现在，也许我们所认为的漏洞利用工具神器，十年后，又该会是什么样子呢？可能大概就像我们现在看到以前的啊d注入工具的样子吧。

近几日，我忽然思考这样一个问题：**如果一种漏洞类型，让你推荐一款与之强相关的漏洞利用神器，你会怎么推荐？**

下面，我来分享一下我心里的答案，**推荐几款我认为的漏洞利用神器**，欢迎各位来一起补充。

1、SQL注入漏洞

推荐项目：SQLmap，项目地址：http://sqlmap.org/

推荐理由：殿堂级工具，注入神器，效果谁用谁知道。

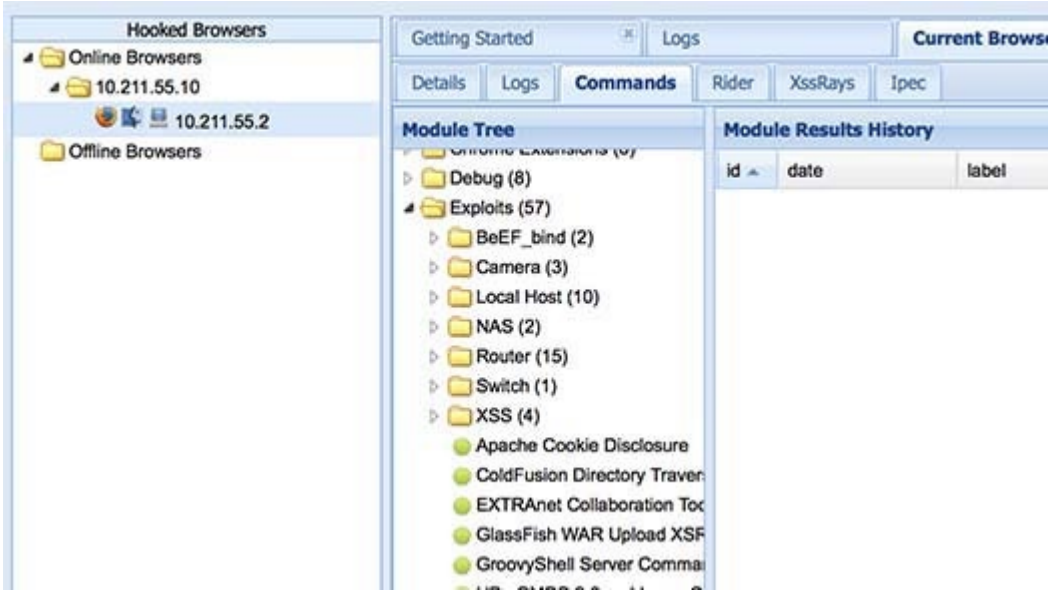
```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.3.4.44#dev}
|_ -| . [']     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent i
s illegal. It is the end user's responsibility to obey all applicable local, state and fed
eral laws. Developers assume no liability and are not responsible for any misuse or damage
 caused by this program

[*] starting @ 10:44:53 /2019-04-30/

[10:44:54] [INFO] testing connection to the target URL
[10:44:54] [INFO] heuristics detected web page charset 'ascii'
[10:44:54] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:44:54] [INFO] testing if the target URL content is stable
[10:44:55] [INFO] target URL content is stable
[10:44:55] [INFO] testing if GET parameter 'id' is dynamic
[10:44:55] [INFO] GET parameter 'id' appears to be dynamic
[10:44:55] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
 (possible DBMS: 'MySQL')
```

