Sri Lanka Institute of Information Technology

VULNERABILITY ASSESSMENT
WEB AUDIT

https://www.aliexpress.com

IE2062 - Web Security

B.Sc. (Hons) in Information Technology
specializing Cyber Security

Student Details

	Student ID	Student Name
1	IT19961118	W.M.J.P.WIJESEKARA

Table of Contents

Acknowledgement

I would like to dedicate this Web audit report to Dr Lakmal Rupasinghe, Ms Chathu Udagedara, Ms Lanesssha Rukgahakotuwa , Ms Chethana Liyanapathirana of the department of cyber security in the faculty of computing in SLIIT who developed the Knowledge and attitudes required to successfully complete the assessment in the web security module. I would like to present all those involved in finding the data needed to make this report a success.

Scope

After enumerating subdomains, I selected following few sub-domains as my scope and target domains.

1. **aliexpress.com**
2. **2014.aliexpress.com**
3. **activities.aliexpress.com**
4. **ajax.aliexpress.com**
5. **amacc.aliexpress.com**
6. **api.dos.aliexpress.com**
7. **best.aliexpress.com**
8. **brands.aliexpress.com**
9. **connectkeyword.aliexpress.com**
10. **message.aliexpress.com**

10.passport.aliexpress.com

11.womenmenclothes439106.aliexpress.com

12.zhouyun19930515.aliexpress.com

Top 10 Web Application Security Risks

A1:2017-Injection:

When untrusted data is provided to an interpreter as part of a command or query, injection issues such as SQL, NoSQL, OS, and LDAP injection occur. The interpreter can be fooled by the attacker's hostile data into executing unwanted commands or accessing data without proper authorization.

A2:2017-Broken Authentication:

Authentication and session management capabilities in applications are frequently built poorly, allowing attackers to compromise passwords, keys, or session tokens, or exploit other technical defects to temporarily or permanently assume the identities of other users.

A3:2017-Sensitive Data Exposure:

Many web apps and APIs fail to adequately protect sensitive data, such as financial, healthcare, and personally identifiable information (PII). In order to commit credit card fraud, identity theft, or other crimes, attackers may steal or manipulate such inadequately protected data. Without added protection, such as encryption at rest or in transit, sensitive data may be compromised, necessitating additional safeguards when communicated with the browser.

A4:2017-XML External Entities (XXE):

External entity references in XML documents are evaluated by many older or poorly configured XML documents. Using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks, external entities can be utilized to expose internal files.

A5:2017-Broken Access Control:

Restrictions on what authenticated users can and cannot do are frequently ignored. Attackers can leverage these weaknesses to get unauthorized access to unauthorized functionality and/or data, such as other users' accounts, sensitive files, other users' data, changing access rights, and so on.

A6:2017-Security Misconfiguration:

The most prevalent problem is security misconfiguration. Insecure default configurations, incomplete or ad hoc setups, exposed cloud storage, misconfigured HTTP headers, and verbose error messages exposing sensitive information are all major causes of this. All operating systems, frameworks, libraries, and programs must not only be configured securely, but they must also be patched/upgraded on a regular basis.

A7:2017-Cross-Site Scripting XSS:

XSS issues arise when an application adds untrusted data in a new web page without sufficient validation or escaping, or when a browser API that can create HTML or JavaScript modifies an existing web page with user-supplied data. XSS allows attackers to run scripts in the victim's browser, allowing them to hijack user sessions, deface websites, or redirect users to malicious websites.

A8:2017-Insecure Deserialization:

Deserialization that isn't secure can lead to remote code execution. Deserialization issues can be leveraged to accomplish attacks such as replay attacks, injection attacks, and privilege escalation even if they do not result in remote code execution.

A9:2017-Using Components with Known Vulnerabilities:

Libraries, frameworks, and other software modules, for example, execute with the same privileges as the application. Such an attack can result in catastrophic data loss or server takeover if a susceptible component is exploited. Applications and APIs that use components that have known vulnerabilities can weaken application defenses and open the door to a variety of assaults and consequences.

A10:2017-Insufficient Logging & Monitoring:

Inadequate logging and monitoring, along with missing or ineffective incident response integration, allows attackers to continue attacking systems, maintain persistence, pivot to new systems, and modify, remove, or delete data. Most breach studies suggest that it takes over 200 days to notice a breach, which is usually found by third parties rather than internal processes or monitoring.

About Domain

What is AliExpress?

The Alibaba Group owns AliExpress, an online retail service based in China. It was founded in 2010 and is made up of small enterprises in China and other countries, including Singapore, that sell to international internet buyers. It is Russia's most popular e-commerce website and Brazil's tenth most popular website. Small enterprises may sell to people all around the world because to it. AliExpress has been compared to eBay because its vendors are self-employed and use the platform to sell their wares to customers.

What is the Alibaba Group?

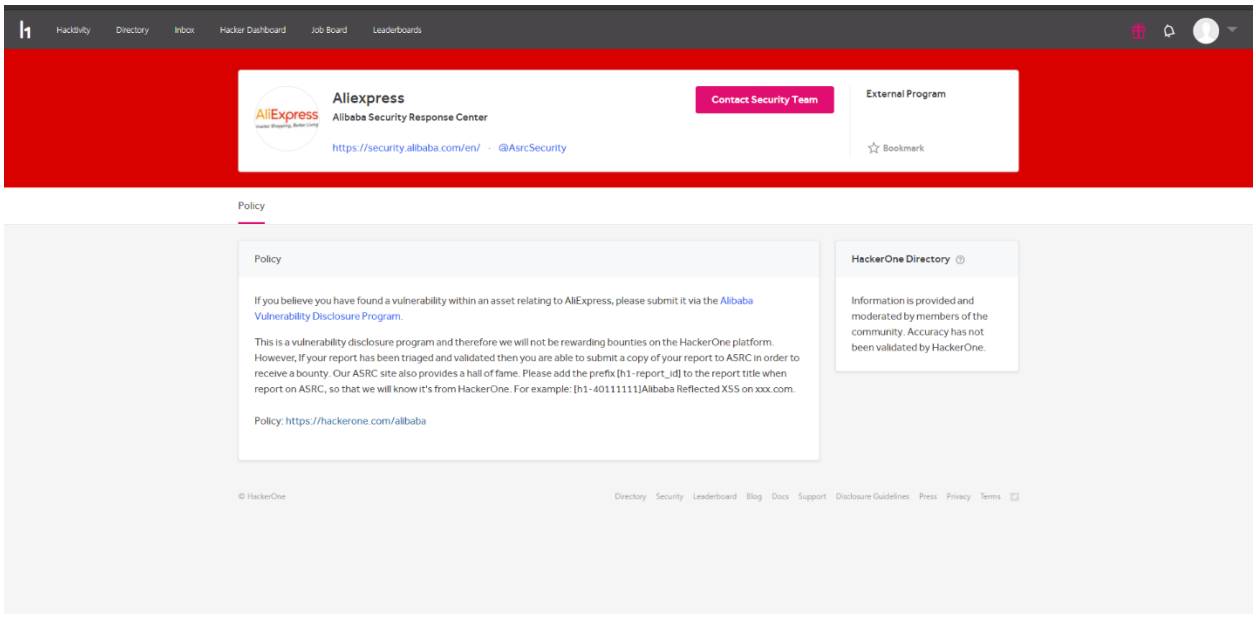
Alibaba Group Holding Limited, usually known as Alibaba Group or Alibaba.com, is a Chinese multinational technology corporation that specializes in e-commerce, retail, the Internet, and technology. The company, which was founded on June 28, 1999 in Hangzhou, Zhejiang, offers web-based consumer-to-consumer (C2C), business-to-consumer (B2C), and business-to-business (B2B) sales services, as well as electronic payment systems, shopping search engines, and cloud computing services. It owns and operates a wide portfolio of businesses in a variety of industries around the world.

