

# 7.正则抓取页面内容

原创

[E1even](#) 于 2021-07-30 14:12:04 发布 92 收藏 1

分类专栏: [通讯协议学习](#)

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/weixin\\_51353029/article/details/119246498](https://blog.csdn.net/weixin_51353029/article/details/119246498)

版权



[通讯协议学习](#) 专栏收录该内容

8 篇文章 0 订阅

订阅专栏

## 文章目录

请求方法:

GET请求:

POST请求:

二者之间的区别:

GET爬取xazlsec.com页面内容:

POST爬取页面信息:

用脚本爬取页面内容:

正则匹配:

元字符 (参见 python 模块 re 文档):

贪婪匹配与非贪婪匹配:

爬取xazlsec.com中存在的域名结果:

## 请求方法:

因为自己这一块是有基础得, 所以下面简单讲解一下请求方法:

### GET请求:

GET方法:

用于使用给定的URI从给定服务器中检索信息, 即从指定资源中请求数据。使用GET方法的请求应该只是检索数据, 并且不应对数据产生其他影响。

单纯跳转页面得请求: `xazlsrc.com/index.php` `xazlsrc.com/login.php`, 即直接在url后面加上要访问得页面名称即可

传值得请求: 例如某登录界面: `xazlsrc.com/?username=1&passwd=2`

说明: GET请求是可以缓存的, 我们可以从浏览器历史记录中查找到GET请求, 还可以把它收藏到书签中; 且GET请求有长度限制, 仅用于请求数据 (不修改)。

注：因GET请求的不安全性，在处理敏感数据时，绝不可以使用GET请求,比如当我们登录一个界面得时候，出现以下情况：

url:www.xazlsrc.com/login.php?id=guest(这是我们得正常的普通客户访问)

如果我们更改以下url:

url:www.xazlsrc.com/login.php?id=admin(那就可以直接admin登录)

因此url里面不能存在敏感信息，不然安全性不高

## POST请求：

POST方法：

POST方法用于将数据发送到服务器以创建或更新资源，它要求服务器确认请求中包含的内容作为由URI区分的Web资源的另一个下属。

POST请求永远不会被缓存，且对数据长度没有限制；我们无法从浏览器历史记录中查找到POST请求

post请求安全性相对来说会更高一点

## 二者之间的区别：

1. GET请求在URL中传送的参数是有长度限制的，而POST没有。
2. GET比POST更不安全，因为参数直接暴露在URL上，所以不能用来传递敏感信息。而POST数据不会显示在URL中。是放在Request body中。
3. 对参数的数据类型，GET只接受ASCII字符，而POST没有限制。
4. GET请求参数会被完整保留在浏览器历史记录里；相反，POST请求参数也不会被浏览器保留。
5. GET请求只能进行url编码（application/x-www-form-urlencoded），而POST支持多种编码方式。
6. GET请求会被浏览器主动缓存，而POST不会，除非手动设置。
7. GET在浏览器回退时是无害的，而POST会再次提交请求。

其他说明：这两种请求方式是最常见的请求方式，还有HEAD,PUT等等请求方式，传参方式除了get和post，还有cookie传参等等方式

## GET爬取xazlsec.com页面内容：

```
import requests
url=' https://www.xazlsec.com'
res=requests.get(url)
#print(res.headers) 返回头部信息
#print(res.cookies) 返回cookies信息
#print(res.status_code) 返回状态码
#print(res.text) 返回编译之后的文本信息
#print(res.url) 返回url
#print(res.content) 字节码
#print(res.encoding) #content中间存的是字节码，而text中存的是Beautifulsoup根据猜测的编码方式将content内容编码成字符串。
result=res.text
print(result)
```

## POST爬取页面信息：

```
import requests

url='http://xazlsec.com'
post_data={
    " ":" " #这里提交POST的内容，常见的账号密码提交应该如此输入： {"username":"admin","passwd":"123456"}
}
res=requests.post(url,data=post_data)
print(res.text)
```

#必要时需要对post\_data进行json解析再传入，对于提交json串，主要是用于发送ajax请求中，动态加载数据。以拼多多网站为例，加载商品的方式为ajax，商品的内容在响应中。

