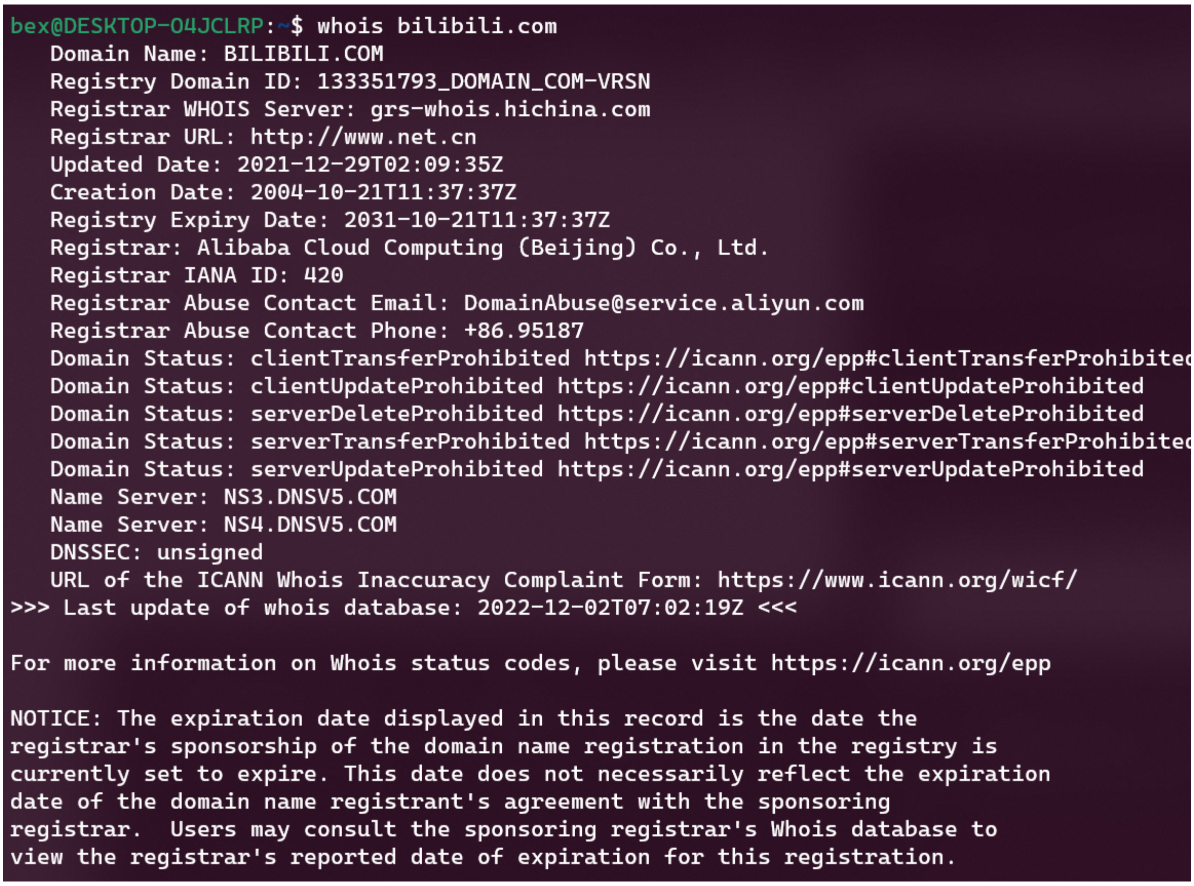
1.使用whois查询zucc的注册信息

查询bilibili.com注册信息



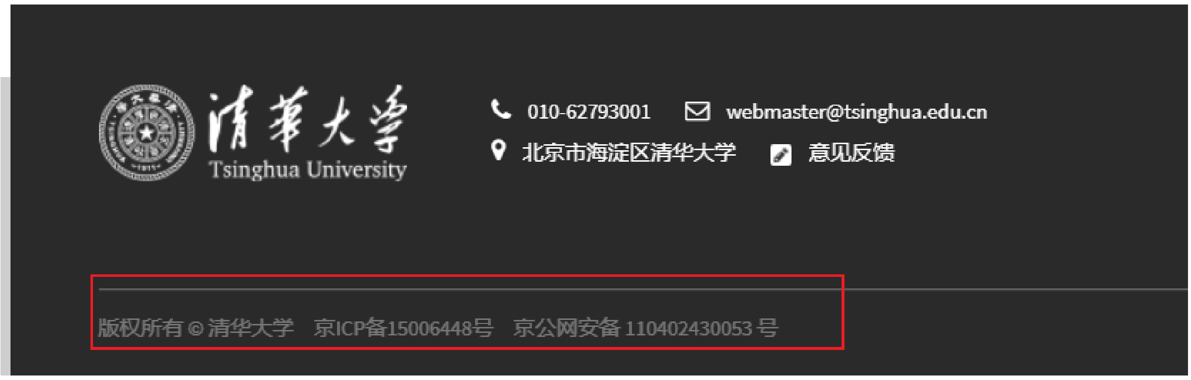
```
bex@DESKTOP-O4JCLRP:~$ whois bilibili.com
   Domain Name: BILIBILI.COM
   Registry Domain ID: 133351793_DOMAIN_COM-VRSN
   Registrar WHOIS Server: grs-whois.hichina.com
   Registrar URL: http://www.net.cn
   Updated Date: 2021-12-29T02:09:35Z
   Creation Date: 2004-10-21T11:37:37Z
   Registry Expiry Date: 2031-10-21T11:37:37Z
   Registrar: Alibaba Cloud Computing (Beijing) Co., Ltd.
   Registrar IANA ID: 420
   Registrar Abuse Contact Email: DomainAbuse@service.aliyun.com
   Registrar Abuse Contact Phone: +86.95187
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibite
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibite
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS3.DNSV5.COM
   Name Server: NS4.DNSV5.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-12-02T07:02:19Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
```

