.py
Line number: 64
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b304-b305-ciphers-and-modes

```
63          # Implement RFC 3394 Key Unwrap - 2.2.2 (index method)
64          decryptor = Cipher(AES(wrapping_key), ECB()).decryptor()
65          n = len(r)
```

blacklist: Use of insecure cipher mode cryptography.hazmat.primitives.ciphers.modes.ECB.
Test ID: B305
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/cryptography/hazmat/primitives/keywrap.py
Line number: 97
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b304-b305-ciphers-and-modes

```
96              # RFC 5649 - 4.1 - exactly 8 octets after padding
97              encryptor = Cipher(AES(wrapping_key), ECB()).encryptor()
98              b = encryptor.update(aiv + key_to_wrap)
```

blacklist: Use of insecure cipher mode cryptography.hazmat.primitives.ciphers.modes.ECB.
Test ID: B305
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/cryptography/hazmat/primitives/keywrap.py
Line number: 119
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b304-b305-ciphers-and-modes

```
118             # RFC 5649 - 4.2 - exactly two 64-bit blocks
119             decryptor = Cipher(AES(wrapping_key), ECB()).decryptor()
120             out = decryptor.update(wrapped_key)
```

blacklist: Use of insecure MD2, MD4, MD5, or SHA1 hash function.
Test ID: B303
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/cryptography/hazmat/primitives/serialization/ssh.py
Line number: 1007
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b303-md5

```
1006                if self._inner_sig_type == _SSH_RSA:
1007                    hash_alg = hashes.SHA1()
1008                elif self._inner_sig_type == _SSH_RSA_SHA256:
```

hashlib: Use of weak SHA1 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/cryptography/x509/extensions.py
Line number: 72
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
71
72          return hashlib.sha1(data).digest()
73
```

blacklist: Using xmlrpc to parse untrusted XML data is known to be vulnerable to XML attacks. Use defusedxml.xmlrpc.monkey_patch() function to monkey-patch xmlrpclib and mitigate XML vulnerabilities.
Test ID: B411
Severity: HIGH
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/defusedxml/__init__.py
Line number: 37
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_imports.html#b411-import-xmlrpclib

```
36          from . import expatreader
37          from . import xmlrpc
38
```

blacklist: Using xml.dom.pulldom.parse to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.dom.pulldom.parse with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B319
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/defusedxml/pulldom.py
Line number: 30
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b313-b320-xml-bad-pulldom

```
29              parser.forbid_external = forbid_external
30          return _parse(stream_or_string, parser, bufsize)
31
```

blacklist: Using xml.dom.pulldom.parseString to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.dom.pulldom.parseString with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B319
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/defusedxml/pulldom.py
Line number: 41
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b313-b320-xml-bad-pulldom

```
40              parser.forbid_external = forbid_external
41          return _parseString(string, parser)
```

blacklist: Using ExpatParser to parse untrusted XML data is known to be vulnerable to XML attacks. Use defusedxml.xmlrpc.monkey_patch() function to monkey-patch xmlrpclib and mitigate XML vulnerabilities.
Test ID: B411
Severity: HIGH
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/defusedxml/xmlrpc.py
Line number: 18
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_imports.html#b411-import-xmlrpclib

```
17          __origin__ = "xmlrpc.client"
18          from xmlrpc.client import ExpatParser
19          from xmlrpc import client as xmlrpc_client
```

blacklist: Using client to parse untrusted XML data is known to be vulnerable to XML attacks. Use defusedxml.xmlrpc.monkey_patch() function to monkey-patch xmlrpclib and mitigate XML vulnerabilities.
Test ID: B411
Severity: HIGH
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/defusedxml/xmlrpc.py
Line number: 19
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_imports.html#b411-import-xmlrpclib

```
18          from xmlrpc.client import ExpatParser
19          from xmlrpc import client as xmlrpc_client
20          from xmlrpc import server as xmlrpc_server
```

blacklist: Using server to parse untrusted XML data is known to be vulnerable to XML attacks. Use defusedxml.xmlrpc.monkey_patch() function to monkey-patch xmlrpclib and mitigate XML vulnerabilities.
Test ID: B411
Severity: HIGH
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/defusedxml/xmlrpc.py
Line number: 20
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_imports.html#b411-import-xmlrpclib

```
19          from xmlrpc import client as xmlrpc_client
20          from xmlrpc import server as xmlrpc_server
21          from xmlrpc.client import gzip_decode as _orig_gzip_decode
```

blacklist: Using gzip_decode to parse untrusted XML data is known to be vulnerable to XML attacks. Use defusedxml.xmlrpc.monkey_patch() function to monkey-patch xmlrpclib and mitigate XML vulnerabilities.
Test ID: B411
Severity: HIGH
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/defusedxml/xmlrpc.py
Line number: 21
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_imports.html#b411-import-xmlrpclib

```
20          from xmlrpc import server as xmlrpc_server
21          from xmlrpc.client import gzip_decode as _orig_gzip_decode
22          from xmlrpc.client import GzipDecodedResponse as _OrigGzipDecodedResponse
```

blacklist: Using GzipDecodedResponse to parse untrusted XML data is known to be vulnerable to XML attacks. Use defusedxml.xmlrpc.monkey_patch() function to monkey-patch xmlrpclib and mitigate XML vulnerabilities.
Test ID: B411
Severity: HIGH
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/defusedxml/xmlrpc.py
Line number: 22
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_imports.html#b411-import-xmlrpclib

```
21          from xmlrpc.client import gzip_decode as _orig_gzip_decode
22          from xmlrpc.client import GzipDecodedResponse as _OrigGzipDecodedResponse
23      else:
```

blacklist: Using ExpatParser to parse untrusted XML data is known to be vulnerable to XML attacks. Use defusedxml.xmlrpc.monkey_patch() function to monkey-patch xmlrpclib and mitigate XML vulnerabilities.
Test ID: B411

Severity: HIGH
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/defusedxml/xmlrpc.py
Line number: 25
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_imports.html#b411-import-xmlrpclib

```
24          __origin__ = "xmlrpclib"
25          from xmlrpclib import ExpatParser
26          import xmlrpclib as xmlrpc_client
```

blacklist: Using xmlrpclib to parse untrusted XML data is known to be vulnerable to XML attacks. Use defusedxml.xmlrpc.monkey_patch() function to monkey-patch xmlrpclib and mitigate XML vulnerabilities.
Test ID: B411
Severity: HIGH
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/defusedxml/xmlrpc.py
Line number: 26
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_imports.html#b411-import-xmlrpclib

```
25          from xmlrpclib import ExpatParser
26          import xmlrpclib as xmlrpc_client
27
```

blacklist: Using gzip_decode to parse untrusted XML data is known to be vulnerable to XML attacks. Use defusedxml.xmlrpc.monkey_patch() function to monkey-patch xmlrpclib and mitigate XML vulnerabilities.
Test ID: B411
Severity: HIGH
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/defusedxml/xmlrpc.py
Line number: 29
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_imports.html#b411-import-xmlrpclib

```
28          xmlrpc_server = None
29          from xmlrpclib import gzip_decode as _orig_gzip_decode
30          from xmlrpclib import GzipDecodedResponse as _OrigGzipDecodedResponse
```

blacklist: Using GzipDecodedResponse to parse untrusted XML data is known to be vulnerable to XML attacks. Use defusedxml.xmlrpc.monkey_patch() function to monkey-patch xmlrpclib and mitigate XML vulnerabilities.
Test ID: B411
Severity: HIGH
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/defusedxml/xmlrpc.py
Line number: 30
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_imports.html#b411-import-xmlrpclib