#所以此时应这样请求：`res = requests.post(url=url,data =json.dumps(post_data))`

## 用脚本爬取页面内容：

既然是要爬取页面内容，那我更倾向于用request模块进行爬取,直接看代码：

```
import requests
import re
url=' https://www.xazlsec.com'
res=requests.get(url)
#print(res.headers)
#print(res.cookies)
#print(res.status_code)
#print(res.text)
#print(res.url)
#print(res.content)
#print(res.encoding) #content中间存的是字节码，而text中存的是Beautifulsoup根据猜测的编码方式将content内容编码成字符串。
result=res.text
sul=re.findall(r"http://.*?\\"|http://.*?\\"|https://.*?\\"", result)
for line in sul:
    try:
        print(line)
    except:
        print('no')
    pass
```

这里要用到RE模块，因为re模块可以使用正则匹配函数

## 正则匹配：

python的正则匹配或者说 php语言的正则匹配，都有极大的相似之处，一开始自己刚看正则匹配的时候还什么也看不懂，后面多学学就好了，下面讲解一下：

个人认为最重要的是元字符：

## 元字符（参见 python 模块 re 文档）：

.	匹配任意字符（不包括换行符）
^	匹配开始位置，多行模式下匹配每一行的开始
\$	匹配结束位置，多行模式下匹配每一行的结束
*	匹配前一个元字符0到多次
+	匹配前一个元字符1到多次
?	匹配前一个元字符0到1次
{m,n}	匹配前一个元字符m到n次
\\	转义字符，跟在其后的字符将失去作为特殊元字符的含义，例如\\.只能匹配.，不能再匹配任意字符
[]	字符集，一个字符的集合，可匹配其中任意一个字符
	逻辑表达式 或，比如 a b 代表可匹配 a 或者 b
(...)	分组，默认为捕获，即被分组的内容可以被单独取出，默认每个分组有个索引，从 1 开始，按照 "(" 的顺序决定索引值
(?iLmsux)	分组中可以设置模式，iLmsux之中的每个字符代表一个模式,用法参见 模式 I
(?:...)	分组的不捕获模式，计算索引时会跳过这个分组
(?P<name>...)	分组的命名模式，取此分组中的内容时可以使用索引也可以使用name
(?P=name)	分组的引用模式，可在同一个正则表达式用引用前面命名过的正则
(?#...)	注释，不影响正则表达式其它部分,用法参见 模式 I
(?=...)	顺序肯定环视，表示所在位置右侧能够匹配括号内正则
(?!...)	顺序否定环视，表示所在位置右侧不能匹配括号内正则
(<=...)	逆序肯定环视，表示所在位置左侧能够匹配括号内正则
(<!...)	逆序否定环视，表示所在位置左侧不能匹配括号内正则
(?(id/name)yes no)	若前面指定id或name的分区匹配成功则执行yes处的正则，否则执行no处的正则
\number	匹配和前面索引为number的分组捕获到的内容一样的字符串
\A	匹配字符串开始位置，忽略多行模式
\Z	匹配字符串结束位置，忽略多行模式
\b	匹配位于单词开始或结束位置的空字符串
\B	匹配不位于单词开始或结束位置的空字符串
\d	匹配一个数字，相当于 [0-9]
\D	匹配非数字,相当于 [^0-9]
\s	匹配任意空白字符，相当于 [ \t\n\r\f\v]
\S	匹配非空白字符，相当于 [^ \t\n\r\f\v]
\w	匹配数字、字母、下划线中任意一个字符，相当于 [a-zA-Z0-9_]
\W	匹配非数字、字母、下划线中的任意字符，相当于 [^a-zA-Z0-9_]

以上为元字符：

我们简单看看元字符的使用：

```
re.findall("^w+",str) : ^表示多行匹配 \w表示匹配字母数字下划线任意一个字符
re.findall("."+str): .表示匹配任意，不受换行符等字符的限制，因此所有内容都可以匹配
后面的+号表示尽可能多的进行匹配，即下面要讲解的贪婪匹配
前面表示我们的匹配规则，后面表示我们要匹配的字符串
```