2.使用清华大学的备案号查询其信息

在清华大学官方网站找到ICP编号



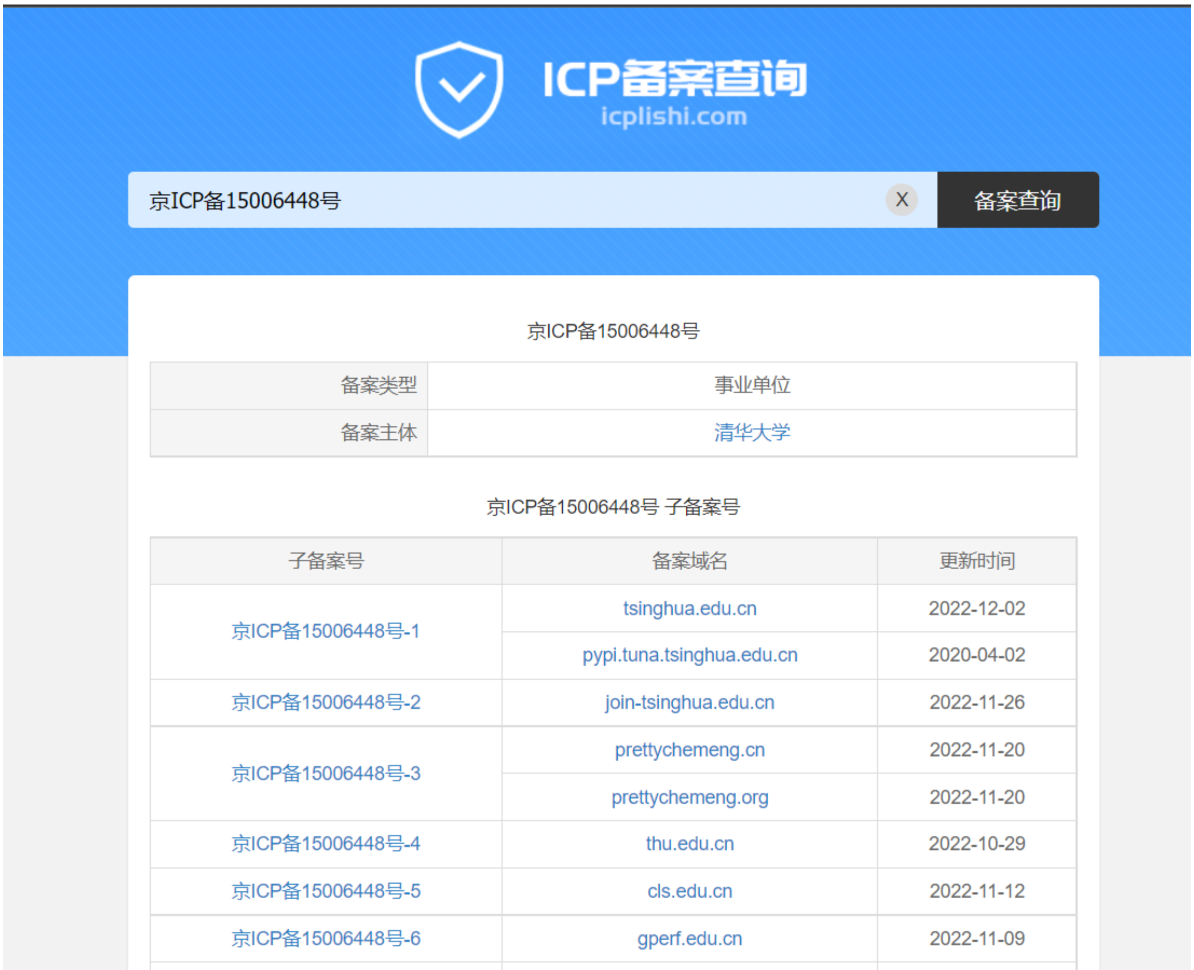
☎ 010-62793001 ✉ webmaster@tsinghua.edu.cn