2、XSS

推荐项目：beef

项目地址：https://beefproject.com/

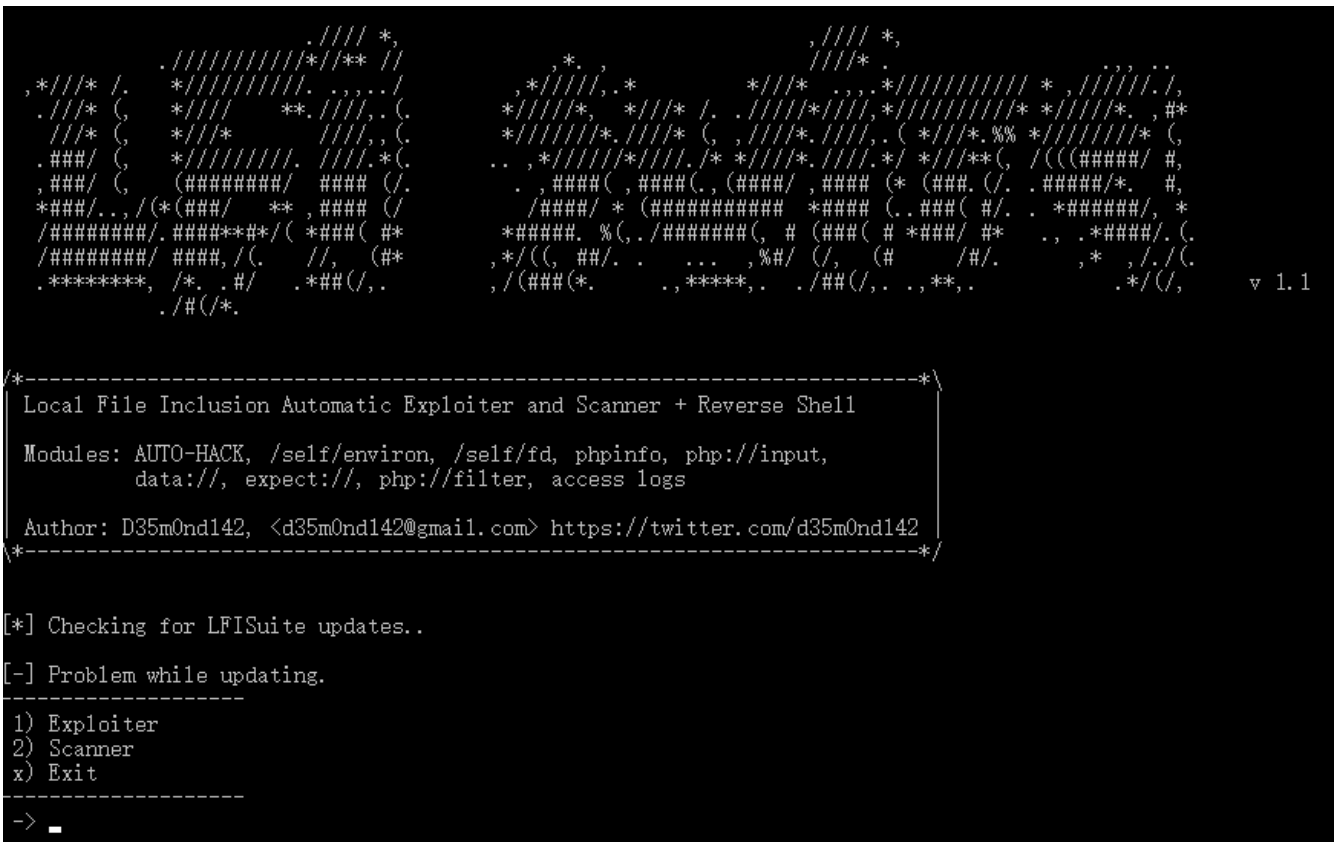
推荐理由：专门针对浏览器攻击的框架。



3、文件包含漏洞

推荐项目：LFISuite，项目地址：https://github.com/D35m0nd142/LFISuite

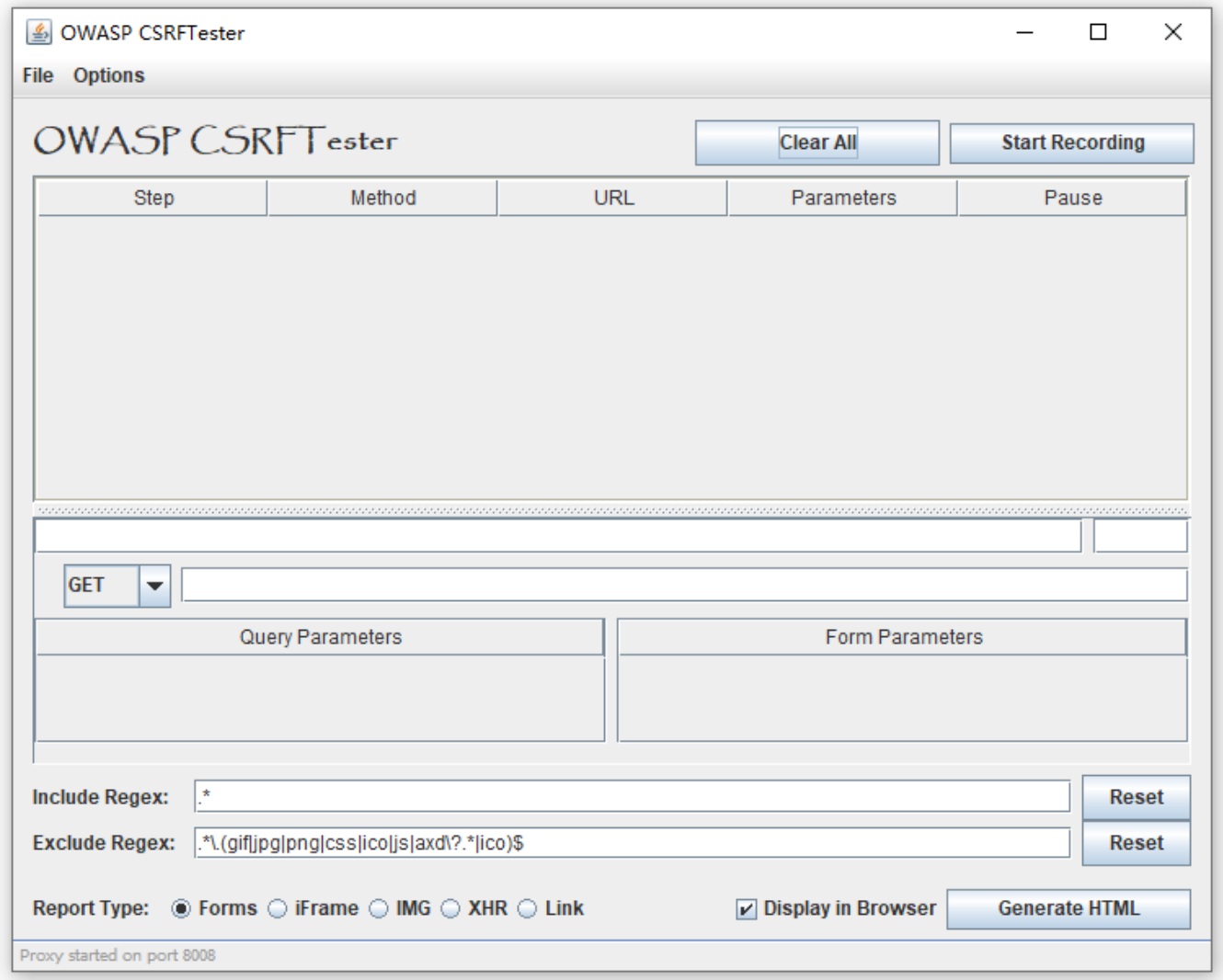
推荐理由：一款全自动工具，能够使用多种不同攻击方法来扫描和利用本地文件包含漏洞。



4、CSRF

推荐项目：CSRFTester，项目地址：https://wiki.owasp.org/index.php/File:CSRFTester-1.0.zip

推荐理由：一款CSRF漏洞的测试工具，集抓包和Poc构造与一体。



5、XXE(外部实体注入漏洞)

推荐项目：XXEinjector，项目地址：https://github.com/enjoiz/XXEinjector

推荐理由：使用直接和不同带外方法自动利用XXE漏洞的工具。

```
root@kali:~/Desktop/XXEinjector# ruby XXEinjector.rb
XXEinjector by Jakub Pałaczyński

XXEinjector automates retrieving files using direct and out of band methods. Dire
ctory listing only works in Java applications. Bruteforcing method needs to be us
ed for other applications.

Options:
  --host        Mandatory - our IP address for reverse connections. (--host=192.1
68.0.2)
  --file        Mandatory - file containing valid HTTP request with xml. You can
also mark with "XXEINJECT" a point where DTD should be injected. (--file=/tmp/req
.txt)
  --path        Mandatory if enumerating directories - Path to enumerate. (--path
=/etc)
  --brute       Mandatory if bruteforcing files - File with paths to bruteforce.
(--brute=/tmp/brute.txt)
  --logger      Log results only. Do not send requests. HTTP logger looks for "p"
 parameter with results.

  --rhost       Remote host's IP address or domain name. Use this argument only f
or requests without Host header. (--rhost=192.168.0.3)
  --rport       Remote host's TCP port. Use this argument only for requests witho
ut Host header and for non-default values. (--rport=8080)
```