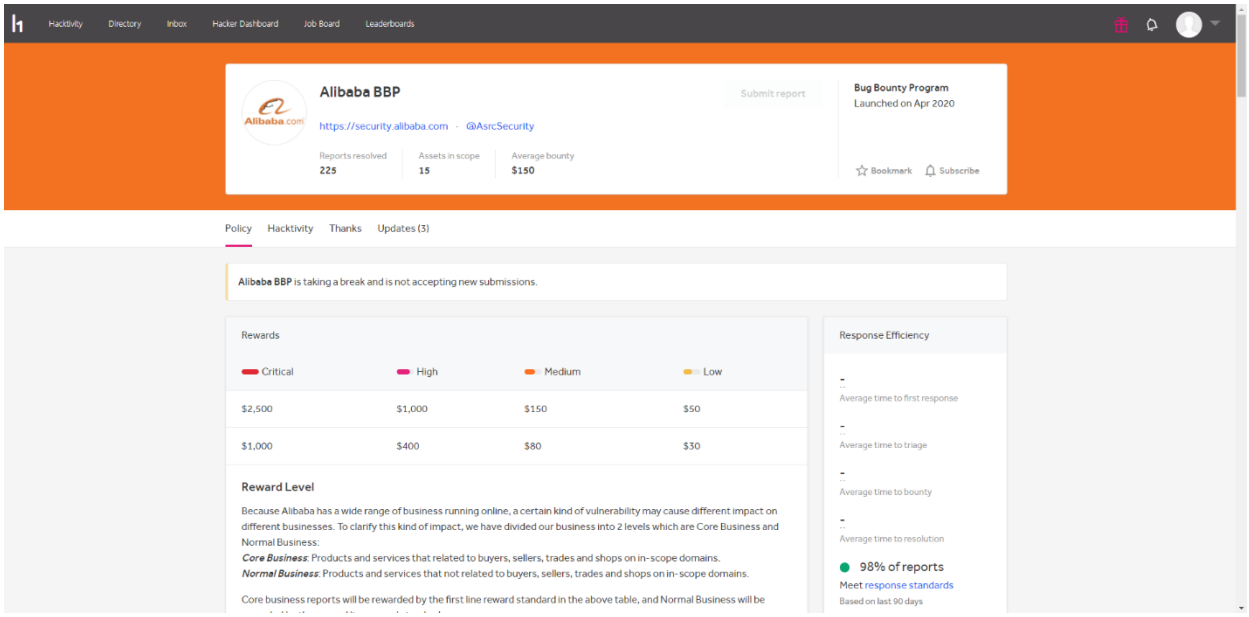
The Alibaba Group, which is headquartered in Hangzhou, China, owns both Alibaba and AliExpress. It was founded by Ma Yun, better known as Jack Ma, the (now ex) Chief Executive. Ma famously applied to Harvard University ten times (and was refused each time) and performed a variety of occupations before finding his destiny as the founder of Alibaba.

HackerOne

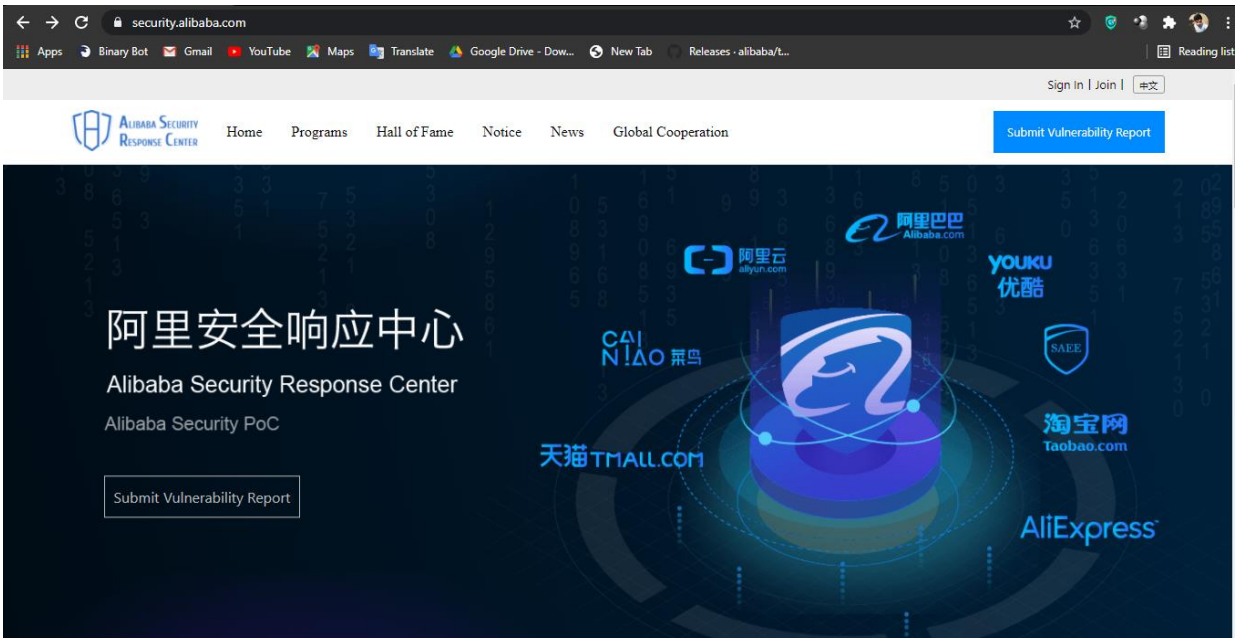
HackerOne is a bug bounty and vulnerability coordination platform that connects companies with penetration testers and cybersecurity experts. Along with Synack and Bugcrowd, it was one of the first organizations to embrace and use crowd-sourced security and cybersecurity researchers as a pillar of its business model; it is the largest cybersecurity firm of its sort. HackerOne's network had handed out $100 million in bounties as of May 2020.