北京市海淀区清华大学 意见反馈

版权所有 © 清华大学 京ICP备15006448号 京公网安备 110402430053 号

在 https://icplishi.com 网站查询

https://icplishi.com/%E4%BA%ACICP%E5%A4%8715006448%E5%8F%B7/



京ICP备15006448号

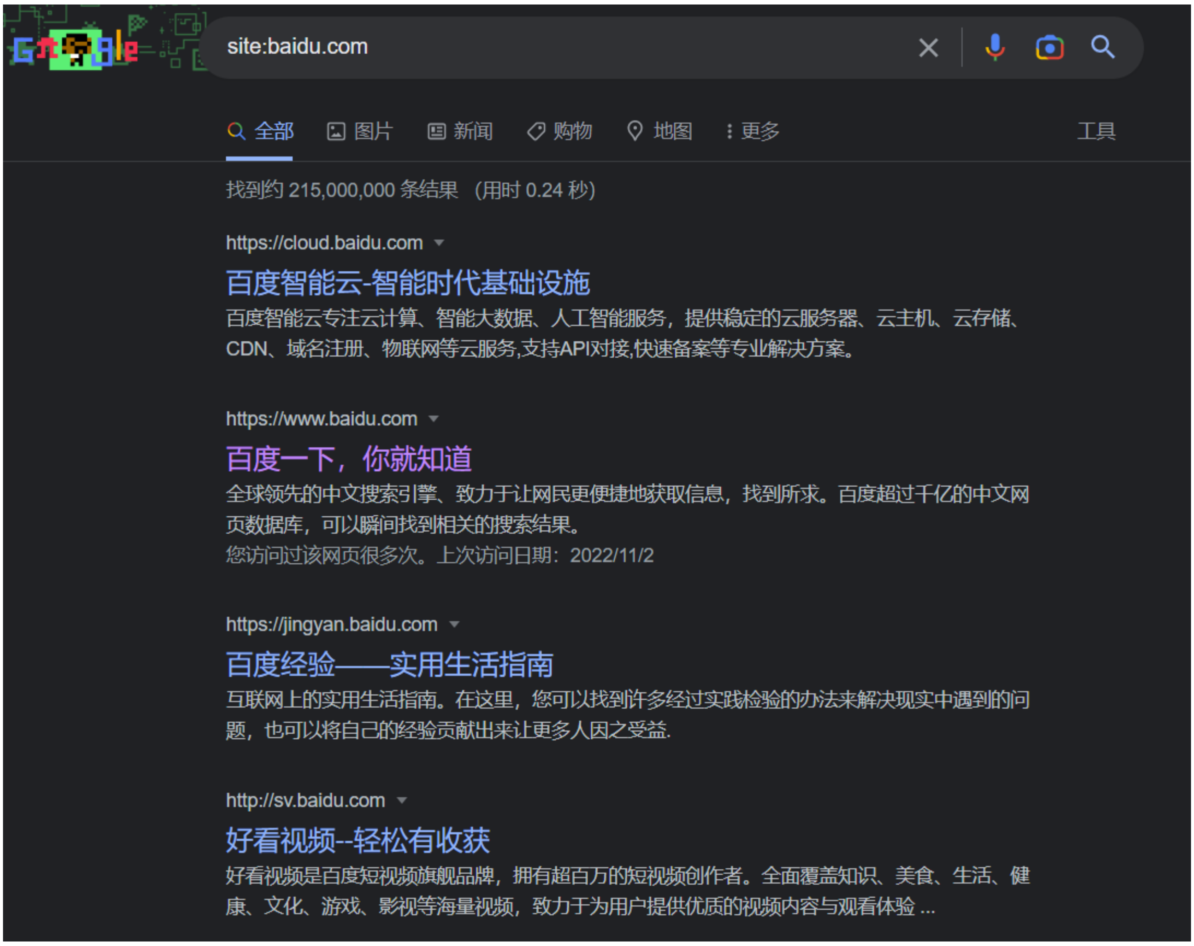
备案类型	事业单位
备案主体	清华大学

京ICP备15006448号 子备案号

子备案号	备案域名	更新时间
京ICP备15006448号-1	tsinghua.edu.cn	2022-12-02
	pypi.tuna.tsinghua.edu.cn	2020-04-02
京ICP备15006448号-2	join-tsinghua.edu.cn	2022-11-26
京ICP备15006448号-3	prettychemeng.cn	2022-11-20
	prettychemeng.org	2022-11-20
京ICP备15006448号-4	thu.edu.cn	2022-10-29
京ICP备15006448号-5	cls.edu.cn	2022-11-12
京ICP备15006448号-6	gperf.edu.cn	2022-11-09

3.分别利用搜索引擎和JsFinder来查找百度从子域名

搜索引擎



找到约 215,000,000 条结果 （用时 0.24 秒）

https://cloud.baidu.com

百度智能云-智能时代基础设施

百度智能云专注云计算、智能大数据、人工智能服务，提供稳定的云服务器、云主机、云存储、CDN、域名注册、物联网等云服务,支持API对接,快速备案等专业解决方案。

https://www.baidu.com

百度一下，你就知道

全球领先的中文搜索引擎、致力于让网民更便捷地获取信息，找到所求。百度超过千亿的中文网页数据库，可以瞬间找到相关的搜索结果。

您访问过该网页很多次。上次访问日期：2022/11/2

https://jingyan.baidu.com

百度经验——实用生活指南

互联网上的实用生活指南。在这里，您可以找到许多经过实践检验的办法来解决现实中遇到的问题，也可以将自己的经验贡献出来让更多人因之受益.