6、Xpath注入

推荐项目：XCat，项目地址：https://github.com/orf/xcat

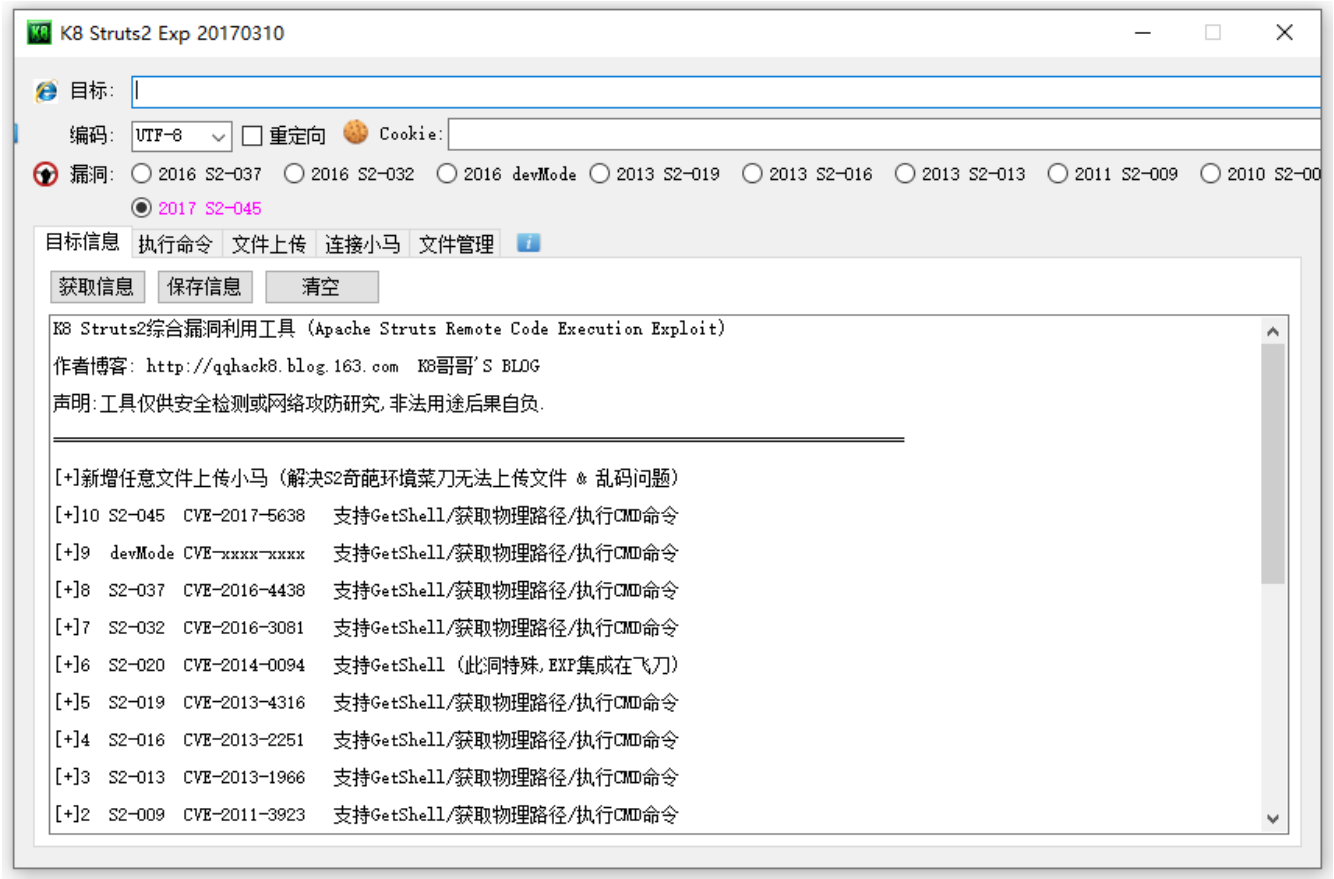
推荐理由：一个命令行工具，可以利用和检测XPath盲注漏洞。

```
C:\xcat-master>run_xcat.py  --method=GET --public-ip="192.168.91.139" http://192
.168.91.139/xml/example2.php name=hacker name "Hello hacker" run retrieve
Injecting using String [']
Detecting features...
Listening on 0
Listening on 2385
Stopping server
Supported features: Substring search speedup
Retrieving /*[1]
<?xml version="1.0" encoding="utf-8"?>
<data>
        <users>
                <user>
                        <name>
                                hacker
                        </name>
                        <message>
                                Hello hacker
                        </message>
                        <password>
                                pentesterlab
                        </password>
                </user>
                <user>
                        <name>
                                admin
                        </name>
                        <message>
                                Hello admin
                        </message>
                        <password>
                                s3cr3tP4ssw0rd
```