The following details on the aliexpress domain were collected using information received from the HackerOne website.

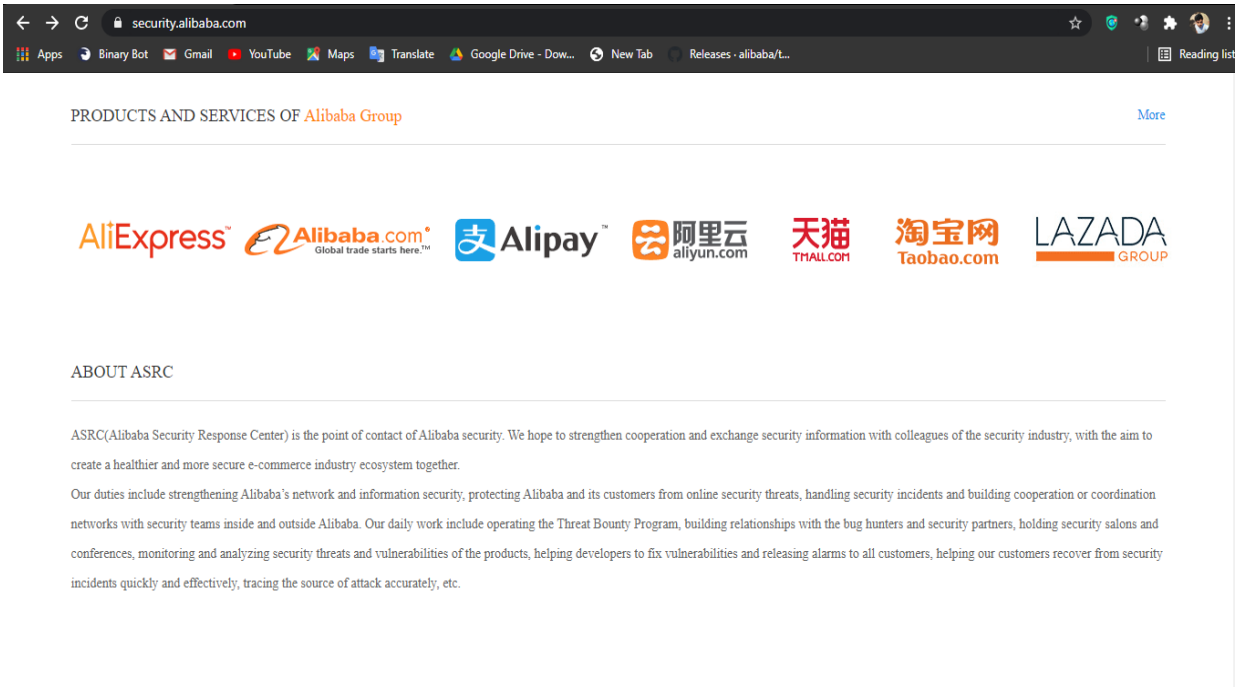




Following is a description of the Alibaba vulnerability disclosure program after studying the above information.



Alibaba Security Response Center



Reconnaissance Phrase (Information Gathering)

Reconnaissance is the most critical aspect of bug hunting or web pen-testing. The main purpose is to obtain and collect as much information on the company we're pursuing as feasible.