```
29          from xmlrpclib import gzip_decode as _orig_gzip_decode
30          from xmlrpclib import GzipDecodedResponse as _OrigGzipDecodedResponse
31
```

hashlib: Use of weak SHA1 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/face/sinter.py
Line number: 139
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
138     def compile_code(code_str, name, env=None, verbose=_VERBOSE):
139         code_hash = hashlib.sha1(code_str.encode('utf8')).hexdigest()[:16]
140         unique_filename = "<sinter generated %s %s>" % (name, code_hash)
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/face/sinter.py
Line number: 145
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
144         if PY3:
145             exec(code, env)
```

```
146         else:
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/face/sinter.py
Line number: 147
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
146         else:
147             exec("exec code in env")
148
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/glom/cli.py
Line number: 222
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
221         if PY3:
222             exec(code, env)
223         else:
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/glom/cli.py
Line number: 224
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
223         else:
224             exec("exec code in env")
225
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/glom/test/test_basic.py
Line number: 251
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
250             ).star(args='args2', kwargs='kwargs')
251         assert repr(eval(repr(repr_spec), locals(), globals())) == repr(repr_spec)
252
```

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
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/glom/test/test_basic.py
Line number: 414
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b313-b320-xml-bad-celementtree

```
413         etree2tuples = Fill(Ref('ElementTree', (T.tag, Iter(Ref('ElementTree')).all())))
414         etree = ElementTree.fromstring('''
415         <html>
416           <head>
417             <title>the title</title>
418           </head>
419           <body id="the-body">
420             <p>A paragraph</p>
421           </body>
422         </html>''')
423         glom(etree, etree2dicts)
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/glom/test/test_match.py
Line number: 235
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
234         assert repr(And(M == 1, float)) == "(M == 1) & float"
235         assert repr(eval(repr(And(M == 1, float)))) == "(M == 1) & float"
236
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/glom/test/test_mutation.py
Line number: 36
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
35          assert repr(assign_spec) == "Assign(T.a, 1, missing=dict)"
36          assert repr(assign_spec) == repr(eval(repr(assign_spec)))
37
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/glom/test/test_path_and_t.py
Line number: 98
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
97
98          rt_spec = pickle.loads(pickle.dumps(spec))
99          assert repr(spec) == repr(rt_spec)
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/glom/test/test_path_and_t.py
Line number: 104
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
103         s_spec = S.attribute
104         assert repr(s_spec) == repr(pickle.loads(pickle.dumps(s_spec)))
105
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/glom/test/test_snippets.py
Line number: 58
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
57              return  # maybe in the future
58          eval(code, SNIPPETS_GLOBALS)
59
```

hashlib: Use of weak SHA1 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/google/protobuf/proto_builder.py
Line number: 68
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
67        # proto files.
68        fields_hash = hashlib.sha1()
```

```
69        for f_name, f_type in field_items:
```

django_extra_used: Use of extra potential SQL attack vector.
Test ID: B610
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-89
File: ./.venv/lib/python3.9/site-packages/httpcore/_backends/anyio.py
Line number: 84
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b610_django_extra_used.html

```
83              if info == "ssl_object":
84                  return self._stream.extra(anyio.streams.tls.TLSAttribute.ssl_object, None)
85              if info == "client_addr":
```

django_extra_used: Use of extra potential SQL attack vector.
Test ID: B610
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-89
File: ./.venv/lib/python3.9/site-packages/httpcore/_backends/anyio.py
Line number: 86
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b610_django_extra_used.html

```
85              if info == "client_addr":
86                  return self._stream.extra(anyio.abc.SocketAttribute.local_address, None)
87              if info == "server_addr":
```

django_extra_used: Use of extra potential SQL attack vector.
Test ID: B610
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-89
File: ./.venv/lib/python3.9/site-packages/httpcore/_backends/anyio.py
Line number: 88
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b610_django_extra_used.html

```
87              if info == "server_addr":
88                  return self._stream.extra(anyio.abc.SocketAttribute.remote_address, None)
89              if info == "socket":
```

django_extra_used: Use of extra potential SQL attack vector.
Test ID: B610
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-89
File: ./.venv/lib/python3.9/site-packages/httpcore/_backends/anyio.py
Line number: 90
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b610_django_extra_used.html

```
89              if info == "socket":
90                  return self._stream.extra(anyio.abc.SocketAttribute.raw_socket, None)
91              if info == "is_readable":
```

django_extra_used: Use of extra potential SQL attack vector.
Test ID: B610
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-89
File: ./.venv/lib/python3.9/site-packages/httpcore/_backends/anyio.py
Line number: 92
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b610_django_extra_used.html

```
91              if info == "is_readable":
92                  sock = self._stream.extra(anyio.abc.SocketAttribute.raw_socket, None)
93                  return is_socket_readable(sock)
```

hashlib: Use of weak SHA1 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/httpx/_auth.py
Line number: 309
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
308
309             return hashlib.sha1(s).hexdigest()[:16].encode()
310
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/jinja2/bccache.py
Line number: 73
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
72              # the source code of the file changed, we need to reload
73              checksum = pickle.load(f)
74              if self.checksum != checksum:
```

blacklist: Deserialization with the marshal module is possibly dangerous.
Test ID: B302
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/jinja2/bccache.py
Line number: 79
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b302-marshal

```
78              try:
79                  self.code = marshal.load(f)
80              except (EOFError, ValueError, TypeError):
```

hashlib: Use of weak SHA1 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/jinja2/bccache.py
Line number: 156
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
155             """Returns the unique hash key for this template name."""
156             hash = sha1(name.encode("utf-8"))
157
```

hashlib: Use of weak SHA1 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/jinja2/bccache.py
Line number: 165
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
164             """Returns a checksum for the source."""
165             return sha1(source.encode("utf-8")).hexdigest()
166
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/jinja2/debug.py
Line number: 145
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
144         try:
145             exec(code, globals, locals)
146         except BaseException:
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/jinja2/environment.py

Line number: 1228
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
1227            namespace = {"environment": environment, "__file__": code.co_filename}
1228            exec(code, namespace)
1229            rv = cls._from_namespace(environment, namespace, globals)
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/environment.py
Line number: 1544
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
1543        def __html__(self) -> Markup:
1544            return Markup(concat(self._body_stream))
1545
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/ext.py
Line number: 176
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
175             if __context.eval_ctx.autoescape:
176                 rv = Markup(rv)
177             # Always treat as a format string, even if there are no
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/ext.py
Line number: 197
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
196             if __context.eval_ctx.autoescape:
197                 rv = Markup(rv)
198             # Always treat as a format string, see gettext comment above.
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/ext.py
Line number: 213
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
212             if __context.eval_ctx.autoescape:
213                 rv = Markup(rv)
214
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/ext.py
Line number: 238
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
237             if __context.eval_ctx.autoescape:
238                 rv = Markup(rv)
239
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH

CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/filters.py
Line number: 316
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
315         if eval_ctx.autoescape:
316             rv = Markup(rv)
317
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/filters.py
Line number: 820
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
819         if eval_ctx.autoescape:
820             rv = Markup(rv)
821
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/filters.py
Line number: 851
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
850         if isinstance(s, Markup):
851             indention = Markup(indention)
852             newline = Markup(newline)
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/filters.py
Line number: 852
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
851             indention = Markup(indention)
852             newline = Markup(newline)
853
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/filters.py
Line number: 1056
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
1055
1056        return Markup(str(value)).striptags()
1057
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/filters.py
Line number: 1377
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
1376        """
1377        return Markup(value)
1378
```

hashlib: Use of weak SHA1 hash for security. Consider usedforsecurity=False
Test ID: B324

Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/jinja2/loaders.py
Line number: 661
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
660         def get_template_key(name: str) -> str:
661             return "tmpl_" + sha1(name.encode("utf-8")).hexdigest()
662
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/nodes.py
Line number: 619
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
618             if eval_ctx.autoescape:
619                 return Markup(self.data)
620             return self.data
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/nodes.py
Line number: 1091
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
1090            eval_ctx = get_eval_context(self, eval_ctx)
1091            return Markup(self.expr.as_const(eval_ctx))
1092
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/nodes.py
Line number: 1112
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
1111            if eval_ctx.autoescape:
1112                return Markup(expr)
1113            return expr
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/runtime.py
Line number: 375
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
374             if self._context.eval_ctx.autoescape:
375                 return Markup(rv)
376
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/runtime.py
Line number: 389
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
388             if self._context.eval_ctx.autoescape:
389                 return Markup(rv)
390
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/runtime.py
Line number: 776
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
775             if autoescape:
776                 return Markup(rv)
777
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/runtime.py
Line number: 787
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
786             if autoescape:
787                 rv = Markup(rv)
788
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/utils.py
Line number: 403
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
402             return "\n\n".join(result)
403         return markupsafe.Markup(
404             "\n".join(f"<p>{markupsafe.escape(x)}</p>" for x in result)
405         )
406
```

markupsafe_markup_xss: Potential XSS with ``markupsafe.Markup`` detected. Do not use ``Markup`` on untrusted data.
Test ID: B704
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-79
File: ./.venv/lib/python3.9/site-packages/jinja2/utils.py
Line number: 668
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b704_markupsafe_markup_xss.html