7、Struts漏洞利用

推荐项目：K8 Struts2 Exploit

推荐理由：Struts2综合漏洞利用工具，包含收集信息，执行命令、文件上传、连接小马、文件管理等功能。



8、Jboss漏洞

推荐项目：JexBoss，项目地址：https://github.com/joaomatosf/jexboss

推荐理由：扫描和检测Jboss中可能存在多个安全漏洞。

```
root@kali:~/Desktop/jexboss# python jexboss.py -h


usage: JexBoss [-h] [--version] [--auto-exploit] [--disable-check-updates]
               [-mode {standalone,auto-scan,file-scan}] [--app-unserialize]
               [--servlet-unserialize] [--jboss] [--jenkins] [--struts2]
               [--jmxtomcat] [--proxy PROXY] [--proxy-cred LOGIN:PASS]
               [--jboss-login LOGIN:PASS] [--timeout TIMEOUT]
               [--cookies NAME=VALUE] [--reverse-host RHOST:RPORT] [--cmd CMD]
               [--dns URL] [--windows] [--post-parameter PARAMETER]
               [--show-payload]
               [--gadget {commons-collections3.1,commons-collections4.0,jdk7u21,j
dk8u20,groovy1,dns}]
               [--load-gadget FILENAME] [--force] [-host HOST]
               [-network NETWORK] [-ports PORTS] [-results FILENAME]
               [-file FILENAME_HOSTS] [-out FILENAME_RESULTS]


 # --- JexBoss: Jboss verify and EXploitation Tool  --- #
 |    And others Java Deserialization Vulnerabilities   |
 |                                                      |
 | @author:  João Filho Matos Figueiredo                |
 | @contact: joaomatosf@gmail.com                       |
 |                                                      |
 | @updates: https://github.com/joaomatosf/jexboss      |
 #______________________________________________________#
 @version: 1.2.4
 Examples: [for more options, type python jexboss.py -h]
```

9、路由器漏洞

推荐项目：RouterSploit 项目地址：https://github.com/threat9/routersploit

推荐理由：一款专门针对嵌入式设备的漏洞利用工具，包含了27个品牌的上百种漏洞利用模块，涉及的路由器、摄像头等设备有几百种。

```
root@kali:~/Desktop/routersploit# python3 rsf.py
 _____                _           _____       _       _ _
 | ___ \              | |         /  ___|     | |     (_) |
 | |_/ /___  _   _  _| |_ ___ _ __\ `--. _ __ | | ___  _| |_
 |    // _ \| | | |/ __/ _ \ '__|`--. \ '_ \| |/ _ \| | __|
 | |\ \ (_) | |_| | ||  __/ |  /\__/ / |_) | | (_) | | |_
 \_| \_\___/ \__,_|\__\___|_|  \____/| .__/|_|\___/|_|\__|
                                     | |
       Exploitation Framework for    |_|    by Threat9
            Embedded Devices

 Codename   : I Knew You Were Trouble
 Version    : 3.4.1
 Homepage   : https://www.threat9.com - @threatnine
 Join Slack : https://www.threat9.com/slack

 Join Threat9 Beta Program - https://www.threat9.com

 Exploits: 132 Scanners: 4 Creds: 171 Generic: 4 Payloads: 32 Encoders: 6

rsf >
```

重复造轮子者甚多，而能够称之为神器的工具甚少，**我们应当时常心怀感激，感谢每一位安全开发者的无私奉献。**

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。