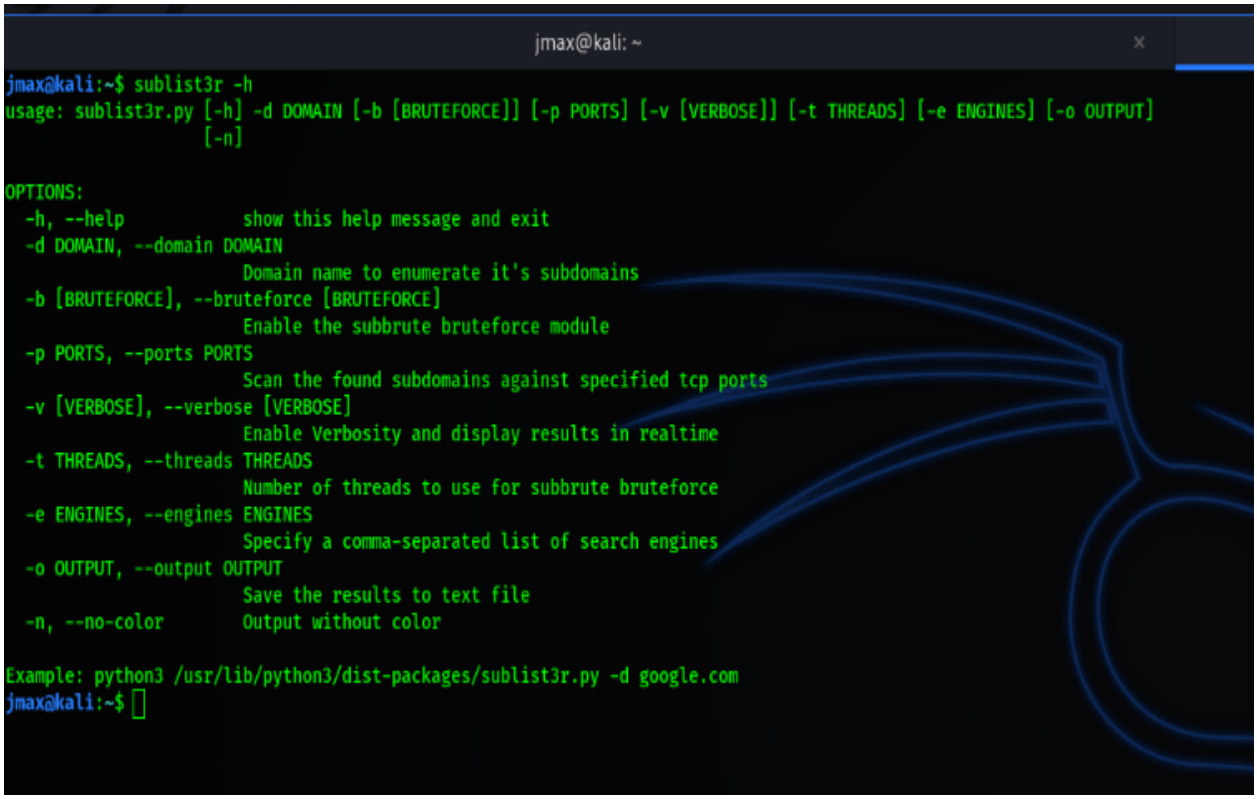
Subdomain Enumeration

1. **Sublist3r**

Sublist3r is a python utility that uses OSINT to enumerate website subdomains. It assists penetration testers and bug hunters in gathering and collecting subdomains for the site they are targeting. Sublist3r uses a variety of search engines to find subdomains, including Google, Yahoo, Bing, Baidu, and Ask.

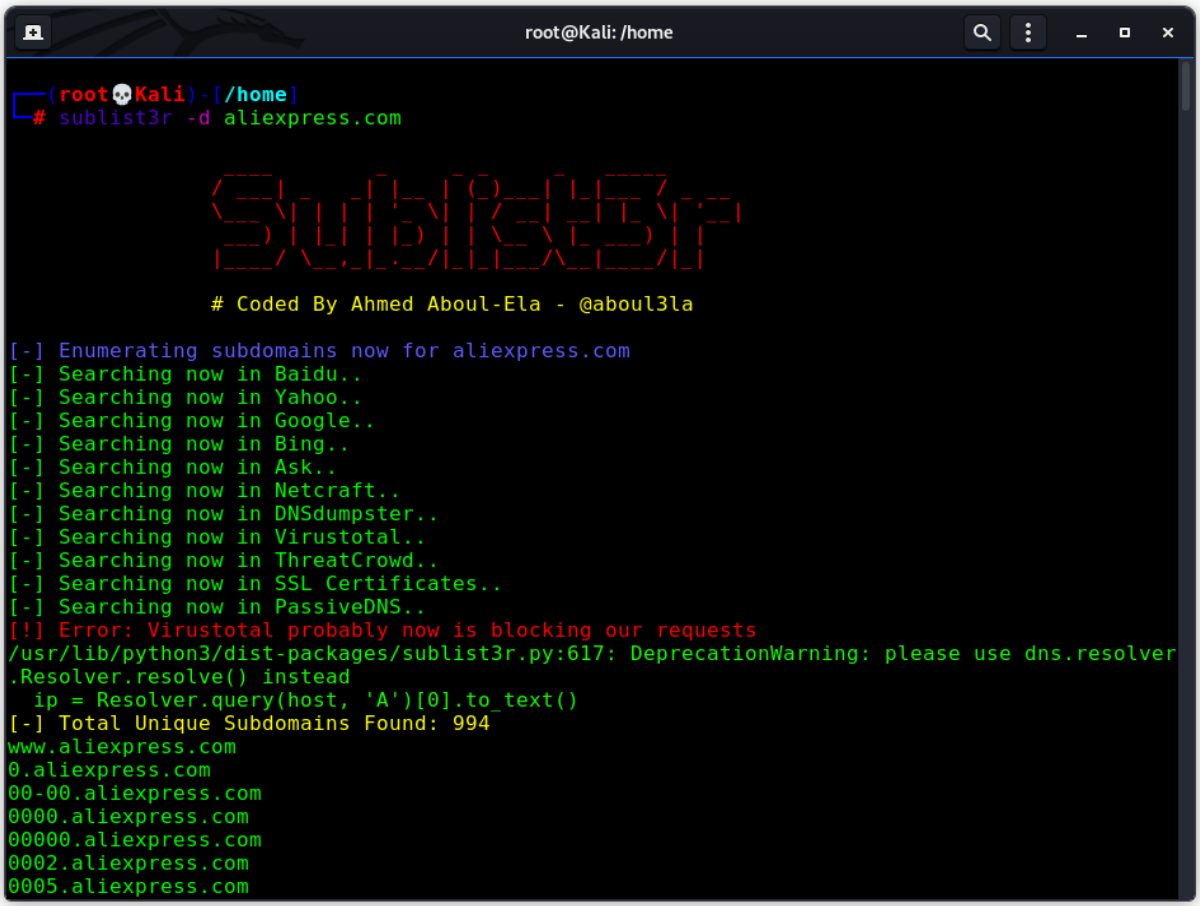
According to my domain that I selected; I used sublist3r tool for enumerating subdomains.