```
667
668         return markupsafe.Markup(
669             dumps(obj, **kwargs)
670             .replace("<", "\\u003c")
671             .replace(">", "\\u003e")
672             .replace("&", "\\u0026")
673             .replace("'", "\\u0027")
674         )
675
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/joblib/_memmapping_reducer.py
Line number: 40
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
39      # as the default folder to dump big arrays to share with subprocesses.
40      SYSTEM_SHARED_MEM_FS = "/dev/shm"
41
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301

Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/joblib/externals/loky/backend/popen_loky_posix.py
Line number: 174
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
173                 try:
174                     prep_data = pickle.load(from_parent)
175                     spawn.prepare(prep_data)
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/joblib/externals/loky/backend/popen_loky_posix.py
Line number: 176
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
175                     spawn.prepare(prep_data)
176                     process_obj = pickle.load(from_parent)
177                 finally:
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/joblib/externals/loky/backend/popen_loky_win32.py
Line number: 166
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
165             try:
166                 preparation_data = load(from_parent)
167                 spawn.prepare(preparation_data, parent_sentinel)
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/joblib/externals/loky/backend/popen_loky_win32.py
Line number: 168
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
167                 spawn.prepare(preparation_data, parent_sentinel)
168                 self = load(from_parent)
169             finally:
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/joblib/numpy_pickle.py
Line number: 175
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
174                 # The array contained Python objects. We need to unpickle the data.
175                 array = pickle.load(unpickler.file_handle)
176             else:
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/joblib/test/common.py
Line number: 78
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
77      with_dev_shm = skipif(
78          not os.path.exists("/dev/shm"),
79          reason="This test requires a large /dev/shm shared memory fs.",
```

hashlib: Use of weak MD5 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_hashing.py
Line number: 228
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
227         def md5_hash(x):
228             return hashlib.md5(memoryview(x)).hexdigest()
229
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_hashing.py
Line number: 350
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
349         b = {string: "bar"}
350         c = pickle.loads(pickle.dumps(b))
351         assert hash([a, b]) == hash([a, c])
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_hashing.py
Line number: 370
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
369
370         dt1_roundtripped = pickle.loads(pickle.dumps(dt1))
371         assert dt1 is not dt1_roundtripped
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_hashing.py
Line number: 383
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
382
383         complex_dt1_roundtripped = pickle.loads(pickle.dumps(complex_dt1))
384         assert complex_dt1_roundtripped is not complex_dt1
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_memmapping.py
Line number: 937
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
936                 pool_temp_folder = p._temp_folder
937                 folder_prefix = "/dev/shm/joblib_memmapping_folder_"
938                 assert pool_temp_folder.startswith(folder_prefix)
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_memmapping.py
Line number: 993
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
992                 pool_temp_folder = p._temp_folder
993                 assert not pool_temp_folder.startswith("/dev/shm")
```

```
994             finally:
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_memory.py
Line number: 164
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
163             my_locals = {}
164             exec(
165                 compile(
166                     textwrap.dedent(ipython_cell_source),
167                     filename=ipython_cell_id,
168                     mode="exec",
169                 ),
170                 # TODO when Python 3.11 is the minimum supported version, use
171                 # locals=my_locals instead of passing globals and locals in the
172                 # next two lines as positional arguments
173                 None,
174                 my_locals,
175             )
176             f = my_locals["f"]
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_memory.py
Line number: 334
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
333         memory = Memory(location=tmpdir.strpath, verbose=0)
334         a1 = eval("lambda x: x")
335         a1 = memory.cache(a1)
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_memory.py
Line number: 336
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
335         a1 = memory.cache(a1)
336         b1 = eval("lambda x: x+1")
337         b1 = memory.cache(b1)
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_memory.py
Line number: 368
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
367
368         m = eval("lambda x: x")
369         mm = memory.cache(m)
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_memory.py
Line number: 598
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
597
598         h = pickle.loads(pickle.dumps(g))
```

599

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_memory.py
Line number: 604
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
603         assert output == h.store_backend.load_item([h.func_id, args_id])
604         memory2 = pickle.loads(pickle.dumps(memory))
605         assert memory.store_backend.location == memory2.store_backend.location
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_memory.py
Line number: 609
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
608         memory = Memory(location=None, verbose=0)
609         pickle.loads(pickle.dumps(memory))
610         g = memory.cache(f)
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_memory.py
Line number: 611
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
610         g = memory.cache(f)
611         gp = pickle.loads(pickle.dumps(g))
612         gp(1)
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_memory.py
Line number: 704
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
703             with open(filename, "rb") as fp:
704                 result2 = pickle.load(fp)
705             assert result2.get() == result.get()
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_memory.py
Line number: 1219
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
1218        with raises(TypeError) as excinfo:
1219            Memory(location="/tmp/joblib", backend="unknown")
1220        excinfo.match(r"Unknown location*")
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_memory.py
Line number: 1340
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
1339        memorized_result_pickle = pickle.dumps(memorized_result)
1340        memorized_result_loads = pickle.loads(memorized_result_pickle)
1341
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_memory.py
Line number: 1374
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
1373
1374        memory_reloaded = pickle.loads(pickle.dumps(memory))
1375
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_memory.py
Line number: 1387
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
1386
1387        func_cached_reloaded = pickle.loads(pickle.dumps(func_cached))
1388
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_memory.py
Line number: 1400
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
1399        memorized_result = func_cached.call_and_shelve(1)
1400        memorized_result_reloaded = pickle.loads(pickle.dumps(memorized_result))
1401
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/joblib/test/test_store_backends.py
Line number: 33
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
32                  with open(filename, "rb") as f:
33                      reloaded = cpickle.load(f)
34                  break
```

blacklist: Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.
Test ID: B310
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/jsonschema/validators.py
Line number: 113
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b310-urllib-urlopen

```
112         request = Request(uri, headers=headers)  # noqa: S310
113         with urlopen(request) as response:  # noqa: S310
114             warnings.warn(
```

blacklist: Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.
Test ID: B310
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/jsonschema/validators.py

Line number: 1228
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b310-urllib-urlopen

```
1227                # Otherwise, pass off to urllib and assume utf-8
1228                with urlopen(uri) as url:  # noqa: S310
1229                    result = json.loads(url.read().decode("utf-8"))
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/nltk/app/chartparser_app.py
Line number: 815
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
814             with open(filename, "rb") as infile:
815                 chart = pickle.load(infile)
816             name = os.path.basename(filename)
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/nltk/app/chartparser_app.py
Line number: 2272
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
2271                with open(filename, "rb") as infile:
2272                    chart = pickle.load(infile)
2273                self._chart = chart
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/nltk/app/chartparser_app.py
Line number: 2310
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
2309                    with open(filename, "rb") as infile:
2310                        grammar = pickle.load(infile)
2311                else:
```

blacklist: Using xml.etree.ElementTree.parse to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.ElementTree.parse with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B314
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/nltk/chunk/named_entity.py
Line number: 236
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b313-b320-xml-bad-elementtree

```
235         with open(annfile) as infile:
236             xml = ET.parse(infile).getroot()
237         for entity in xml.findall("document/entity"):
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/nltk/chunk/named_entity.py
Line number: 351
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
350             fmt = self._fmt
351             save_maxent_params(wgt, mpg, lab, aon, tab_dir=f"/tmp/english_ace_{fmt}/")
352
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM

Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/nltk/classify/maxent.py
Line number: 1586
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
1585
1586    def save_maxent_params(wgt, mpg, lab, aon, tab_dir="/tmp"):
1587
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/nltk/classify/weka.py
Line number: 375
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
374         def make_classifier(featuresets):
375             return WekaClassifier.train("/tmp/name.model", featuresets, "C4.5")
376
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/nltk/collocations.py
Line number: 398
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
397         try:
398             scorer = eval("BigramAssocMeasures." + sys.argv[1])
399         except IndexError:
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/nltk/collocations.py
Line number: 402
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
401         try:
402             compare_scorer = eval("BigramAssocMeasures." + sys.argv[2])
403         except IndexError:
```

blacklist: Using xml.etree.ElementTree.parse to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.ElementTree.parse with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B314
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/nltk/corpus/reader/bcp47.py
Line number: 40
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b313-b320-xml-bad-elementtree

```
39                  self.subdiv = self.subdiv_dict(
40                      et.parse(fp).iterfind("localeDisplayNames/subdivisions/subdivision")
41                  )
```

blacklist: Using xml.etree.ElementTree.parse to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.ElementTree.parse with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B314
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/nltk/corpus/reader/nombank.py
Line number: 111
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b313-b320-xml-bad-elementtree

```
110             with self.abspath(framefile).open() as fp:
111                 etree = ElementTree.parse(fp).getroot()
112             for roleset in etree.findall("predicate/roleset"):
```

blacklist: Using xml.etree.ElementTree.parse to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.ElementTree.parse with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B314
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/nltk/corpus/reader/nombank.py
Line number: 134
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b313-b320-xml-bad-elementtree

```
133                 with self.abspath(framefile).open() as fp:
134                     etree = ElementTree.parse(fp).getroot()
135                 rsets.append(etree.findall("predicate/roleset"))
```

blacklist: Using xml.etree.ElementTree.parse to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.ElementTree.parse with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B314
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/nltk/corpus/reader/propbank.py
Line number: 107
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b313-b320-xml-bad-elementtree

```
106             with self.abspath(framefile).open() as fp:
107                 etree = ElementTree.parse(fp).getroot()
108             for roleset in etree.findall("predicate/roleset"):
```

blacklist: Using xml.etree.ElementTree.parse to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.ElementTree.parse with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B314
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/nltk/corpus/reader/propbank.py
Line number: 130
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b313-b320-xml-bad-elementtree

```
129                 with self.abspath(framefile).open() as fp:
130                     etree = ElementTree.parse(fp).getroot()
131                 rsets.append(etree.findall("predicate/roleset"))
```

blacklist: Using xml.etree.ElementTree.fromstring to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.ElementTree.fromstring with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B314
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/nltk/corpus/reader/senseval.py
Line number: 114
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b313-b320-xml-bad-elementtree

```
113                     xml_block = _fixXML(xml_block)
114                     inst = ElementTree.fromstring(xml_block)
115                     return [self._parse_instance(inst, lexelt)]
```

blacklist: Using xml.etree.ElementTree.parse to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.ElementTree.parse with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B314
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/nltk/corpus/reader/xmldocs.py
Line number: 45
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b313-b320-xml-bad-elementtree

```
44              with self.abspath(fileid).open() as fp:
45                  elt = ElementTree.parse(fp).getroot()
46              # If requested, wrap it.
```

blacklist: Using xml.etree.ElementTree.fromstring to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.ElementTree.fromstring with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B314
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/nltk/corpus/reader/xmldocs.py

Line number: 393
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b313-b320-xml-bad-elementtree

```
392                 elt_handler(
393                     ElementTree.fromstring(elt.encode("ascii", "xmlcharrefreplace")),
394                     context,
```

blacklist: Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.
Test ID: B310
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/nltk/data.py
Line number: 967
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b310-urllib-urlopen

```
966         else:
967             return urlopen(resource_url)
968
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/nltk/decorators.py
Line number: 136
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
135         src = "lambda %(signature)s: _wrapper_(%(signature)s)" % infodict
136         funcopy = eval(src, dict(_wrapper_=wrapper))
137         return update_wrapper(funcopy, model, infodict)
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/nltk/decorators.py
Line number: 204
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
203             # import sys; print >> sys.stderr, src # for debugging purposes
204             dec_func = eval(src, dict(_func_=func, _call_=caller))
205             return update_wrapper(dec_func, func, infodict)
```

blacklist: Using xml.etree.ElementTree.parse to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.ElementTree.parse with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B314
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/nltk/downloader.py
Line number: 268
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b313-b320-xml-bad-elementtree

```
267             if isinstance(xml, str):
268                 xml = ElementTree.parse(xml)
269             for key in xml.attrib:
```

blacklist: Using xml.etree.ElementTree.parse to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.ElementTree.parse with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B314
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/nltk/downloader.py
Line number: 308
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b313-b320-xml-bad-elementtree

```
307             if isinstance(xml, str):
308                 xml = ElementTree.parse(xml)
309             for key in xml.attrib:
```

blacklist: Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.
Test ID: B310

Severity: MEDIUM
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/nltk/downloader.py
Line number: 694
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b310-urllib-urlopen

```
693             try:
694                 infile = urlopen(info.url)
695                 with open(filepath, "wb") as outfile:
```

blacklist: Using xml.etree.ElementTree.parse to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.ElementTree.parse with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B314
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/nltk/downloader.py
Line number: 937
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b313-b320-xml-bad-elementtree

```
936             self._index = nltk.internals.ElementWrapper(
937                 ElementTree.parse(urlopen(self._url)).getroot()
938             )
```

blacklist: Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.
Test ID: B310
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/nltk/downloader.py
Line number: 937
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b310-urllib-urlopen

```
936             self._index = nltk.internals.ElementWrapper(
937                 ElementTree.parse(urlopen(self._url)).getroot()
938             )
```

hashlib: Use of weak MD5 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/nltk/downloader.py
Line number: 2245
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
2244    def _md5_hexdigest(fp):
2245        md5_digest = md5()
2246        while True:
```

blacklist: Using xml.etree.ElementTree.parse to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.ElementTree.parse with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B314
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/nltk/downloader.py
Line number: 2450
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b313-b320-xml-bad-elementtree

```
2449                     xmlfile = os.path.join(dirname, filename)
2450                     yield ElementTree.parse(xmlfile).getroot()
2451
```

blacklist: Using xml.etree.ElementTree.parse to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.ElementTree.parse with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B314
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/nltk/downloader.py
Line number: 2478
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b313-b320-xml-bad-elementtree

```
2477                     try:
2478                         pkg_xml = ElementTree.parse(xmlfilename).getroot()
```

```
2479                    except Exception as e:
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/nltk/internals.py
Line number: 231
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
230         try:
231             return eval(s[start_position : match.end()]), match.end()
232         except ValueError as e:
```

blacklist: Using xml.etree.ElementTree.fromstring to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.ElementTree.fromstring with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B314
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/nltk/internals.py
Line number: 924
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b313-b320-xml-bad-elementtree

```
923             if isinstance(etree, str):
924                 etree = ElementTree.fromstring(etree)
925             self.__dict__["_etree"] = etree
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/nltk/parse/featurechart.py
Line number: 655
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
654
655         profile.run("for i in range(1): demo()", "/tmp/profile.out")
656         import pstats
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/nltk/parse/featurechart.py
Line number: 658
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
657
658         p = pstats.Stats("/tmp/profile.out")
659         p.strip_dirs().sort_stats("time", "cum").print_stats(60)
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/nltk/parse/transitionparser.py
Line number: 555
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
554             # First load the model
555             model = pickle.load(open(modelFile, "rb"))
556             operation = Transition(self._algorithm)
```

subprocess_popen_with_shell_equals_true: subprocess call with shell=True identified, security issue.
Test ID: B602
Severity: HIGH
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/nltk/sem/boxer.py
Line number: 271
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b602_subprocess_popen_with_shell_equals_true.html

```
270                 p = subprocess.Popen(
271                     cmd, stdout=subprocess.PIPE, stderr=subprocess.PIPE, shell=True
272                 )
273             stdout, stderr = p.communicate()
274
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-89
File: ./.venv/lib/python3.9/site-packages/nltk/sem/chat80.py
Line number: 435
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b608_hardcoded_sql_expressions.html