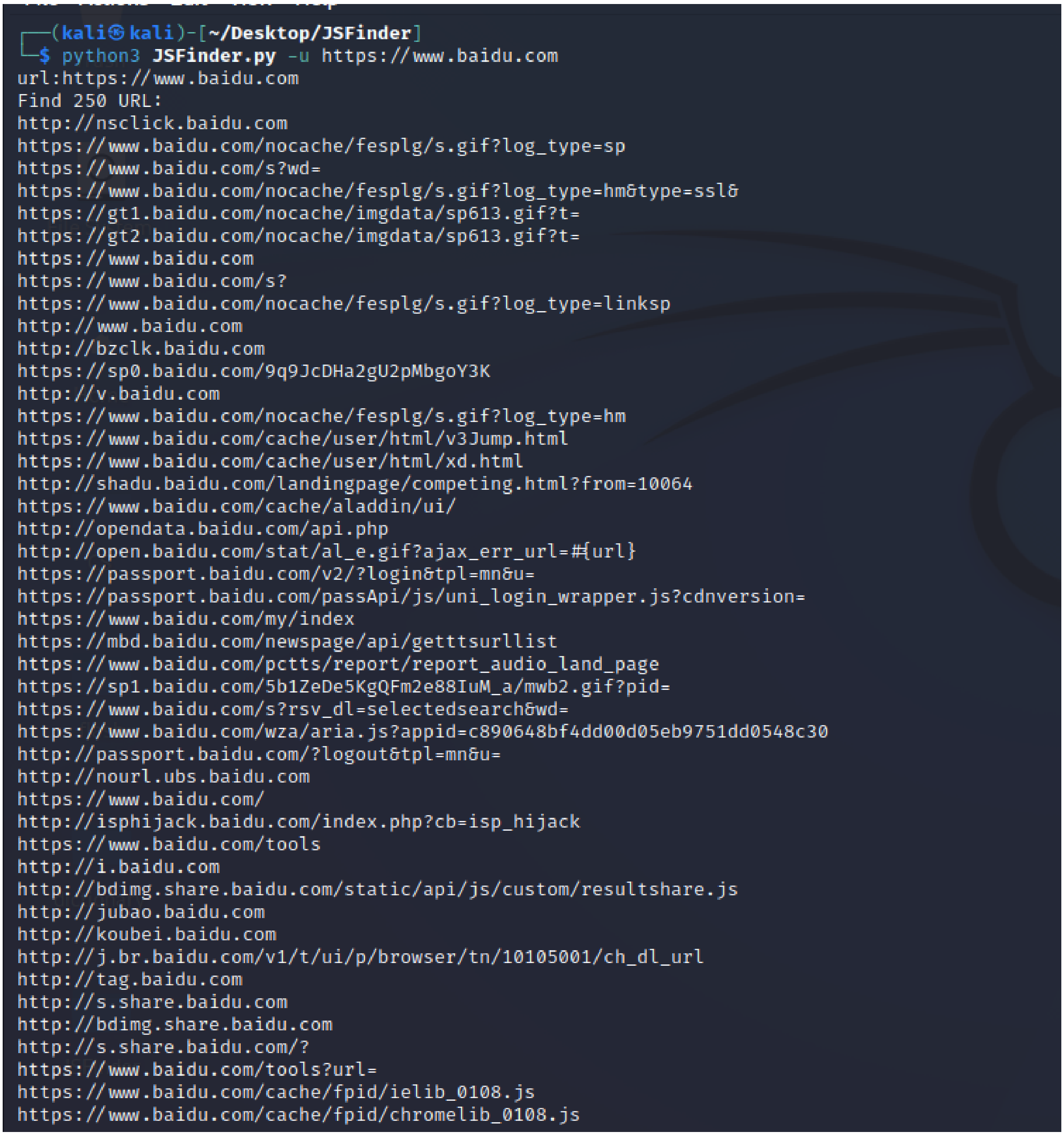
http://sv.baidu.com

好看视频--轻松有收获

好看视频是百度短视频旗舰品牌，拥有超百万的短视频创作者。全面覆盖知识、美食、生活、健康、文化、游戏、影视等海量视频，致力于为用户提供优质的视频内容与观看体验 ...