### 贪婪匹配与非贪婪匹配：

那么元字符的正则匹配更像是一套规则，里面规定了匹配的方式，对于我们想要匹配的特定的信息，用上面的元字符肯定是不可取的，因此下面我们将采用非贪婪模式的方式进行内容匹配：

```
example = "abbbbbbc"
pattern = re.compile("ab+")
```

这里匹配到的就是 abbbbbbc

这就是贪婪匹配，尽可能多的匹配ab开头的字符串

如果我们要进行非贪婪匹配，应该怎么匹配呢？：

*	允许前一个字符可以出现0次或者无限次
+	前一个字符至少出现1次
?	前一个字符只能出现一次或者不出现
{m}	允许前一个字符只能出现m次
{m,n}	允许前一个字符至少出现m次,最多出现n次(如果不写n, 则代表至少出现m次)

这是

python非贪婪模式的量词使用

具体使用情况如下：

```
import re

example = "<div>test1</div><div>test2</div>"

res1 = re.compile("<div>.*</div>")
res2 = re.compile("<div>.*?</div>")
```

输出内容：

```
res1=<div>test1</div><div>test2</div>
res2=<div>test1</div>
```

这就是区别，想必看完了实例，应该能够理解贪婪匹配与非贪婪匹配了吧

那么我在使用非贪婪匹配来匹配写脚本爬取xazlsec.com存在域名的时候，使用到的正则匹配是怎么样的呢？：

```
url=re.findall(r"http://.*?\\"|http://.*?\\"|https://.*?\\"", result)
```

很显然，对里面存在的http或者https开头的字符串进行匹配，匹配到第一个存在的"位置（因为写代码的时候肯定会用""对网址进行包裹），而我这里为什么要用?呢，因为防止不恰当的内容出现，给出错误示例图就清楚了：

```
https://www.xazlsec.com/index.php/archives/1259/">两周面试心得总结</a></li><li class="list-group-item clearfix"><a href="https://www.xazlsec.com/index.php/archives/1258/">努力学习还是为了更好的生活</a></li><li class="list-group-item clearfix"><a href="https://www.xazlsec.com/index.php/archives/1257/">提升技术光看还不够还要动手</a></li><li class="list-group-item clearfix"><a href="https://www.xazlsec.com/index.php/archives/1255/">聊一聊个人成长这些事</a></li><li class="list-group-item clearfix"><a href="https://www.xazlsec.com/index.php/archives/1247/">突破封闭 Web 系统的技巧之正面冲锋</a></li><li class="list-group-item clearfix"><a href="https://www.xazlsec.com/index.php/archives/1246/">Cobalt Strike 初体验</a></li><li class="list-group-item clearfix"><a href="https://www.xazlsec.com/index.php/archives/145/">wifi 杀手</a></li><li class="list-group-item clearfix"><a href="https://www.xazlsec.com/index.php/archives/1244/">罕见的远程执行命令方式整理</a></li><li class="list-group-item clearfix"><a href="https://www.xazlsec.com/index.php/archives/1243/">https://www.xazlsec.com/index.php/archives/1168/" title="记一次详细的勒索病毒分析">记一次详细的勒索病毒分析</a></li><li class="list-group-item clearfix"><a href="https://www.xazlsec.com/index.php/archives/1109/" title="如果是你，你对信安之路会有哪些期望">如果是你，你对信安之路会有哪些期望</a></li><li class="list-group-item clearfix"><a href="https://www.xazlsec.com/index.php/archives/1018/" title="iOS12 越狱漏洞分析">iOS12-2 越狱漏洞分析</a></li><li class="list-group-item clearfix"><a href="https://www.xazlsec.com/index.php/archives/64/" title="Splunk学习与实践">Splunk学习与实践</a></li><li class="list-group-item clearfix"><a href="https://www.xazlsec.com/index.php/archives/985/" title="低成本轻松实现移动式钓鱼 Wifi 网络">低成本轻松实现移动式钓鱼 Wifi 网络</a></li><li class="list-group-item clearfix"><a href="https://www.xazlsec.com/index.php/archives/1071/" title="微信PC端技术研究(3)-如何找到消息发送接口">微信PC端技术研究(3)-如何找到消息发送接口</a></li><li class="list-group-item clearfix"><a href="https://www.xazlsec.com/index.php/archives/1095/" title="RedTeam 技巧集合">RedTeam 技巧集合</a></li><li class="list-group-item clearfix"><a href="https://www.xazlsec.com/index.php/archives/1184/" title="揭露某些所谓"大佬"不为人知的另一面">揭露某些所谓"大佬"不为人知的另一面</a></li><li class="list-group-item clearfix"><a href="https://www.xazlsec.com/index.php/archives/997/" title="从零开始打造一款简单的 apache module 后门">从零开始打造一款简单的 apache module 后门</a></li><li class="list-group-item clearfix"><a href="https://www.xazlsec.com/index.php/archives/1094/" title="轻松了解 web 日志分析过程">轻松了解 web 日志分析过程</a></li>
```