```
434         for t in records:
435             cur.execute("insert into %s values (?,?,?)" % table_name, t)
436             if verbose:
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/nltk/sem/chat80.py
Line number: 615
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
614         valuation = make_valuation(concepts, read=True)
615         db_out = shelve.open(db, "n")
616
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/nltk/sem/chat80.py
Line number: 635
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
634         else:
635             db_in = shelve.open(db)
636             from nltk.sem import Valuation
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/nltk/sem/util.py
Line number: 274
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
273         if options.model:
274             exec("import %s as model" % options.model)
275
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/nltk/tbl/demo.py
Line number: 256
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
255             with open(cache_baseline_tagger) as print_rules:
256                 baseline_tagger = pickle.load(print_rules)
257                 print(f"Reloaded pickled tagger from {cache_baseline_tagger}")
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH

CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/nltk/tbl/demo.py
Line number: 328
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
327             with open(serialize_output) as print_rules:
328                 brill_tagger_reloaded = pickle.load(print_rules)
329             print(f"Reloaded pickled tagger from {serialize_output}")
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/nltk/tokenize/punkt.py
Line number: 1591
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
1590            print("writing to /tmp/punkt.new...")
1591            with open("/tmp/punkt.new", "w") as outfile:
1592                for aug_tok in tokens:
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/nltk/tokenize/punkt.py
Line number: 1754
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
1753        def save_params(self):
1754            save_punkt_params(self._params, dir=f"/tmp/{self._lang}")
1755
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/nltk/tokenize/punkt.py
Line number: 1774
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
1773
1774    def save_punkt_params(params, dir="/tmp/punkt_tab"):
1775        from os import mkdir
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/nltk/tokenize/texttiling.py
Line number: 451
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
450         else:
451             w = eval("numpy." + window + "(window_len)")
452
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/packaging/licenses/__init__.py
Line number: 100
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
99          try:
100             invalid = eval(python_expression, globals(), locals())
101         except Exception:
```

exec_used: Use of exec detected.
Test ID: B102

Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/peewee.py
Line number: 174
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
173         multi_types = (list, tuple, frozenset, set)
174         exec('def reraise(tp, value, tb=None): raise tp, value, tb')
175         def print_(s):
```

hashlib: Use of weak MD5 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/peewee.py
Line number: 3045
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
3044        if len(constraint) > maxlen:
3045            name_hash = hashlib.md5(constraint.encode('utf-8')).hexdigest()
3046            constraint = '%s_%s' % (constraint[:(maxlen - 8)], name_hash[:7])
```

subprocess_popen_with_shell_equals_true: subprocess call with shell=True identified, security issue.
Test ID: B602
Severity: HIGH
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/pip/_internal/commands/configuration.py
Line number: 247
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b602_subprocess_popen_with_shell_equals_true.html

```
246             try:
247                 subprocess.check_call(f'{editor} "{fname}"', shell=True)
248             except FileNotFoundError as e:
```

blacklist: Using xmlrpc.client to parse untrusted XML data is known to be vulnerable to XML attacks. Use defusedxml.xmlrpc.monkey_patch() function to monkey-patch xmlrpclib and mitigate XML vulnerabilities.
Test ID: B411
Severity: HIGH
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/pip/_internal/commands/search.py
Line number: 7
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_imports.html#b411-import-xmlrpclib

```
6       import textwrap
7       import xmlrpc.client
8       from collections import OrderedDict
```

blacklist: Using xmlrpc.client to parse untrusted XML data is known to be vulnerable to XML attacks. Use defusedxml.xmlrpc.monkey_patch() function to monkey-patch xmlrpclib and mitigate XML vulnerabilities.
Test ID: B411
Severity: HIGH
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/pip/_internal/network/xmlrpc.py
Line number: 5
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_imports.html#b411-import-xmlrpclib

```
4       import urllib.parse
5       import xmlrpc.client
6       from typing import TYPE_CHECKING
```

blacklist: Using _HostType to parse untrusted XML data is known to be vulnerable to XML attacks. Use defusedxml.xmlrpc.monkey_patch() function to monkey-patch xmlrpclib and mitigate XML vulnerabilities.
Test ID: B411
Severity: HIGH
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/pip/_internal/network/xmlrpc.py
Line number: 13
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_imports.html#b411-import-xmlrpclib

```
12      if TYPE_CHECKING:
13          from xmlrpc.client import _HostType, _Marshallable
```

14

tarfile_unsafe_members: tarfile.extractall used without any validation. Please check and discard dangerous members.
Test ID: B202
Severity: HIGH
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/pip/_internal/utils/unpacking.py
Line number: 245
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b202_tarfile_unsafe_members.html

```
244
245                 tar.extractall(location, filter=pip_filter)
246
```

blacklist: Using xmlrpclib to parse untrusted XML data is known to be vulnerable to XML attacks. Use defusedxml.xmlrpc.monkey_patch() function to monkey-patch xmlrpclib and mitigate XML vulnerabilities.
Test ID: B411
Severity: HIGH
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/pip/_vendor/distlib/compat.py
Line number: 42
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_imports.html#b411-import-xmlrpclib

```
41          import httplib
42          import xmlrpclib
43          import Queue as queue
```

blacklist: Using xmlrpc.client to parse untrusted XML data is known to be vulnerable to XML attacks. Use defusedxml.xmlrpc.monkey_patch() function to monkey-patch xmlrpclib and mitigate XML vulnerabilities.
Test ID: B411
Severity: HIGH
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/pip/_vendor/distlib/compat.py
Line number: 81
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_imports.html#b411-import-xmlrpclib

```
80          import urllib.request as urllib2
81          import xmlrpc.client as xmlrpclib
82          import queue
```

tarfile_unsafe_members: tarfile.extractall used without any validation. Please check and discard dangerous members.
Test ID: B202
Severity: HIGH
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/pip/_vendor/distlib/util.py
Line number: 1285
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b202_tarfile_unsafe_members.html

```
1284
1285            archive.extractall(dest_dir)
1286
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/pip/_vendor/packaging/licenses/__init__.py
Line number: 100
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
99          try:
100             invalid = eval(python_expression, globals(), locals())
101         except Exception:
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/pip/_vendor/pkg_resources/__init__.py
Line number: 1714
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
1713                code = compile(source, script_filename, 'exec')
1714                exec(code, namespace, namespace)
1715            else:
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/pip/_vendor/pkg_resources/__init__.py
Line number: 1725
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
1724                script_code = compile(script_text, script_filename, 'exec')
1725                exec(script_code, namespace, namespace)
1726
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/pip/_vendor/platformdirs/unix.py
Line number: 182
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
181                     if not Path(path).exists():
182                         path = f"/tmp/runtime-{getuid()}"  # noqa: S108
183                 else:
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/pip/_vendor/pygments/formatters/__init__.py
Line number: 103
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
102             with open(filename, 'rb') as f:
103                 exec(f.read(), custom_namespace)
104             # Retrieve the class `formattername` from that namespace
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/pip/_vendor/pygments/lexers/__init__.py
Line number: 154
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
153             with open(filename, 'rb') as f:
154                 exec(f.read(), custom_namespace)
155             # Retrieve the class `lexername` from that namespace
```

hashlib: Use of weak MD5 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/pip/_vendor/requests/auth.py
Line number: 148
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
147                     x = x.encode("utf-8")
148                 return hashlib.md5(x).hexdigest()
149
```

hashlib: Use of weak SHA1 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/pip/_vendor/requests/auth.py