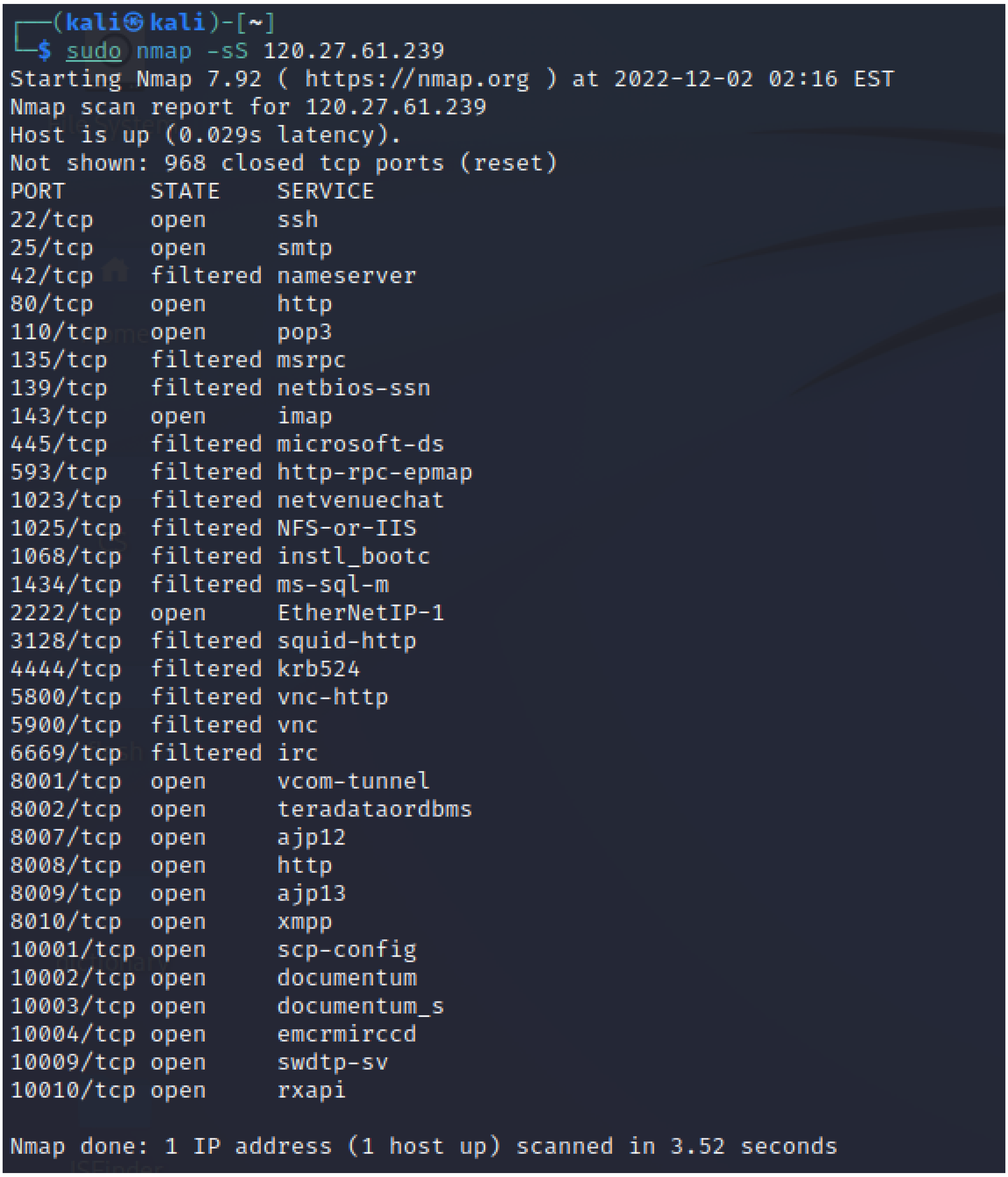
JsFinder

```
python3 JSFinder.py -u https://www.baidu.com
```



```
┌──(kali㉿kali)-[~/Desktop/JSFinder]
└─$ python3 JSFinder.py -u https://www.baidu.com
url:https://www.baidu.com
Find 250 URL:
http://nsclick.baidu.com
https://www.baidu.com/nocache/fesplg/s.gif?log_type=sp
https://www.baidu.com/s?wd=
https://www.baidu.com/nocache/fesplg/s.gif?log_type=hm&type=ssl&
https://gt1.baidu.com/nocache/imgdata/sp613.gif?t=
https://gt2.baidu.com/nocache/imgdata/sp613.gif?t=
https://www.baidu.com
https://www.baidu.com/s?
https://www.baidu.com/nocache/fesplg/s.gif?log_type=linksp
http://www.baidu.com
http://bzclk.baidu.com
https://sp0.baidu.com/9q9JcDHa2gU2pMbgoY3K
http://v.baidu.com
https://www.baidu.com/nocache/fesplg/s.gif?log_type=hm
https://www.baidu.com/cache/user/html/v3Jump.html
https://www.baidu.com/cache/user/html/xd.html
http://shadu.baidu.com/landingpage/competing.html?from=10064
https://www.baidu.com/cache/aladdin/ui/
http://opendata.baidu.com/api.php
http://open.baidu.com/stat/al_e.gif?ajax_err_url=#{url}
https://passport.baidu.com/v2/?login&tpl=mn&u=
https://passport.baidu.com/passApi/js/uni_login_wrapper.js?cdnversion=
https://www.baidu.com/my/index
https://mbd.baidu.com/newspage/api/getttsurllist
https://www.baidu.com/pctts/report/report_audio_land_page
https://sp1.baidu.com/5b1ZeDe5KgQFm2e88IuM_a/mwb2.gif?pid=
https://www.baidu.com/s?rsv_dl=selectedsearch&wd=
https://www.baidu.com/wza/aria.js?appid=c890648bf4dd00d05eb9751dd0548c30
http://passport.baidu.com/?logout&tpl=mn&u=
http://nourl.ubs.baidu.com
https://www.baidu.com/
http://isphijack.baidu.com/index.php?cb=isp_hijack
https://www.baidu.com/tools
http://i.baidu.com
http://bdimg.share.baidu.com/static/api/js/custom/resultshare.js
http://jubao.baidu.com
http://koubei.baidu.com
http://j.br.baidu.com/v1/t/ui/p/browser/tn/10105001/ch_dl_url
http://tag.baidu.com
http://s.share.baidu.com
http://bdimg.share.baidu.com
http://s.share.baidu.com/?
https://www.baidu.com/tools?url=
https://www.baidu.com/cache/fpid/ielib_0108.js
https://www.baidu.com/cache/fpid/chromelib_0108.js
```