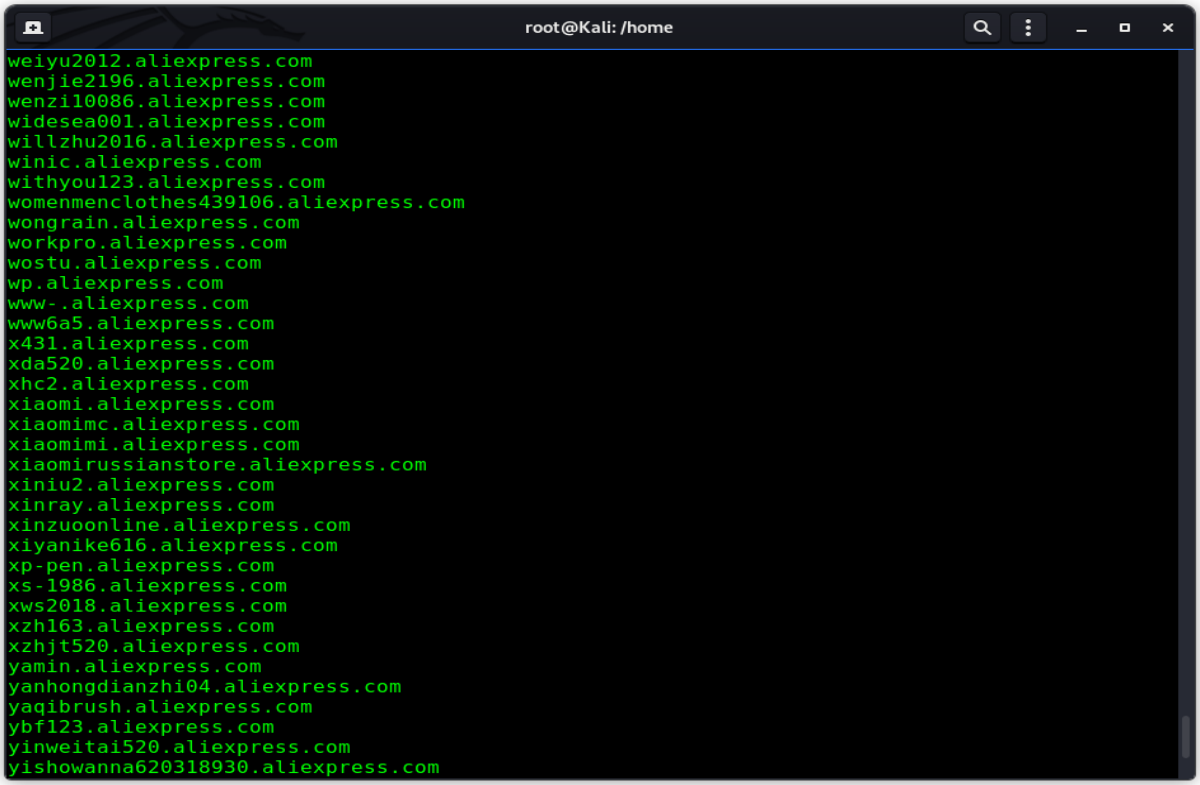
Here is the tool using help commands.