Line number: 156
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
155                         x = x.encode("utf-8")
156                     return hashlib.sha1(x).hexdigest()
157
```

hashlib: Use of weak SHA1 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/pip/_vendor/requests/auth.py
Line number: 205
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
204
205             cnonce = hashlib.sha1(s).hexdigest()[:16]
206             if _algorithm == "MD5-SESS":
```

blacklist: Deserialization with the marshal module is possibly dangerous.
Test ID: B302
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/pip/_vendor/rich/style.py
Line number: 475
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b302-marshal

```
474             """Get meta information (can not be changed after construction)."""
475             return {} if self._meta is None else cast(Dict[str, Any], loads(self._meta))
476
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/pip/_vendor/urllib3/packages/six.py
Line number: 787
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
786                 _locs_ = _globs_
787             exec ("""exec _code_ in _globs_, _locs_""")
788
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/pkg_resources/__init__.py
Line number: 1738
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
1737                 code = compile(source, script_filename, 'exec')
1738                 exec(code, namespace, namespace)
1739             else:
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/pkg_resources/__init__.py
Line number: 1749
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
1748                 script_code = compile(script_text, script_filename, 'exec')
1749                 exec(script_code, namespace, namespace)
1750
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM

CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/platformdirs/unix.py
Line number: 182
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
181                     if not Path(path).exists():
182                         path = f"/tmp/runtime-{getuid()}"  # noqa: S108
183                 else:
```

hashlib: Use of weak MD5 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/playhouse/migrate.py
Line number: 178
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
177         if len(index_name) > 64:
178             index_hash = hashlib.md5(index_name.encode('utf-8')).hexdigest()
179             index_name = '%s_%s' % (index_name[:56], index_hash[:7])
```

hardcoded_sql_expressions: Possible SQL injection vector through string-based query construction.
Test ID: B608
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-89
File: ./.venv/lib/python3.9/site-packages/playhouse/reflection.py
Line number: 388
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b608_hardcoded_sql_expressions.html

```
387             # Look up the actual column type for each column.
388             cursor = self.execute('SELECT * FROM `%s` LIMIT 1' % table)
389
```

blacklist: Using xml.etree.ElementTree.fromstring to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.ElementTree.fromstring with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called
Test ID: B314
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-20
File: ./.venv/lib/python3.9/site-packages/psutil/_psbsd.py
Line number: 276
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b313-b320-xml-bad-elementtree

```
275                     s = s[: index + 9]
276                     root = ElementTree.fromstring(s)
277                     try:
```

blacklist: Use of insecure and deprecated function (mktemp).
Test ID: B306
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/psutil/tests/__init__.py
Line number: 978
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b306-mktemp-q

```
977         while True:
978             name = tempfile.mktemp(prefix=TESTFN_PREFIX, suffix=suffix, dir=dir)
979             if not os.path.exists(name):  # also include dirs
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/psutil/tests/test_connections.py
Line number: 358
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
357             tcp4_proc = self.pyrun(tcp4_template)
358             tcp4_addr = eval(wait_for_file(testfile, delete=True))
359             udp4_proc = self.pyrun(udp4_template)
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/psutil/tests/test_connections.py
Line number: 360
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
359             udp4_proc = self.pyrun(udp4_template)
360             udp4_addr = eval(wait_for_file(testfile, delete=True))
361             if supports_ipv6():
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/psutil/tests/test_connections.py
Line number: 363
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
362                 tcp6_proc = self.pyrun(tcp6_template)
363                 tcp6_addr = eval(wait_for_file(testfile, delete=True))
364                 udp6_proc = self.pyrun(udp6_template)
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/psutil/tests/test_connections.py
Line number: 365
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
364                 udp6_proc = self.pyrun(udp6_template)
365                 udp6_addr = eval(wait_for_file(testfile, delete=True))
366             else:
```

hardcoded_bind_all_interfaces: Possible binding to all interfaces.
Test ID: B104
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-605
File: ./.venv/lib/python3.9/site-packages/psutil/tests/test_linux.py
Line number: 952
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b104_hardcoded_bind_all_interfaces.html

```
951                         else:
952                             assert get_ipv4_broadcast(name) == '0.0.0.0'
953                     elif addr.family == socket.AF_INET6:
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/psutil/tests/test_misc.py
Line number: 248
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
247                 a = pickle.dumps(ret)
248                 b = pickle.loads(a)
249                 assert ret == b
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/psutil/tests/test_misc.py
Line number: 282
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
281
282             b = pickle.loads(
```

```
283                 pickle.dumps(
284                     psutil.NoSuchProcess(pid=4567, name='name', msg='msg')
285                 )
286             )
287             assert isinstance(b, psutil.NoSuchProcess)
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/psutil/tests/test_misc.py
Line number: 292
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
291
292             b = pickle.loads(
293                 pickle.dumps(
294                     psutil.ZombieProcess(pid=4567, name='name', ppid=42, msg='msg')
295                 )
296             )
297             assert isinstance(b, psutil.ZombieProcess)
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/psutil/tests/test_misc.py
Line number: 303
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
302
303             b = pickle.loads(
304                 pickle.dumps(psutil.AccessDenied(pid=123, name='name', msg='msg'))
305             )
306             assert isinstance(b, psutil.AccessDenied)
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/psutil/tests/test_misc.py
Line number: 311
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
310
311             b = pickle.loads(
312                 pickle.dumps(
313                     psutil.TimeoutExpired(seconds=33, pid=4567, name='name')
314                 )
315             )
316             assert isinstance(b, psutil.TimeoutExpired)
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/py_serializable/__init__.py
Line number: 974
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
973                                 # Will load any class already loaded assuming fully qualified name
974                                 self._type_ = eval(f'{mapped_array_type}[{results.get("array_of")}]')
975                                 self._concrete_type = eval(str(results.get('array_of')))
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/py_serializable/__init__.py
Line number: 975
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
974                                 self._type_ = eval(f'{mapped_array_type}[{results.get("array_of")}]')
975                                 self._concrete_type = eval(str(results.get('array_of')))
976                             except NameError:
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/py_serializable/__init__.py
Line number: 1007
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
1006                                # Will load any class already loaded assuming fully qualified name
1007                                self._type_ = eval(f'{mapped_array_type}[{results.get("array_of")}]')
1008                                self._concrete_type = eval(str(results.get('array_of')))
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/py_serializable/__init__.py
Line number: 1008
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
1007                                self._type_ = eval(f'{mapped_array_type}[{results.get("array_of")}]')
1008                                self._concrete_type = eval(str(results.get('array_of')))
1009                            except NameError:
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/pycparser/ply/cpp.py
Line number: 600
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
599             try:
600                 result = eval(expr)
601             except Exception:
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/pycparser/ply/lex.py
Line number: 215
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
214             else:
215                 exec('import %s' % tabfile)
216                 lextab = sys.modules[tabfile]
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/pycparser/ply/lex.py
Line number: 1039
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
1038                        pkgname = '.'.join(parts[:-1])
1039                        exec('import %s' % pkgname)
1040                        srcfile = getattr(sys.modules[pkgname], '__file__', '')
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/pycparser/ply/yacc.py

Line number: 1562
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
1561                    try:
1562                        c = eval(s)
1563                        if (len(c) > 1):
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/pycparser/ply/yacc.py
Line number: 1982
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
1981            else:
1982                exec('import %s' % module)
1983                parsetab = sys.modules[module]
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/pycparser/ply/yacc.py
Line number: 3254
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
3253                    pkgname = '.'.join(parts[:-1])
3254                    exec('import %s' % pkgname)
3255                    srcfile = getattr(sys.modules[pkgname], '__file__', '')
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/pydantic/deprecated/parse.py
Line number: 54
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
53              bb = b if isinstance(b, bytes) else b.encode()  # type: ignore
54              return pickle.loads(bb)
55          else:
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/pydantic/v1/parse.py
Line number: 42
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
41              bb = b if isinstance(b, bytes) else b.encode()
42              return pickle.loads(bb)
43          else:
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/pydantic/v1/utils.py
Line number: 195
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
194         try:
195             eval('__IPYTHON__')
196         except NameError:
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH

CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/pygments/formatters/__init__.py
Line number: 103
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
102             with open(filename, 'rb') as f:
103                 exec(f.read(), custom_namespace)
104             # Retrieve the class `formattername` from that namespace
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/pygments/lexers/__init__.py
Line number: 154
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
153             with open(filename, 'rb') as f:
154                 exec(f.read(), custom_namespace)
155             # Retrieve the class `lexername` from that namespace
```

blacklist: Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.
Test ID: B310
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/pygments/lexers/_lua_builtins.py
Line number: 225
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b310-urllib-urlopen

```
224         def get_newest_version():
225             f = urlopen('http://www.lua.org/manual/')
226             r = re.compile(r'^<A HREF="(\d\.\d)/">(Lua )?\1</A>')
```

blacklist: Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.
Test ID: B310
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/pygments/lexers/_lua_builtins.py
Line number: 233
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b310-urllib-urlopen

```
232         def get_lua_functions(version):
233             f = urlopen(f'http://www.lua.org/manual/{version}/')
234             r = re.compile(r'^<A HREF="manual.html#pdf-(?!lua|LUA)([^:]+)">\1</A>')
```

blacklist: Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.
Test ID: B310
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/pygments/lexers/_mysql_builtins.py
Line number: 1248
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b310-urllib-urlopen

```
1247            # Pull content from lex.h.
1248            lex_file = urlopen(LEX_URL).read().decode('utf8', errors='ignore')
1249            keywords = parse_lex_keywords(lex_file)
```

blacklist: Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.
Test ID: B310
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/pygments/lexers/_mysql_builtins.py
Line number: 1254
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b310-urllib-urlopen

```
1253            # Parse content in item_create.cc.
1254            item_create_file = urlopen(ITEM_CREATE_URL).read().decode('utf8', errors='ignore')
1255            functions.update(parse_item_create_functions(item_create_file))
```

blacklist: Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.
Test ID: B310

Severity: MEDIUM
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/pygments/lexers/_php_builtins.py
Line number: 3299
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b310-urllib-urlopen

```
3298        def get_php_references():
3299            download = urlretrieve(PHP_MANUAL_URL)
3300            with tarfile.open(download[0]) as tar:
```

tarfile_unsafe_members: tarfile.extractall used without any validation. Please check and discard dangerous members.
Test ID: B202
Severity: HIGH
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/pygments/lexers/_php_builtins.py
Line number: 3301
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b202_tarfile_unsafe_members.html

```
3300            with tarfile.open(download[0]) as tar:
3301                tar.extractall()
3302            yield from glob.glob(f"{PHP_MANUAL_DIR}{PHP_REFERENCE_GLOB}")
```

blacklist: Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.
Test ID: B310
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/pygments/lexers/_postgres_builtins.py
Line number: 642
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b310-urllib-urlopen

```
641         def update_myself():
642             content = urlopen(DATATYPES_URL).read().decode('utf-8', errors='ignore')
643             data_file = list(content.splitlines())
```

blacklist: Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.
Test ID: B310
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/pygments/lexers/_postgres_builtins.py
Line number: 647
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b310-urllib-urlopen

```
646
647             content = urlopen(KEYWORDS_URL).read().decode('utf-8', errors='ignore')
648             keywords = parse_keywords(content)
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/regex/test_regex.py
Line number: 3775
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
3774            p = pickle.dumps(r)
3775            r = pickle.loads(p)
3776            self.assertEqual(r.match('foo').span(), (0, 3))
```

hashlib: Use of weak MD5 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/requests/auth.py
Line number: 148
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
147                         x = x.encode("utf-8")
148                     return hashlib.md5(x).hexdigest()
149
```

hashlib: Use of weak SHA1 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/requests/auth.py
Line number: 156
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
155                         x = x.encode("utf-8")
156                     return hashlib.sha1(x).hexdigest()
157
```

hashlib: Use of weak SHA1 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/requests/auth.py
Line number: 205
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
204
205             cnonce = hashlib.sha1(s).hexdigest()[:16]
206             if _algorithm == "MD5-SESS":
```

blacklist: Deserialization with the marshal module is possibly dangerous.
Test ID: B302
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/rich/style.py
Line number: 475
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b302-marshal

```
474             """Get meta information (can not be changed after construction)."""
475             return {} if self._meta is None else cast(Dict[str, Any], loads(self._meta))
476
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/ruamel/yaml/compat.py
Line number: 151
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
150     nprint = Nprint()
151     nprintf = Nprint('/var/tmp/ruamel.yaml.log')
152
```

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
CWE: CWE-94
File: ./.venv/lib/python3.9/site-packages/safety/alerts/utils.py
Line number: 154
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b701_jinja2_autoescape_false.html

```
153         p = Path(__file__).parent / "templates"
154         env = jinja2.Environment(loader=jinja2.FileSystemLoader(Path(p)))  # type: ignore
155         template = env.get_template("pr.jinja2")
```

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
CWE: CWE-94
File: ./.venv/lib/python3.9/site-packages/safety/alerts/utils.py
Line number: 204
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b701_jinja2_autoescape_false.html

```
203         p = Path(__file__).parent / "templates"
204         env = jinja2.Environment(loader=jinja2.FileSystemLoader(Path(p)))  # type: ignore
205         template = env.get_template("issue.jinja2")
```

hashlib: Use of weak SHA1 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/safety/alerts/utils.py
Line number: 262
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
261         """
262         return hashlib.sha1(
263             b"blob " + str(len(raw_contents)).encode("ascii") + b"\0" + raw_contents
264         ).hexdigest()
265
```

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
CWE: CWE-94
File: ./.venv/lib/python3.9/site-packages/safety/output_utils.py
Line number: 1251
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b701_jinja2_autoescape_false.html

```
1250        file_loader = PackageLoader('safety', 'templates')
1251        env = Environment(loader=file_loader)
1252        template = env.get_template(template)
```

start_process_with_a_shell: Starting a process with a shell, possible injection detected, security issue.
Test ID: B605
Severity: HIGH
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/setuptools/_distutils/command/bdist_rpm.py
Line number: 357
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b605_start_process_with_a_shell.html

```
356
357             out = os.popen(q_cmd)
358             try:
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/setuptools/_distutils/compilers/C/base.py
Line number: 1120
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
1119            expected = '"static", "shared", "dylib", "xcode_stub"'
1120            if lib_type not in eval(expected):
1121                raise ValueError(f"'lib_type' must be {expected}")
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/setuptools/_distutils/core.py
Line number: 268
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
267                     code = f.read().replace(r'\r\n', r'\n')
268                     exec(code, g)
269             finally:
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM

Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/setuptools/_distutils/tests/test_build_ext.py
Line number: 115
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
114                     libz_so = sorted(libz_so, key=lambda lib_path: len(lib_path))
115                     shutil.copyfile(libz_so[-1], '/tmp/libxx_z.so')
116
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/setuptools/_distutils/tests/test_build_ext.py
Line number: 120
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
119                         [xx_c],
120                         library_dirs=['/tmp'],
121                         libraries=['xx_z'],
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/setuptools/_distutils/tests/test_build_ext.py
Line number: 122
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
121                         libraries=['xx_z'],
122                         runtime_library_dirs=['/tmp'],
123                     )
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/setuptools/_distutils/tests/test_build_ext.py
Line number: 145
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
144             if sys.platform == 'linux' and copy_so:
145                 os.unlink('/tmp/libxx_z.so')
146
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/setuptools/_distutils/tests/test_build_ext.py
Line number: 182
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
181                     # Linked against a library in /tmp
182                     assert "/tmp" in rpaths
183                     # The import is the real test here
```

set_bad_file_permissions: Chmod setting a permissive mask 0o777 on file (exe).
Test ID: B103
Severity: HIGH
Confidence: HIGH
CWE: CWE-732
File: ./.venv/lib/python3.9/site-packages/setuptools/_distutils/tests/test_spawn.py
Line number: 32
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b103_set_bad_file_permissions.html