4.使用nmap查找120.27.61.239开放的端口号及服务



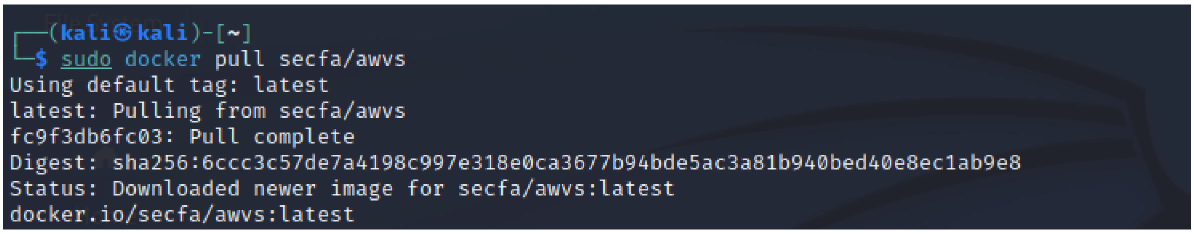
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 120.27.61.239
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-02 02:16 EST
Nmap scan report for 120.27.61.239
Host is up (0.029s latency).
Not shown: 968 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    open     smtp
42/tcp    filtered nameserver
80/tcp    open     http
110/tcp   open     pop3
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
143/tcp   open     imap
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
1023/tcp  filtered netvenuechat
1025/tcp  filtered NFS-or-IIS
1068/tcp  filtered instl_bootc
1434/tcp  filtered ms-sql-m
2222/tcp  open     EtherNetIP-1
3128/tcp  filtered squid-http
4444/tcp  filtered krb524
5800/tcp  filtered vnc-http
5900/tcp  filtered vnc
6669/tcp  filtered irc
8001/tcp  open     vcom-tunnel
8002/tcp  open     teradataordbms
8007/tcp  open     ajp12
8008/tcp  open     http
8009/tcp  open     ajp13
8010/tcp  open     xmpp
10001/tcp open     scp-config
10002/tcp open     documentum
10003/tcp open     documentum_s
10004/tcp open     emcrmirccd
10009/tcp open     swdtp-sv
10010/tcp open     rxapi

Nmap done: 1 IP address (1 host up) scanned in 3.52 seconds
```

5.安装并使用awvs

从docker上拉去相关镜像

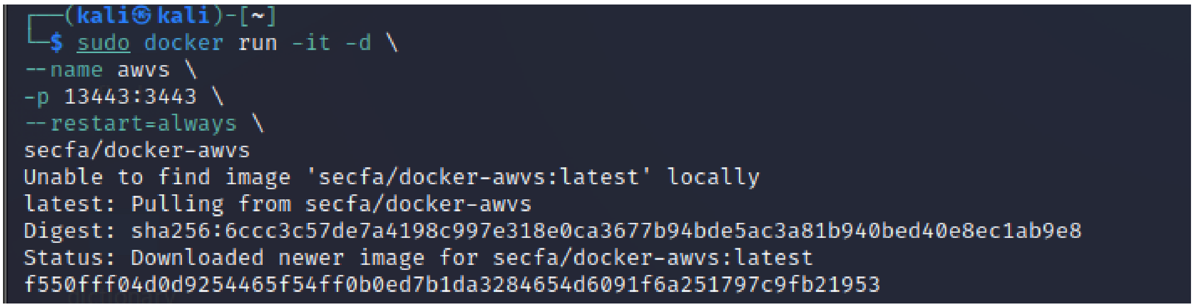
```
sudo docker pull secfa/docker-awvs
```