根据图中的标记可以看到的确满足了我们https开头 匹配到“结束，但是内容如此之多，肯定不是我们最初想要的结果，所以，为了防止出现这种情况的出现，我们一定要使用两次：？，即：https://.\*?" (是转义符号)

### 爬取xazlsec.com中存在的域名结果：

```
https://www.xazlsec.com/usr/themes/default/favicon.ico"
https://www.xazlsec.com/usr/themes/default/css/bootstrap.min.css"
https://www.xazlsec.com/usr/themes/default/css/font-awesome.min.css"
https://www.xazlsec.com/usr/themes/default/css/main.css"
https://www.xazlsec.com/index.php/feed/"
https://www.xazlsec.com/index.php/feed/rss/"
https://www.xazlsec.com/index.php/feed/atom/"
https://www.xazlsec.com/"
https://www.xazlsec.com/usr/uploads/2019/05/1025297443.png"
https://www.xazlsec.com/"
https://www.xazlsec.com/usr/uploads/2019/05/1025297443.png"
https://www.xazlsec.com/"
https://www.xazlsec.com/index.php/1276.html"
https://www.xazlsec.com/index.php/1272.html"
https://www.xazlsec.com/index.php/923.html"
https://www.xazlsec.com/index.php/941.html"
https://www.xazlsec.com/index.php/166.html"
https://www.xazlsec.com/index.php/918.html"
https://www.xazlsec.com/index.php/109.html"
https://www.xazlsec.com/index.php/921.html"
https://www.xazlsec.com/index.php/73.html"
https://www.xazlsec.com/index.php/942.html"
https://www.xazlsec.com/"
https://www.xazlsec.com/index.php/archives/1271/"
https://www.xazlsec.com/index.php/archives/1271/"
https://www.xazlsec.com/index.php/archives/1271/"
https://www.xazlsec.com/index.php/author/1/"
https://www.xazlsec.com/index.php/archives/1271/#comments"
https://www.xazlsec.com/index.php/category/czjy/"
https://www.xazlsec.com/index.php/archives/1259/"
https://www.xazlsec.com/index.php/archives/1259/"
https://www.xazlsec.com/index.php/archives/1259/"
https://www.xazlsec.com/index.php/author/1/"
https://www.xazlsec.com/index.php/archives/1259/#comments"
https://www.xazlsec.com/index.php/category/czjy/"
https://www.xazlsec.com/index.php/archives/1258/"
https://www.xazlsec.com/index.php/archives/1258/"
https://www.xazlsec.com/index.php/archives/1258/"
https://www.xazlsec.com/index.php/author/1/"
https://www.xazlsec.com/index.php/archives/1258/#comments"
https://www.xazlsec.com/index.php/category/czjy/"
https://www.xazlsec.com/index.php/archives/1257/"
https://www.xazlsec.com/index.php/archives/1257/"
https://www.xazlsec.com/index.php/archives/1257/"
https://www.xazlsec.com/index.php/author/1/"
https://www.xazlsec.com/index.php/archives/1257/#comments"
https://www.xazlsec.com/index.php/category/czjy/"
https://www.xazlsec.com/index.php/archives/1255/"
https://www.xazlsec.com/index.php/archives/1255/"
https://www.xazlsec.com/index.php/archives/1255/"
https://www.xazlsec.com/index.php/author/1/"
https://www.xazlsec.com/index.php/archives/1255/#comments"
https://www.xazlsec.com/index.php/page/1/"
https://www.xazlsec.com/index.php/page/2/"
https://www.xazlsec.com/index.php/page/3/"
```