```
31
32              os.chmod(exe, 0o777)
33              with pytest.raises(DistutilsExecError):
```

set_bad_file_permissions: Chmod setting a permissive mask 0o777 on file (exe).
Test ID: B103
Severity: HIGH
Confidence: HIGH
CWE: CWE-732
File: ./.venv/lib/python3.9/site-packages/setuptools/_distutils/tests/test_spawn.py
Line number: 44
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b103_set_bad_file_permissions.html

```
43
44              os.chmod(exe, 0o777)
45              spawn([exe])  # should work without any error
```

blacklist: Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.
Test ID: B310
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/setuptools/_vendor/jaraco/context.py
Line number: 63
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b310-urllib-urlopen

```
62          try:
63              req = urllib.request.urlopen(url)
64              with tarfile.open(fileobj=req, mode='r|*') as tf:
```

tarfile_unsafe_members: tarfile.extractall used without any validation. Please check and discard dangerous members.
Test ID: B202
Severity: HIGH
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/setuptools/_vendor/jaraco/context.py
Line number: 65
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b202_tarfile_unsafe_members.html

```
64              with tarfile.open(fileobj=req, mode='r|*') as tf:
65                  tf.extractall(path=target_dir, filter=strip_first_component)
66              yield target_dir
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/setuptools/_vendor/jaraco/functools/__init__.py
Line number: 522
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
521                     try:
522                         return eval(use)
523                     except TypeError:
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/setuptools/_vendor/packaging/licenses/__init__.py
Line number: 100
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
99          try:
100             invalid = eval(python_expression, globals(), locals())
101         except Exception:
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/setuptools/_vendor/platformdirs/unix.py
Line number: 179
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
178                     if not Path(path).exists():
179                         path = f"/tmp/runtime-{getuid()}"  # noqa: S108
```

```
180                 else:
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/setuptools/build_meta.py
Line number: 317
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
316             try:
317                 exec(code, locals())
318             except SystemExit as e:
```

blacklist: Deserialization with the marshal module is possibly dangerous.
Test ID: B302
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/setuptools/command/bdist_egg.py
Line number: 383
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b302-marshal

```
382         f.read(skip)
383         code = marshal.load(f)
384         f.close()
```

blacklist: Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.
Test ID: B310
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/setuptools/config/_validate_pyproject/formats.py
Line number: 152
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b310-urllib-urlopen

```
151         context = ssl.create_default_context()
152         with urlopen(url, context=context) as response:  # noqa: S310 (audit URLs)
153             headers = Message()
```

blacklist: Deserialization with the marshal module is possibly dangerous.
Test ID: B302
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/setuptools/depends.py
Line number: 133
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b302-marshal

```
132                     f.read(8)  # skip magic & date
133                     code = marshal.load(f)
134                 elif kind == PY_FROZEN:
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/setuptools/launch.py
Line number: 32
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
31          code = compile(norm_script, script_name, 'exec')
32          exec(code, namespace)
33
```

blacklist: Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.
Test ID: B310
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/setuptools/tests/config/downloads/__init__.py
Line number: 53
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b310-urllib-urlopen

```
52      def download(url: str, dest: Path):
53          with urlopen(url) as f:
54              data = f.read()
```

subprocess_popen_with_shell_equals_true: subprocess call with shell=True identified, security issue.
Test ID: B602
Severity: HIGH
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/setuptools/tests/environment.py
Line number: 77
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b602_subprocess_popen_with_shell_equals_true.html

```
76                  stderr=_PIPE,
77                  shell=shell,
78                  env=env,
79                  encoding="utf-8",
80              )
81
82              if isinstance(data_stream, tuple):
83                  data_stream = slice(*data_stream)
84              data = proc.communicate()[data_stream]
85          except OSError:
```

blacklist: Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.
Test ID: B310
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/setuptools/tests/integration/test_pip_install_sdist.py
Line number: 174
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b310-urllib-urlopen

```
173         id_ = package if version is LATEST else f"{package}/{version}"
174         with urlopen(f"https://pypi.org/pypi/{id_}/json") as f:
175             metadata = json.load(f)
```

blacklist: Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.
Test ID: B310
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/setuptools/tests/integration/test_pip_install_sdist.py
Line number: 187
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b310-urllib-urlopen

```
186     def download(url, dest, md5_digest):
187         with urlopen(url) as f:
188             data = f.read()
```

hashlib: Use of weak MD5 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.9/site-packages/setuptools/tests/integration/test_pip_install_sdist.py
Line number: 190
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
189
190         assert md5(data).hexdigest() == md5_digest
191
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/setuptools/tests/test_editable_install.py
Line number: 449
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
448             loc = {}
449             exec(finder, loc, loc)
450             loc["install"]()
```

blacklist: Pickle and modules that wrap it can be unsafe when used to deserialize untrusted data, possible security issue.
Test ID: B301
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-502
File: ./.venv/lib/python3.9/site-packages/setuptools/tests/test_extern.py
Line number: 15
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b301-pickle

```
14      def test_distribution_picklable():
15          pickle.loads(pickle.dumps(Distribution()))
```

blacklist: Audit url open for permitted schemes. Allowing use of file:/ or custom schemes is often unexpected.
Test ID: B310
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-22
File: ./.venv/lib/python3.9/site-packages/setuptools/tests/test_virtualenv.py
Line number: 33
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b310-urllib-urlopen

```
32              try:
33                  urlopen('https://pypi.org', timeout=1)
34              except URLError:
```

set_bad_file_permissions: Chmod setting a permissive mask 0o777 on file (runsh).
Test ID: B103
Severity: HIGH
Confidence: HIGH
CWE: CWE-732
File: ./.venv/lib/python3.9/site-packages/setuptools/tests/test_wheel.py
Line number: 626
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b103_set_bad_file_permissions.html

```
625                 runsh = pathlib.Path(source_dir) / "script.sh"
626                 os.chmod(runsh, 0o777)
627                 subprocess.check_call(
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/setuptools/wheel.py
Line number: 211
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
210                         raw_req,
211                         (req for req in reqs if for_extra(req) and eval(req, extra=extra)),
212                     )
```

hardcoded_tmp_directory: Probable insecure usage of temp file/directory.
Test ID: B108
Severity: MEDIUM
Confidence: MEDIUM
CWE: CWE-377
File: ./.venv/lib/python3.9/site-packages/stevedore/tests/test_cache.py
Line number: 29
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b108_hardcoded_tmp_directory.html

```
28              """
29              with mock.patch.object(sys, 'executable', '/tmp/fake'):
30                  sot = _cache.Cache()
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/tqdm/cli.py
Line number: 38
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
37              if re.match(r"^\\\w+$", val):
38                  return eval(f'"{val}"').encode()
39              raise TqdmTypeError(f"{val} : {typ}")
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/typing_extensions.py
Line number: 4034
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
4033            return_value = {key:
4034                value if not isinstance(value, str) else eval(value, globals, locals)
4035                for key, value in ann.items() }
```

blacklist: Use of possibly insecure function - consider using safer ast.literal_eval.
Test ID: B307
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/typing_extensions.py
Line number: 4116
More info: https://bandit.readthedocs.io/en/1.8.6/blacklists/blacklist_calls.html#b307-eval

```
4115                code = forward_ref.__forward_code__
4116                value = eval(code, globals, locals)
4117            forward_ref.__forward_evaluated__ = True
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/typing_inspection/typing_objects.py
Line number: 101
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
100         globals_: dict[str, Any] = {'Any': Any, 'typing': typing, 'typing_extensions': typing_extensions}
101         exec(func_code, globals_, locals_)
102         return locals_[function_name]
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/typing_inspection/typing_objects.py
Line number: 133
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
132         globals_: dict[str, Any] = {'Any': Any, 'typing': typing, 'typing_extensions': typing_extensions}
133         exec(func_code, globals_, locals_)
134         return locals_[function_name]
```

exec_used: Use of exec detected.
Test ID: B102
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-78
File: ./.venv/lib/python3.9/site-packages/wrapt/decorators.py
Line number: 23
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b102_exec_used.html

```
22                  _locs_ = _globs_
23              exec("""exec _code_ in _globs_, _locs_""")
24
```