```
┌──(kali㉿kali)-[~]
└─$ sudo docker pull secfa/awvs
Using default tag: latest
latest: Pulling from secfa/awvs
fc9f3db6fc03: Pull complete
Digest: sha256:6ccc3c57de7a4198c997e318e0ca3677b94bde5ac3a81b940bed40e8ec1ab9e8
Status: Downloaded newer image for secfa/awvs:latest
docker.io/secfa/awvs:latest
```

运行容器

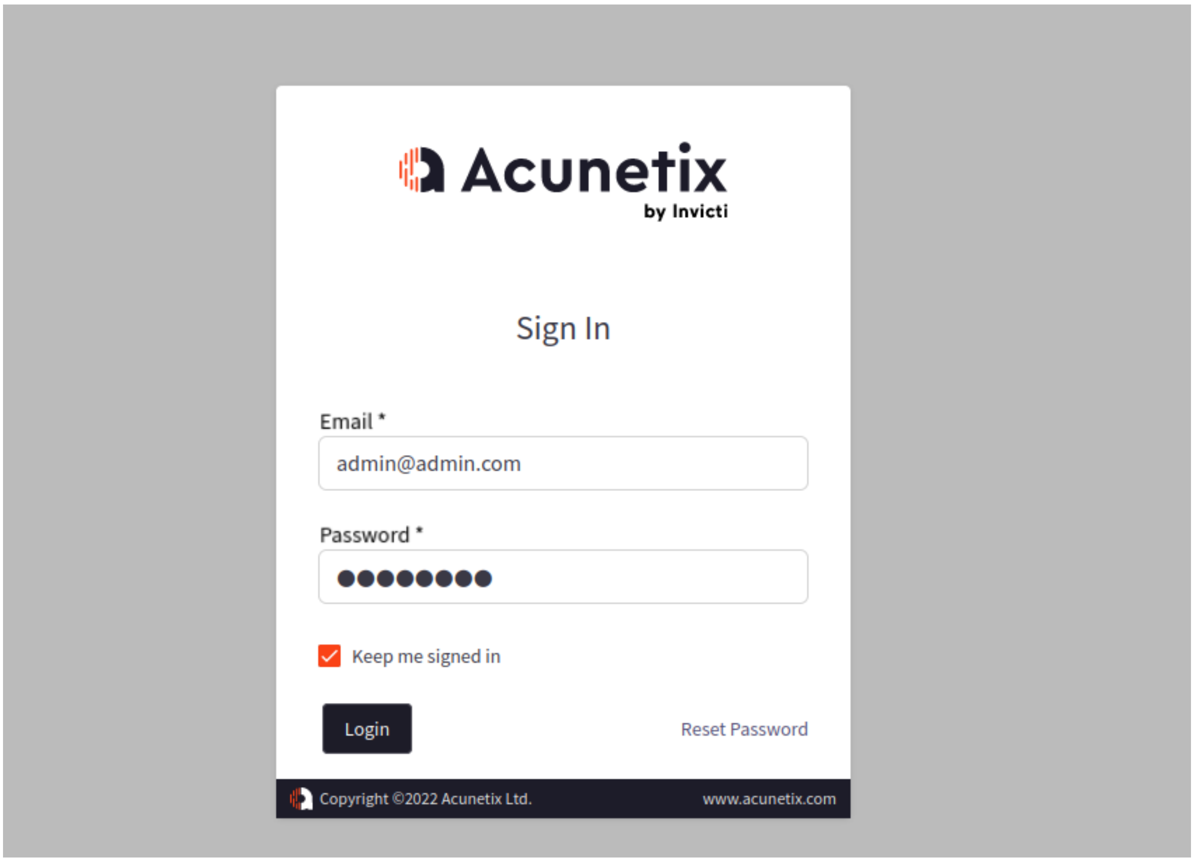
```
docker run -it -d \
--name awvs \
-p 13443:3443 \
--restart=always \
secfa/docker-awvs:latest
```



```
┌──(kali㉿kali)-[~]
└─$ sudo docker run -it -d \
--name awvs \
-p 13443:3443 \
--restart=always \
secfa/docker-awvs
Unable to find image 'secfa/docker-awvs:latest' locally
latest: Pulling from secfa/docker-awvs
Digest: sha256:6ccc3c57de7a4198c997e318e0ca3677b94bde5ac3a81b940bed40e8ec1ab9e8
Status: Downloaded newer image for secfa/docker-awvs:latest
f550fff04d0d9254465f54ff0b0ed7b1da3284654d6091f6a251797c9fb21953
```

进入管理界面

