攻防世界 WEB题 cat writeup

原创

一个脐橙 于 2019-10-25 20:37:12 发布

文章标签： web ctf

本文链接：https://blog.csdn.net/qq_45139955/article/details/102749594

攻防世界 WEB题 cat writeup

打开题目

打开题目

Cloud Automated Testing

输入你的域名，例如：loli.club

Submit

输入baidu.com

Cloud Automated Testing

输入你的域名，例如：loli.club

baidu.com Submit

页面毫无反应，但是发现，输入百度的ip时，有不一样

Cloud Automated Testing

输入你的域名，例如：loli.club

220.181.38.148 Submit

```
PING 220.181.38.148 (220.181.38.148) 56(84) bytes of data.

--- 220.181.38.148 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```


页面执行了ping命令并返回，说明页面有命令执行的功能，想到尝试命令拼接执行和使用管道进行命令执行

输入你的域名，例如：loli.club

220.181.38.148 & ls Submit

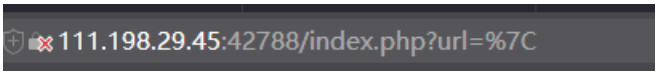
```
Invalid URL
```

输入你的域名，例如：loli.club

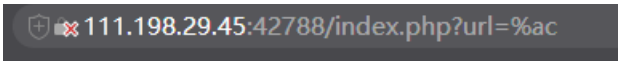
220.181.38.148 | ls Submit

```
Invalid URL
```

发现都报错，应该是系统对字符进行了过滤
输入 | 发现被编码成了%7c



尝试宽字节输入，将7改为a



提交

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta http-equiv="content-type" content="text/html; charset=utf-8">
  <meta name="robots" content="NONE,NOARCHIVE">
  <title>UnicodeEncodeError at /api/ping</title>
  <style type="text/css">
    html * { padding:0; margin:0; }
    body * { padding:10px 20px; }
    body * * { padding:0; }
    body { font:small sans-serif; }
    body>div { border-bottom:1px solid #ddd; }
    h1 { font-weight:normal; }
    h2 { margin-bottom:.8em; }
    h2 span { font-size:80%; color:#666; font-weight:normal; }
    h3 { margin:1em 0 .5em 0; }
    h4 { margin:0 0 .5em 0; font-weight: normal; }
    code, pre { font-size: 100%; white-space: pre-wrap; }
    table { border:1px solid #ccc; border-collapse: collapse; width:100%; background:white; }
    tbody td, tbody th { vertical-align:top; padding:2px 3px; }
    thead th {
      padding:1px 6px 1px 3px; background:#fefefe; text-align:left;
      font-weight:normal; font-size:11px; border:1px solid #ddd;
    }
    tbody th { width:12em; text-align:right; color:#666; padding-right:.5em; }
    table.vars { margin:5px 0 2px 40px; }
    table.vars td, table.req td { font-family:monospace; }
    table td.code { width:100%; }
    table td.code pre { overflow:hidden; }
    table.source th { color:#666; }
    table.source td { font-family:monospace; white-space:pre; border-bottom:1px solid #eee; }
    ul.traceback { list-style-type:none; color: #222; }
    ul.traceback li.frame { padding-bottom:1em; color:#666; }
    ul.traceback li.user { background-color:#e0e0e0; color:#000 }
    div.context { padding:10px 0; overflow:hidden; }
    div.context ol { padding-left:30px; margin:0 10px; list-style-position: inside; }
    div.context ol li { font-family:monospace; white-space:pre; color:#777; cursor:pointer; padding-left: 2px; }
    div.context ol li pre { display:inline; }
    div.context ol.context-line li { color:#505050; background-color:#dfdfdf; padding: 3px 2px; }
    div.context ol.context-line li span { position:absolute; right:32px; }
    .user div.context ol.context-line li { background-color:#bbb; color:#000; }
    .user div.context ol li { color:#666; }
    div.commands { margin-left: 40px; }
    div.commands a { color:#555; text-decoration:none; }
    .user div.commands a { color: black; }
```


页面报错，复制下来，打开，发现是django报错页面

UnicodeEncodeError at /api/ping

'gbk' codec can't encode character u'\ufffd' in position 0: illegal multibyte sequence

Request Method:	POST
Request URL:	http://127.0.0.1:8000/api/ping
Django Version:	1.10.4
Exception Type:	UnicodeEncodeError
Exception Value:	'gbk' codec can't encode character u'\ufffd' in position 0: illegal multibyte sequence
Exception Location:	/opt/api/dnsapi/utils.py in escape, line 9
Python Executable:	/usr/bin/python
Python Version:	2.7.12
Python Path:	['/opt/api', '/usr/lib/python2.7', '/usr/lib/python2.7/plat-x86_64-linux-gnu', '/usr/lib/python2.7/lib-tk', '/usr/lib/python2.7/lib-old', '/usr/lib/python2.7/lib-dynload', '/usr/local/lib/python2.7/dist-packages', '/usr/lib/python2.7/dist-packages']
Server time:	Fri, 25 Oct 2019 12:06:32 +0000