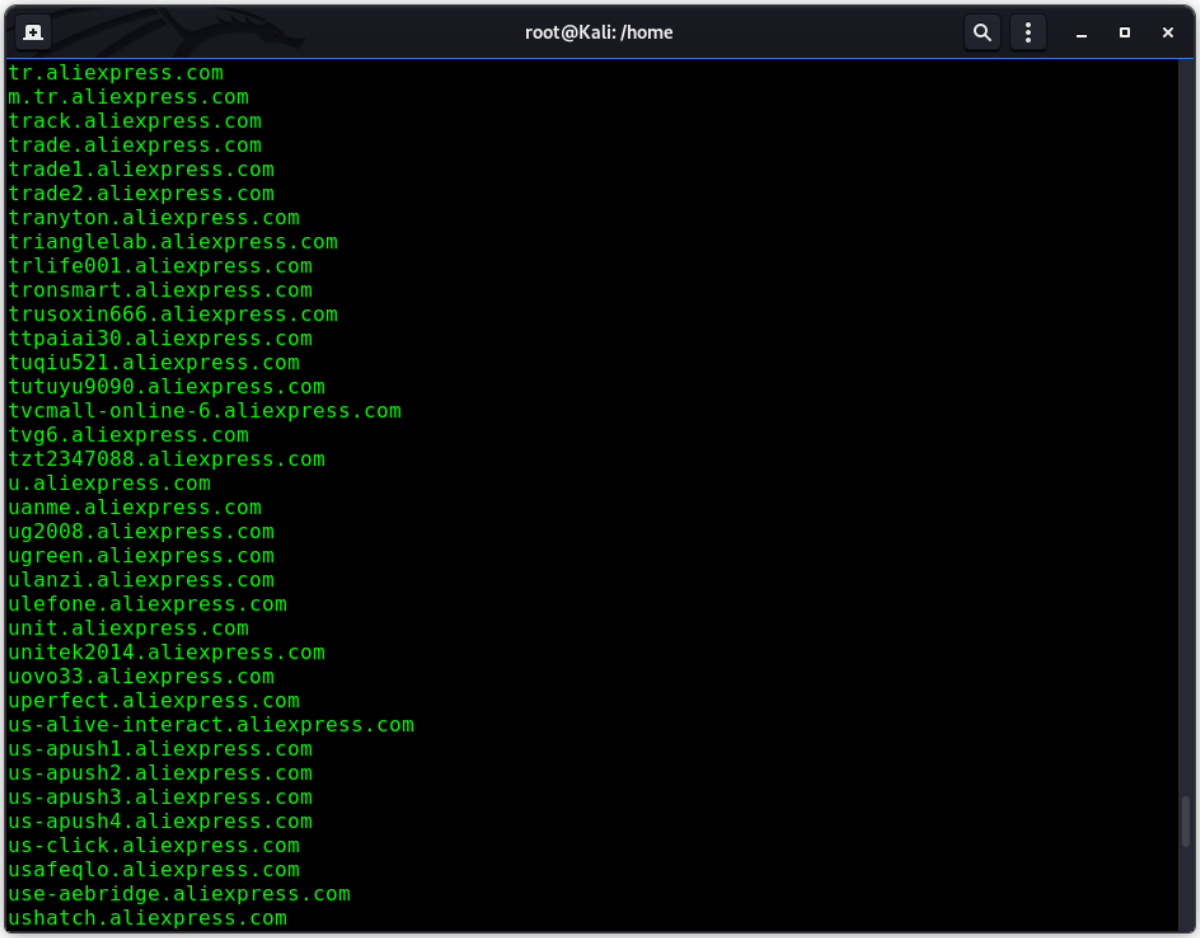


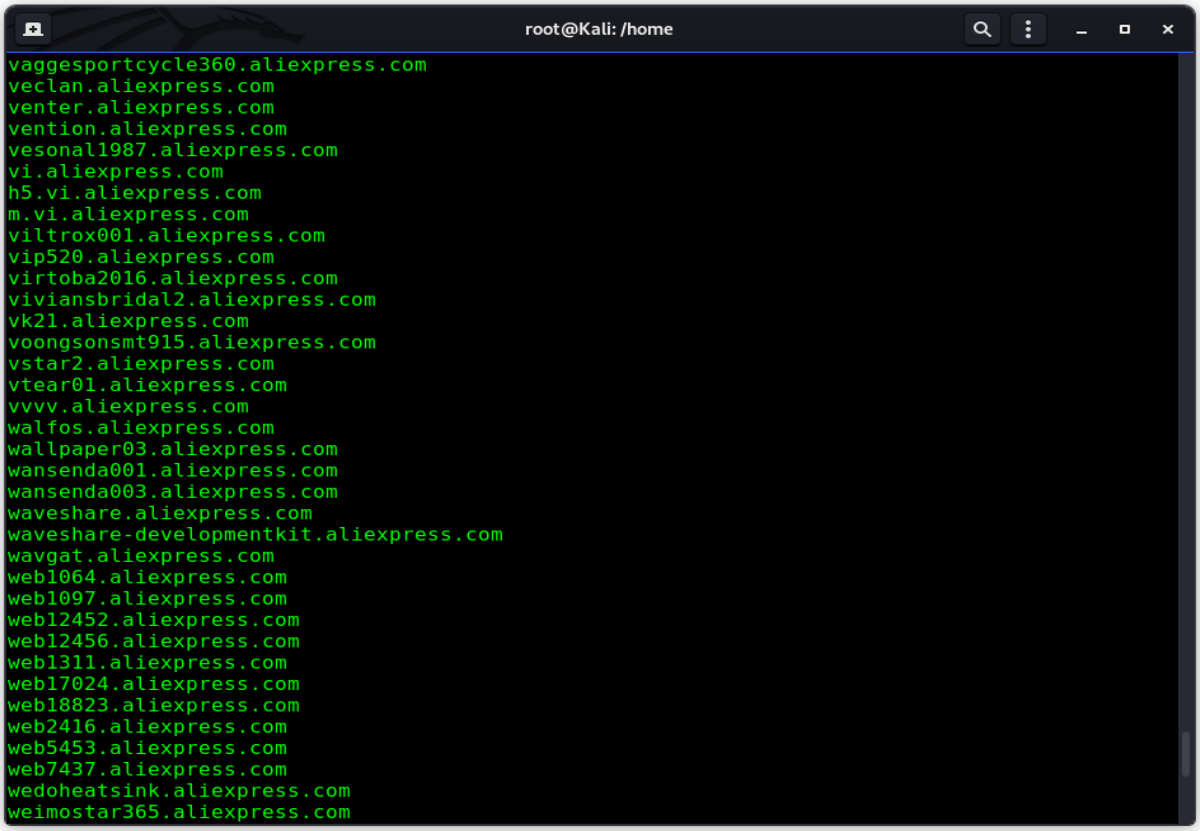
When performing the sublist3r, to enumerate subdomains. We can do a full complete scan adding above functionalities like number of threads and using specific ports etc.

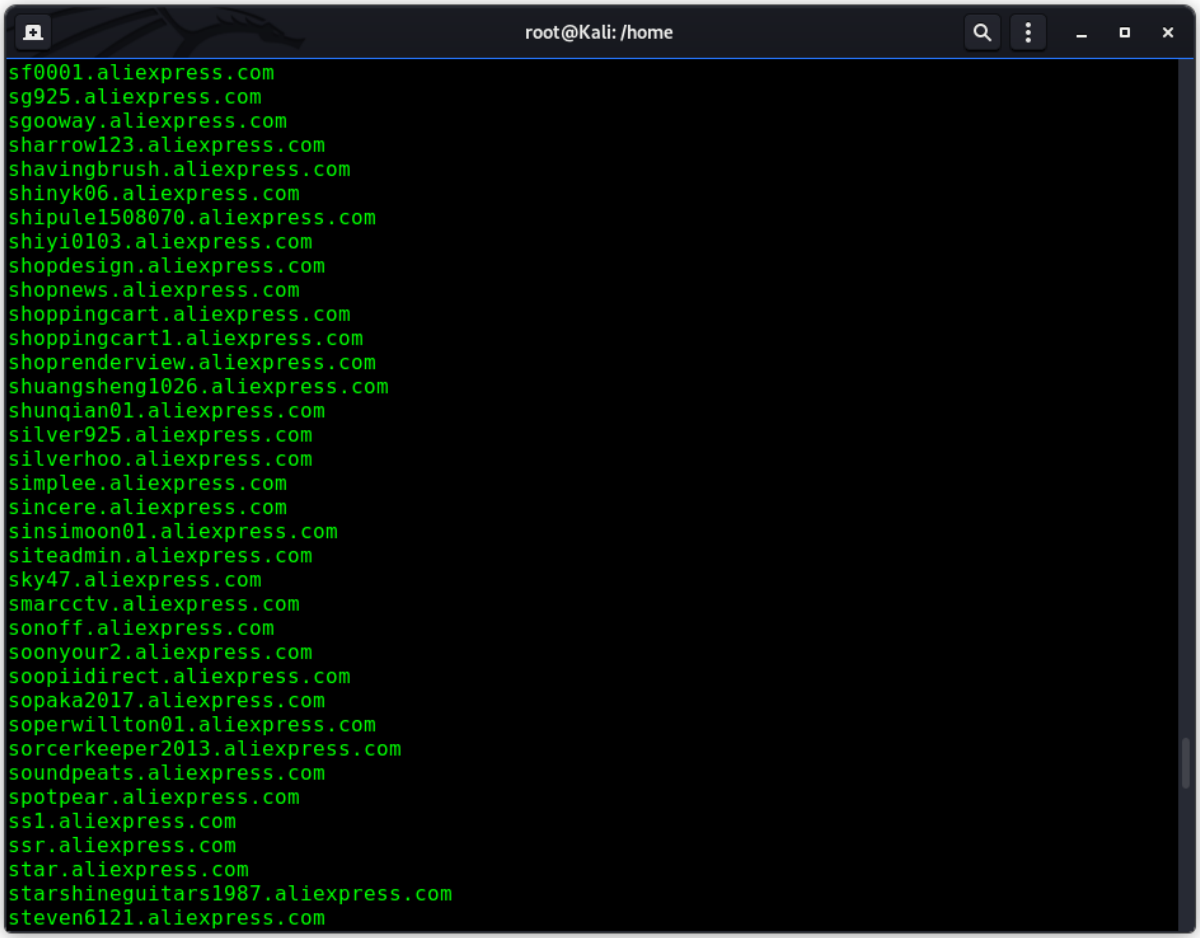
After done the scan I could get the following result sheet.