https://www.xazlsec.com/index.php/page/3/  
https://www.xazlsec.com/index.php/page/4/"  
https://www.xazlsec.com/index.php/page/76/"  
https://www.xazlsec.com/index.php/page/2/"  
https://www.xazlsec.com/index.php/archives/1271/"  
https://www.xazlsec.com/index.php/archives/1259/"  
https://www.xazlsec.com/index.php/archives/1258/"  
https://www.xazlsec.com/index.php/archives/1257/"  
https://www.xazlsec.com/index.php/archives/1255/"  
https://www.xazlsec.com/index.php/archives/1247/"  
https://www.xazlsec.com/index.php/archives/1246/"  
https://www.xazlsec.com/index.php/archives/1245/"  
https://www.xazlsec.com/index.php/archives/1244/"  
https://www.xazlsec.com/index.php/archives/1243/"  
https://www.xazlsec.com/index.php/archives/685/"  
https://www.xazlsec.com/index.php/archives/1032/"  
https://www.xazlsec.com/index.php/archives/1005/"  
https://www.xazlsec.com/index.php/archives/1236/"  
https://www.xazlsec.com/index.php/archives/1171/"  
https://www.xazlsec.com/index.php/archives/1177/"  
https://www.xazlsec.com/index.php/archives/1204/"  
https://www.xazlsec.com/index.php/archives/1258/"  
https://www.xazlsec.com/index.php/archives/1118/"  
https://www.xazlsec.com/index.php/archives/882/"  
https://edu.xazlsec.com"  
https://tools.xazlsec.com"  
https://www.xazlsec.com/index.php/category/pentest/"  
https://www.xazlsec.com/index.php/category/yunweise/"  
https://www.xazlsec.com/index.php/category/websec/"  
https://www.xazlsec.com/index.php/category/networksec/"  
https://www.xazlsec.com/index.php/category/sectools/"  
https://www.xazlsec.com/index.php/category/ctf/"  
https://www.xazlsec.com/index.php/category/yewusec/"  
https://www.xazlsec.com/index.php/category/WiFi/"  
https://www.xazlsec.com/index.php/category/appsec/"  
https://www.xazlsec.com/index.php/category/codereview/"  
https://www.xazlsec.com/index.php/category/dujia/"  
https://www.xazlsec.com/index.php/category/czjy/"  
https://www.xazlsec.com/index.php/category/jianshe/"  
https://www.xazlsec.com/index.php/category/apt/"  
https://www.xazlsec.com/index.php/category/yingji/"  
https://www.xazlsec.com/index.php/category/bin/"  
https://www.xazlsec.com/index.php/category/bingdu/"  
https://www.xazlsec.com/index.php/tag/%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95/"  
https://www.xazlsec.com/index.php/tag/linux/"  
https://www.xazlsec.com/index.php/tag/Windows/"  
https://www.xazlsec.com/index.php/tag/ctf/"  
https://www.xazlsec.com/index.php/tag/%E4%BF%A1%E6%81%AF%E6%94%B6%E9%9B%86/"  
https://www.xazlsec.com/index.php/tag/%E5%AE%89%E5%85%A8%E5%B7%A5%E5%85%B7/"  
https://www.xazlsec.com/index.php/tag/%E6%8F%90%E6%9D%83/"  
https://www.xazlsec.com/index.php/tag/python/"  
https://www.xazlsec.com/index.php/tag/SQL%E6%B3%A8%E5%85%A5/"  
https://www.xazlsec.com/index.php/tag/%E6%96%B9%E6%B3%95/"  
https://www.xazlsec.com/index.php/tag/msf/"  
https://www.xazlsec.com/index.php/tag/%E6%97%A0%E7%BA%BF%E5%AE%89%E5%85%A8/"  
https://www.xazlsec.com/index.php/tag/nmap/"  
https://www.xazlsec.com/index.php/tag/web/"  
https://www.xazlsec.com/index.php/tag/%E9%80%86%E5%90%91/"  
https://www.xazlsec.com/index.php/tag/%E5%AF%86%E7%A0%81/"  
https://www.xazlsec.com/index.php/tag/%E7%A0%B4%E8%A7%A3/"