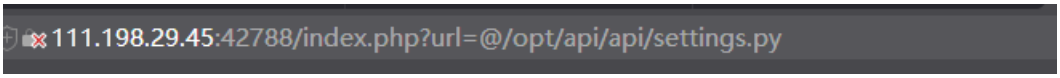
Unicode error hint

The string that could not be encoded/decoded was: ﷽

Traceback Switch to copy-and-paste view

发现文件的绝对路径是/opt/api

接下来就是django的基础知识了：django项目下一般有个settings.py文件是设置网站数据库路径且django项目生成时settings.py会存放在以项目目录下再以项目名称命名的文件夹下面，查看settings.py




```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta http-equiv="content-type" content="text/html; charset=utf-8">
  <meta name="robots" content="NONE,NOARCHIVE">
  <title>UnicodeDecodeError at /api/ping</title>
  <style type="text/css">
    html * { padding:0; margin:0; }
    body * { padding:10px 20px; }
    body * * { padding:0; }
    body { font:small sans-serif; }
    body>div { border-bottom:1px solid #ddd; }
    h1 { font-weight:normal; }
    h2 { margin-bottom:.8em; }
    h2 span { font-size:80%; color:#666; font-weight:normal; }
    h3 { margin:1em 0 .5em 0; }
    h4 { margin:0 0 .5em 0; font-weight: normal; }
    code, pre { font-size: 100%; white-space: pre-wrap; }
    table { border:1px solid #ccc; border-collapse: collapse; width:100%; background:white; }
    tbody td, tbody th { vertical-align:top; padding:2px 3px; }
    thead th {
      padding:1px 6px 1px 3px; background:#fefefe; text-align:left;
      font-weight:normal; font-size:11px; border:1px solid #ddd;
    }
    tbody th { width:12em; text-align:right; color:#666; padding-right:.5em; }
    table.vars { margin:5px 0 2px 40px; }
    table.vars td, table.req td { font-family:monospace; }
    table td.code { width:100%; }
    table td.code pre { overflow:hidden; }
    table.source th { color:#666; }
    table.source td { font-family:monospace; white-space:pre; border-bottom:1px solid #eee; }
    ul.traceback { list-style-type:none; color: #222; }
    ul.traceback li.frame { padding-bottom:1em; color:#666; }
    ul.traceback li.user { background-color:#e0e0e0; color:#000 }
    div.context { padding:10px 0; overflow:hidden; }
    div.context ol { padding-left:30px; margin:0 10px; list-style-position: inside; }
    div.context ol li { font-family:monospace; white-space:pre; color:#777; cursor:pointer; padding-left: 2px; }
    div.context ol li pre { display:inline; }
    div.context ol.context-line li { color:#505050; background-color:#dfdfdf; padding: 3px 2px; }
    div.context ol.context-line li span { position:absolute; right:32px; }
    .user div.context ol.context-line li { background-color:#bbb; color:#000; }
    .user div.context ol li { color:#666; }
```


同样，以html文件打开，通过观察发现敏感信息

```
CACHE_MIDDLEWARE_SECONDS          600
CSRF_COOKIE_AGE                   31449600
CSRF_COOKIE_DOMAIN                None
CSRF_COOKIE_HTTPONLY              False
CSRF_COOKIE_NAME                  u'csrftoken'
CSRF_COOKIE_PATH                  u'/'
CSRF_COOKIE_SECURE                False
CSRF_FAILURE_VIEW                 u'django.views.csrf.csrf_failure'
CSRF_HEADER_NAME                  u'HTTP_X_CSRFTOKEN'
CSRF_TRUSTED_ORIGINS              []
DATABASES                         {'default': {'ATOMIC_REQUESTS': False,
                                               'AUTOCOMMIT': True,
                                               'CONN_MAX_AGE': 0,
                                               'ENGINE': 'django.db.backends.sqlite3',
                                               'HOST': '',
                                               'NAME': '/opt/api/database.sqlite3',
                                               'OPTIONS': {},
                                               'PASSWORD': u'********************',
                                               'PORT': '',
                                               'TEST': {'CHARSET': None,
                                                        'COLLATION': None,
                                                        'MIRROR': None,
                                                        'NAME': None},
                                               'TIME_ZONE': None,
                                               'USER': ''}}
DATABASE_ROUTERS                  []
DATA_UPLOAD_MAX_MEMORY_SIZE       2621440
DATA_UPLOAD_MAX_NUMBER_FIELDS     1000
```


查看该文件

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta http-equiv="content-type" content="text/html; charset=utf-8">
  <meta name="robots" content="NONE,NOARCHIVE">
  <title>UnicodeDecodeError at /api/ping</title>
  <style type="text/css">
    html * { padding:0; margin:0; }
    body * { padding:10px 20px; }
    body * * { padding:0; }
    body { font:small sans-serif; }
    body>div { border-bottom:1px solid #ddd; }
    h1 { font-weight:normal; }
    h2 { margin-bottom:.8em; }
    h2 span { font-size:80%; color:#666; font-weight:normal; }
    h3 { margin:1em 0 .5em 0; }
    h4 { margin:0 0 .5em 0; font-weight: normal; }
    code, pre { font-size: 100%; white-space: pre-wrap; }
    table { border:1px solid #ccc; border-collapse: collapse; width:100%; background:white; }
    tbody td, tbody th { vertical-align:top; padding:2px 3px; }
    thead th {
      padding:1px 6px 1px 3px; background:#fefefe; text-align:left;
      font-weight:normal; font-size:11px; border:1px solid #ddd;
    }
    tbody th { width:12em; text-align:right; color:#666; padding-right:.5em; }
    table.vars { margin:5px 0 2px 40px; }
    table.vars td, table.req td { font-family:monospace; }
    table td.code { width:100%; }
    table td.code pre { overflow:hidden; }
    table.source th { color:#666; }
    table.source td { font-family:monospace; white-space:pre; border-bottom:1px solid #eee; }
    ul.traceback { list-style-type:none; color: #222; }
    ul.traceback li.frame { padding-bottom:1em; color:#666; }
    ul.traceback li.user { background-color:#e0e0e0; color:#000 }
    div.context { padding:10px 0; overflow:hidden; }
    div.context ol { padding-left:30px; margin:0 10px; list-style-position: inside; }
    div.context ol li { font-family:monospace; white-space:pre; color:#777; cursor:pointer; padding-left: 2px; }
```


在报错信息中查找ctf，得到flag