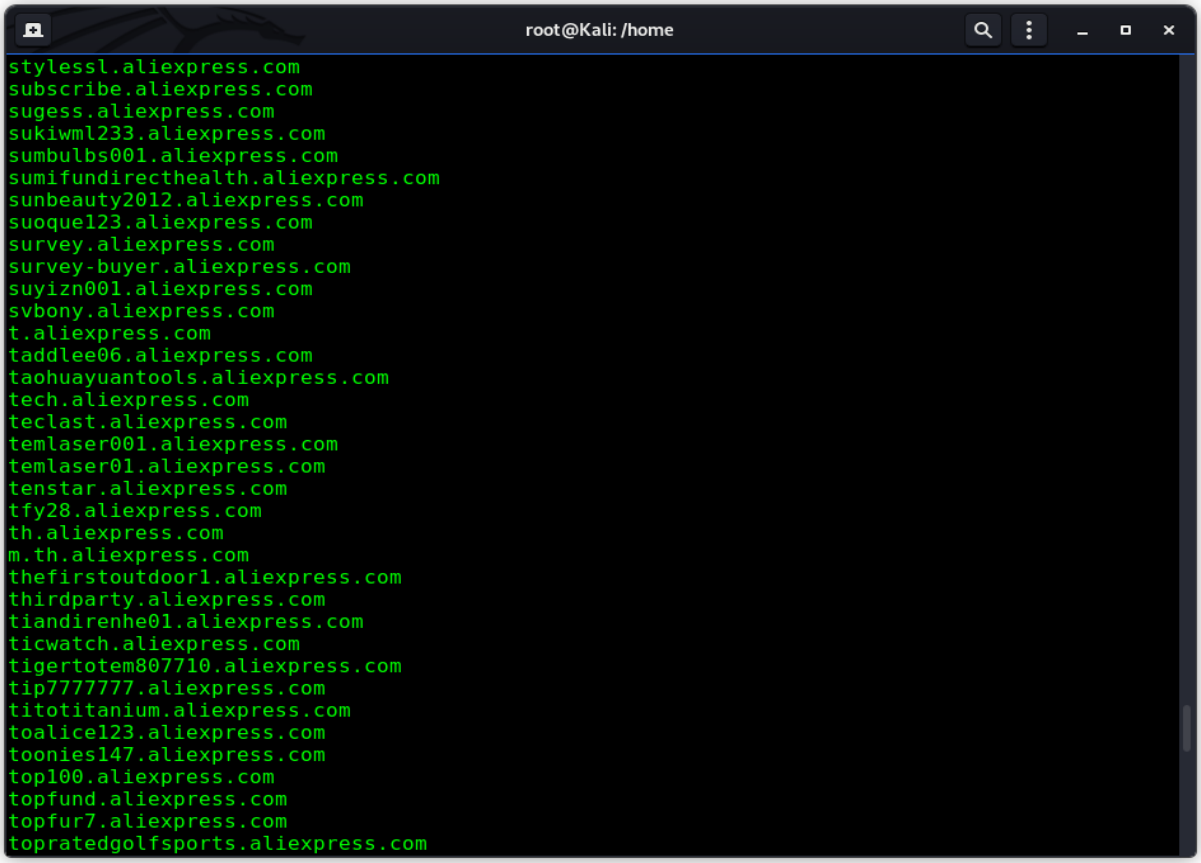

root@Kali: /home
┌──(root💀Kali)-[/home]
└─# sublist3r -d aliexpress.com
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for aliexpress.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
/usr/lib/python3/dist-packages/sublist3r.py:617: DeprecationWarning: please use dns.resolver
.Resolver.resolve() instead
ip = Resolver.query(host, 'A')[0].to_text()
[-] Total Unique Subdomains Found: 994
www.aliexpress.com
0.aliexpress.com
00-00.aliexpress.com
0000.aliexpress.com
00000.aliexpress.com
0002.aliexpress.com
0005.aliexpress.com