```
URL:https://localhost:13443/#/login
Username:admin@admin.com
password:Admin123
```



Sign In

Email *

admin@admin.com

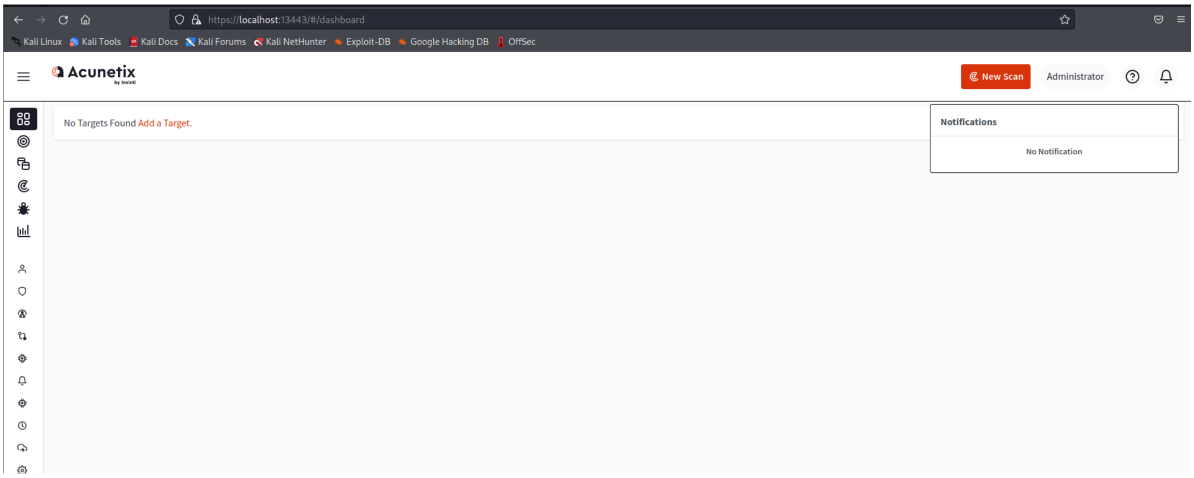
Password *

●●●●●●●●

☑ Keep me signed in

Copyright ©2022 Acunetix Ltd.

www.acunetix.com

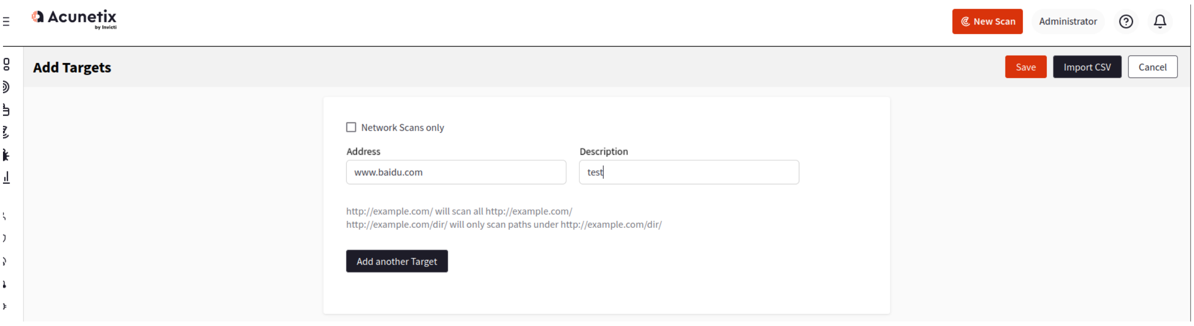


No Targets Found Add a Target.

Notifications

No Notification

新建扫描目标并进行扫描



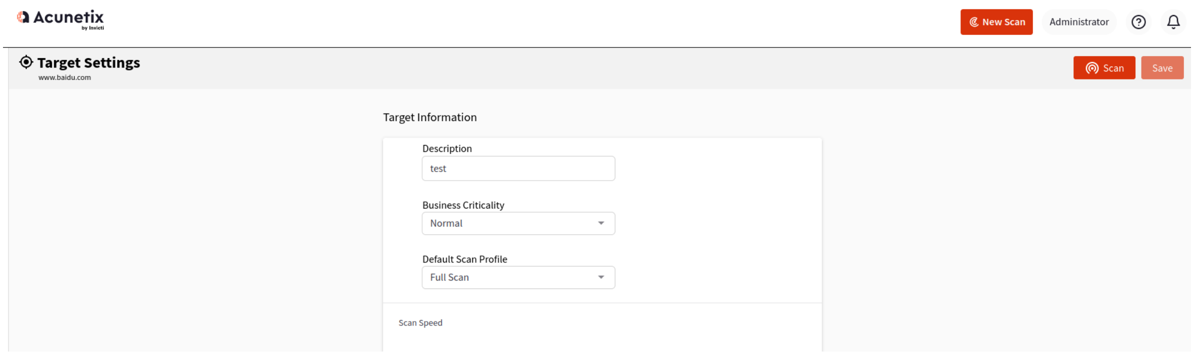
Add Targets

□ Network Scans only

Address: www.baidu.com

Description: test

http://example.com/ will scan all http://example.com/
http://example.com/dir/ will only scan paths under http://example.com/dir/



Target Settings
www.baidu.com

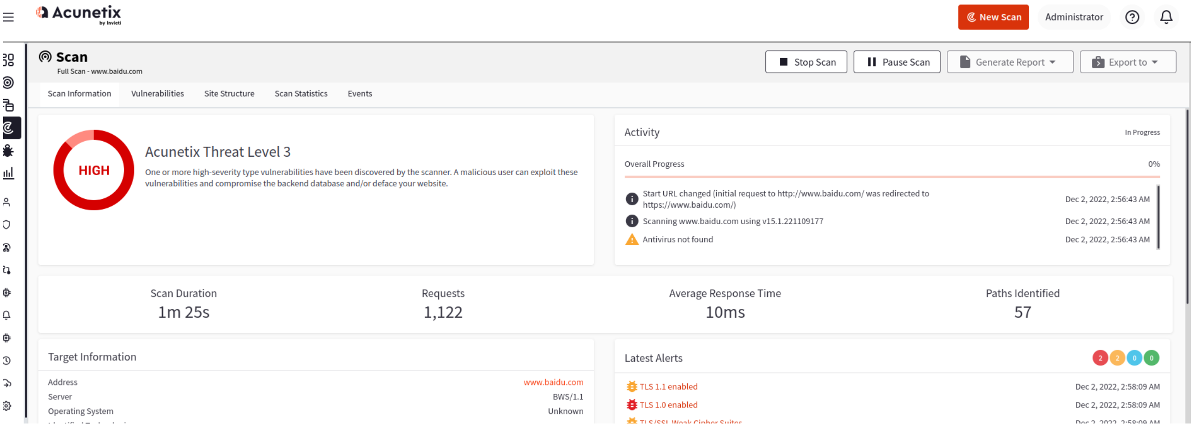
Target Information

Description: test

Business Criticality: Normal

Default Scan Profile: Full Scan

Scan Speed



Scan
Full Scan - www.baidu.com

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Activity — In Progress

Overall Progress 0%

```
Start URL changed (initial request to http://www.baidu.com/ was redirected to    Dec 2, 2022, 2:56:43 AM
https://www.baidu.com/)
Scanning www.baidu.com using v15.1.221109177                                      Dec 2, 2022, 2:56:43 AM
Antivirus not found                                                               Dec 2, 2022, 2:56:43 AM
```

Scan Duration	Requests	Average Response Time	Paths Identified
1m 25s	1,122	10ms	57

Target Information

Address	www.baidu.com
Server	BWS/1.1
Operating System	Unknown

Latest Alerts

```
TLS 1.1 enabled                 Dec 2, 2022, 2:58:09 AM
TLS 1.0 enabled                 Dec 2, 2022, 2:58:09 AM
TLS/SSL Weak Cipher Suites      Dec 2, 2022, 2:58:09 AM
```