https://www.xazlsec.com/index.php/tag/hash/"

https://www.xazlsec.com/index.php/tag/kali/"

https://www.xazlsec.com/index.php/tag/shell/"

https://www.xazlsec.com/index.php/tag/%E6%B5%8B%E8%AF%95%E6%B5%81%E7%A8%8B/"

https://www.xazlsec.com/index.php/tag/%E5%86%85%E7%BD%91%E6%B8%97%E9%80%8F/"

https://www.xazlsec.com/index.php/tag/%E4%B8%8B%E8%BD%BD%E6%96%87%E4%BB%B6/"

https://www.xazlsec.com/index.php/tag/DNS/"

https://www.xazlsec.com/index.php/tag/%E4%B8%BB%E6%9C%BA%E5%8F%91%E7%8E%B0/"

https://www.xazlsec.com/index.php/tag/%E6%BC%8F%E6%B4%9E%E5%AD%A6%E4%B9%A0/"

https://www.xazlsec.com/index.php/tag/HTTP/"

https://www.xazlsec.com/index.php/tag/%E5%AD%A6%E4%B9%A0%E7%BB%8F%E9%AA%8C/"

https://www.xazlsec.com/index.php/tag/XSS/"

https://www.xazlsec.com/index.php/tag/%E4%BB%A3%E7%A0%81%E5%AE%A1%E8%AE%A1/"

https://www.xazlsec.com/index.php/tag/PHP/"

https://www.xazlsec.com/index.php/tag/Android/"

https://www.xazlsec.com/index.php/tag/%E6%AD%A3%E5%88%99/"

https://www.xazlsec.com/index.php/tag/%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8/"

https://www.xazlsec.com/index.php/tag/%E7%BF%BB%E8%AF%91/"

https://www.xazlsec.com/index.php/tag/%E6%95%8F%E6%84%9F%E6%96%87%E4%BB%B6/"

https://www.xazlsec.com/index.php/tag/%E4%BF%A1%E6%81%AF%E6%B3%84%E9%9C%B2/"

https://www.xazlsec.com/index.php/tag/%E4%B8%9A%E5%8A%A1%E5%AE%89%E5%85%A8/"

https://www.xazlsec.com/index.php/tag/%E5%91%BD%E4%BB%A4/"

https://www.xazlsec.com/index.php/tag/%E5%AD%97%E5%85%B8/"

https://www.xazlsec.com/index.php/tag/hashcat/"

https://www.xazlsec.com/index.php/tag/%E5%B7%A5%E5%85%B7/"

https://www.xazlsec.com/index.php/tag/%E7%AB%AF%E5%8F%A3/"

https://www.xazlsec.com/index.php/tag/%E7%BD%91%E7%BB%9C/"

https://www.xazlsec.com/index.php/tag/DDOS/"

https://www.xazlsec.com/index.php/tag/%E8%BF%90%E7%BB%B4%E5%AE%89%E5%85%A8/"

https://www.xazlsec.com/index.php/tag/writeup/"

https://www.xazlsec.com/index.php/tag/Empire/"

https://www.xazlsec.com/index.php/tag/CURL/"

https://www.xazlsec.com/index.php/tag/MITMF/"

https://www.xazlsec.com/index.php/tag/%E4%B8%AD%E9%97%B4%E4%BA%BA/"

https://www.xazlsec.com/index.php/tag/%E4%B8%AD%E9%97%B4%E4%BA%BA%E6%94%BB%E5%87%BB/"

https://www.xazlsec.com/index.php/tag/wpad/"

https://www.xazlsec.com/index.php/tag/%E9%9A%A7%E9%81%93%E6%8A%80%E6%9C%AF/"

https://www.xazlsec.com/index.php/tag/%E5%8F%8D%E5%BC%B9/"

https://www.xazlsec.com/index.php/tag/%E4%B8%8A%E4%BC%A0/"

https://www.xazlsec.com/index.php/tag/%E5%91%BD%E4%BB%A4%E8%A1%8C/"

