Metrics:

Total lines of code: 123039
Total lines skipped (#nosec): 0

Skipped files:

./server_mesh.py **reason:** syntax error while parsing AST from 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/python3.13/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/python3.13/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
```

blacklist: Use of insecure MD2, MD4, MD5, or SHA1 hash function.
Test ID: B303
Severity: MEDIUM
Confidence: HIGH
CWE: CWE-327
File: ./.venv/lib/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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
```

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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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
```

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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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/python3.13/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__', '')
```

hashlib: Use of weak SHA1 hash for security. Consider usedforsecurity=False
Test ID: B324
Severity: HIGH
Confidence: HIGH
CWE: CWE-327
File: ./ws.py
Line number: 8
More info: https://bandit.readthedocs.io/en/1.8.6/plugins/b324_hashlib.html

```
7           import hashlib
8           return hashlib.sha1(data).digest()
9
```