https://www.xazlsec.com/index.php/tag/%E5%9F%9F/"

https://www.xazlsec.com/index.php/tag/%E5%86%85%E7%BD%91/"

https://www.xazlsec.com/index.php/tag/whois/"

https://www.xazlsec.com/index.php/tag/%E7%AB%AF%E5%8F%A3%E6%89%AB%E6%8F%8F/"

https://www.xazlsec.com/index.php/tag/%E5%AF%86%E7%A0%81%E7%A0%B4%E8%A7%A3/"

https://www.xazlsec.com/index.php/tag/oracle/"

https://www.xazlsec.com/index.php/tag/web%E5%AE%89%E5%85%A8/"

https://www.xazlsec.com/index.php/tag/%E5%AE%89%E5%85%A8%E5%AD%A6%E4%B9%A0/"

https://www.xazlsec.com/index.php/tag/APT/"

https://www.xazlsec.com/index.php/tag/office/"

https://www.xazlsec.com/index.php/tag/EAP/"

https://www.xazlsec.com/index.php/tag/bwapp/"

https://www.xazlsec.com/index.php/tag/%E7%94%9F%E6%88%90%E5%AD%97%E5%85%B8/"

https://www.xazlsec.com/index.php/tag/%E6%9A%B4%E5%8A%9B%E7%A0%B4%E8%A7%A3/"

https://www.xazlsec.com/index.php/tag/WEB%E6%9C%8D%E5%8A%A1/"

https://www.xazlsec.com/index.php/tag/Pentester/"

https://www.xazlsec.com/index.php/tag/%E6%96%87%E4%BB%B6%E5%8C%85%E5%90%AB/"

https://www.xazlsec.com/index.php/tag/%E6%95%B0%E6%8D%AE%E5%BA%93/"

https://www.xazlsec.com/index.php/tag/Oauth/"

https://www.xazlsec.com/index.php/tag/next-aaaa-1/"



https://www.xazlsec.com/index.php/tag/postgresql/

https://www.xazlsec.com/index.php/tag/XXE/

https://www.xazlsec.com/index.php/tag/%E5%AE%89%E5%85%A8%E5%8A%A0%E5%9B%BA/

https://www.xazlsec.com/index.php/tag/splunk/

https://www.xazlsec.com/index.php/tag/%E5%90%8E%E9%97%A8/

https://www.xazlsec.com/index.php/tag/%E7%BB%84%E4%BB%B6/

https://www.xazlsec.com/index.php/tag/%E4%BC%9A%E8%AF%9D%E5%8A%AB%E6%8C%81/

https://www.xazlsec.com/index.php/tag/tcp/

https://www.xazlsec.com/index.php/tag/sqlmap/

https://www.xazlsec.com/index.php/tag/%E5%85%8D%E6%9D%80/

https://www.xazlsec.com/index.php/tag/%E6%A0%88%E6%BA%A2%E5%87%BA/

https://www.xazlsec.com/index.php/tag/%E6%96%87%E7%AB%A0%E6%B1%87%E6%80%BB/

https://www.xazlsec.com/index.php/tag/hacker/

https://www.xazlsec.com/index.php/tag/pwn/

https://www.xazlsec.com/index.php/tag/ida/

https://www.xazlsec.com/index.php/tag/gdb/

https://www.xazlsec.com/index.php/tag/%E5%BF%98%E8%AE%B0%E5%AF%86%E7%A0%81/

https://www.xazlsec.com/index.php/tag/%E7%BB%95%E8%BF%87/

http://www.w3.org/2000/svg"

http://www.w3.org/1999/xlink"

https://www.xazlsec.com/

http://www.beian.miit.gov.cn"

https://www.xazlsec.com/usr/themes/default/js/jquery2.14.min.js"

https://www.xazlsec.com/usr/themes/default/js/bootstrap.min.js"

https://www.xazlsec.com/usr/themes/default/js/functionall.js"

https://www.xazlsec.com/usr/themes/default/js/tagcanvas.min.js"

https://www.xazlsec.com/usr/themes/default/js/particles.min.js"

https://www.xazlsec.com/usr/themes/default/js/headerCanvas.js"

https://www.xazlsec.com/usr/themes/default/js/home.js"