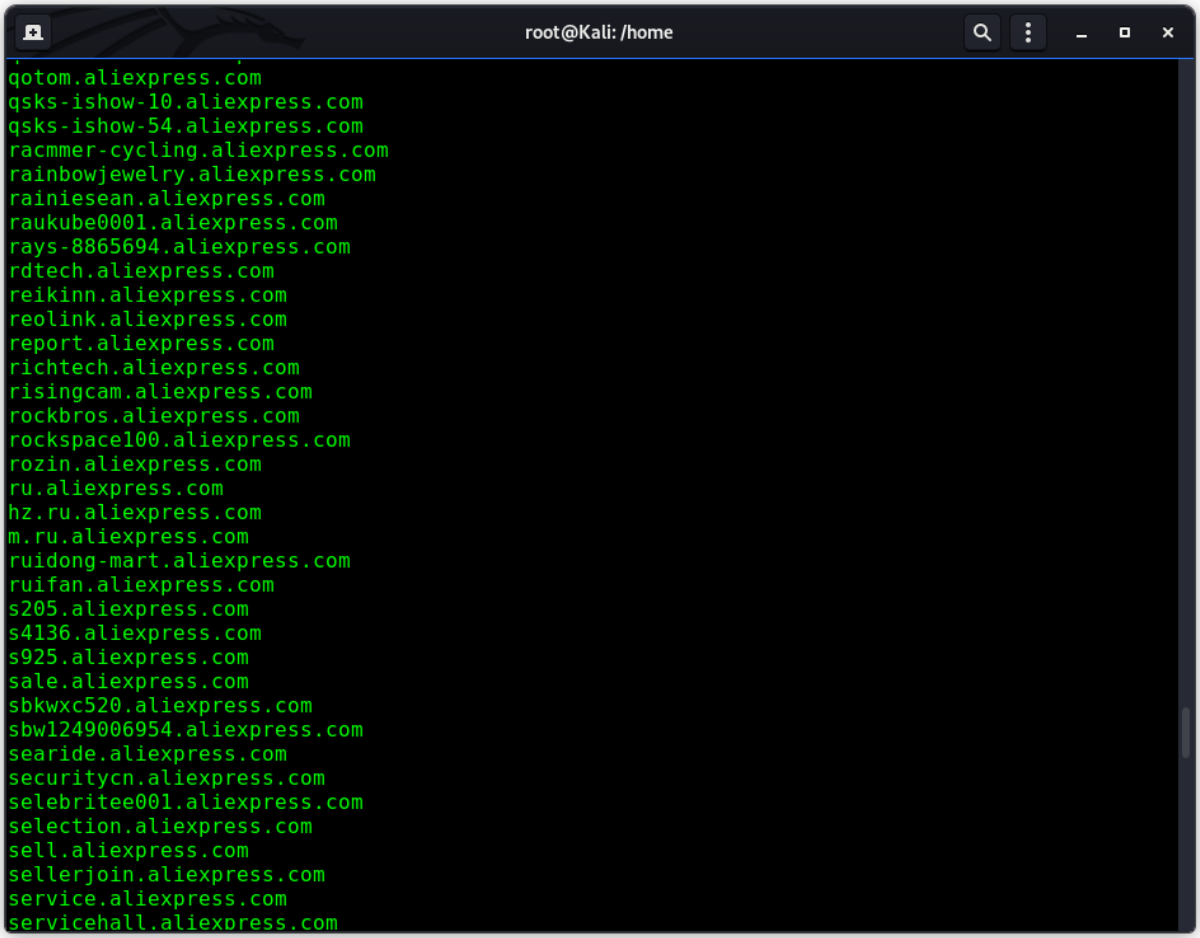

root@Kali: /home
weiyu2012.aliexpress.com
wenjie2196.aliexpress.com
wenzi10086.aliexpress.com
widesea001.aliexpress.com
willzhu2016.aliexpress.com
winic.aliexpress.com
withyou123.aliexpress.com
womenmenclothes439106.aliexpress.com
wongrain.aliexpress.com
workpro.aliexpress.com
wostu.aliexpress.com
wp.aliexpress.com
www-.aliexpress.com
www6a5.aliexpress.com
x431.aliexpress.com
xda520.aliexpress.com
xhc2.aliexpress.com
xiaomi.aliexpress.com
xiaomimc.aliexpress.com
xiaomimi.aliexpress.com
xiaomirussianstore.aliexpress.com
xiniu2.aliexpress.com
xinray.aliexpress.com
xinzuoonline.aliexpress.com
xiyanike616.aliexpress.com
xp-pen.aliexpress.com
xs-1986.aliexpress.com
xws2018.aliexpress.com
xzh163.aliexpress.com
xzhjt520.aliexpress.com
yamin.aliexpress.com
yanhongdianzhi04.aliexpress.com
yaqibrush.aliexpress.com
ybf123.aliexpress.com
yinweitai520.aliexpress.com
yishowanna620318930.aliexpress.com

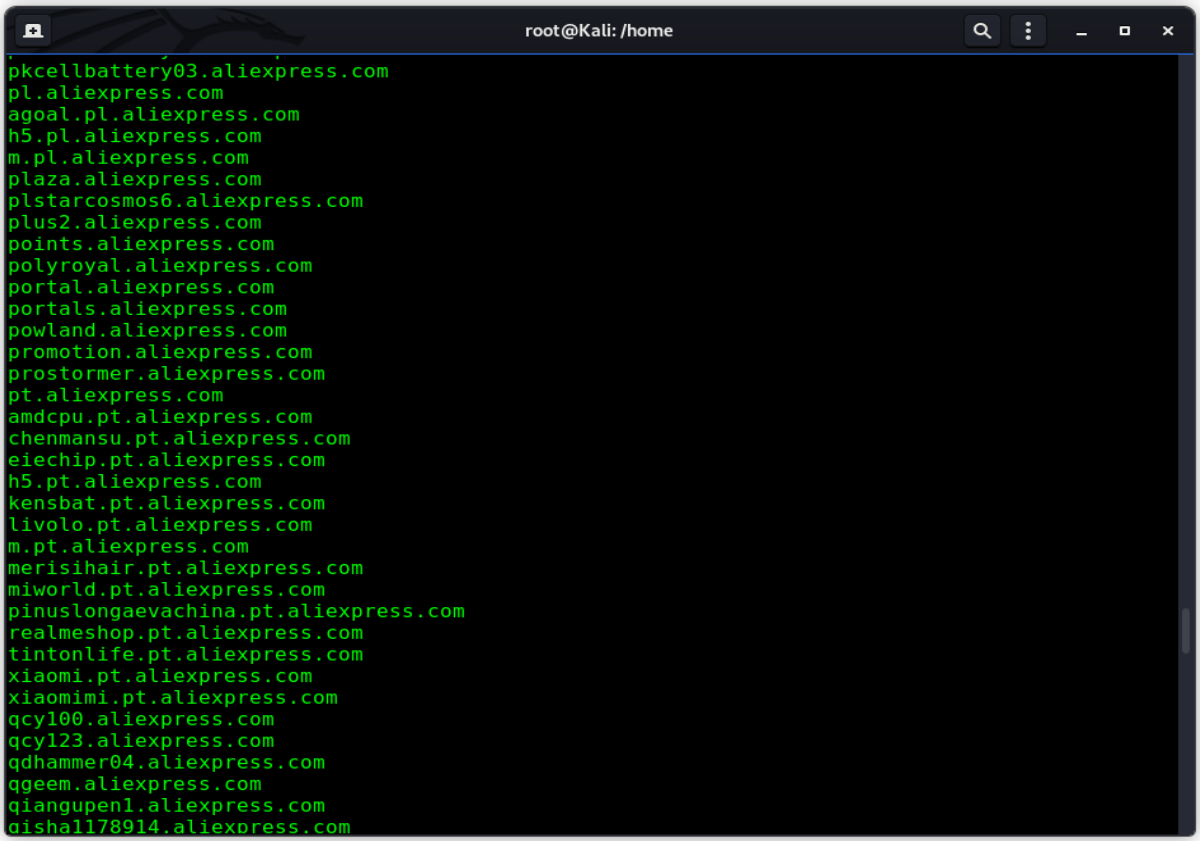

root@Kali: /home
tr.aliexpress.com
m.tr.aliexpress.com
track.aliexpress.com
trade.aliexpress.com
trade1.aliexpress.com
trade2.aliexpress.com
tranyton.aliexpress.com
trianglelab.aliexpress.com
trlife001.aliexpress.com
tronsmart.aliexpress.com
trusoxin666.aliexpress.com
ttpaiai30.aliexpress.com
tuqiu521.aliexpress.com
tutuyu9090.aliexpress.com
tvcmall-online-6.aliexpress.com
tvg6.aliexpress.com
tzt2347088.aliexpress.com
u.aliexpress.com
uanme.aliexpress.com
ug2008.aliexpress.com
ugreen.aliexpress.com
ulanzi.aliexpress.com
ulefone.aliexpress.com
unit.aliexpress.com
unitek2014.aliexpress.com
uovo33.aliexpress.com
uperfect.aliexpress.com
us-alive-interact.aliexpress.com
us-apush1.aliexpress.com
us-apush2.aliexpress.com
us-apush3.aliexpress.com
us-apush4.aliexpress.com
us-click.aliexpress.com
usafeqlo.aliexpress.com
use-aebridge.aliexpress.com
ushatch.aliexpress.com

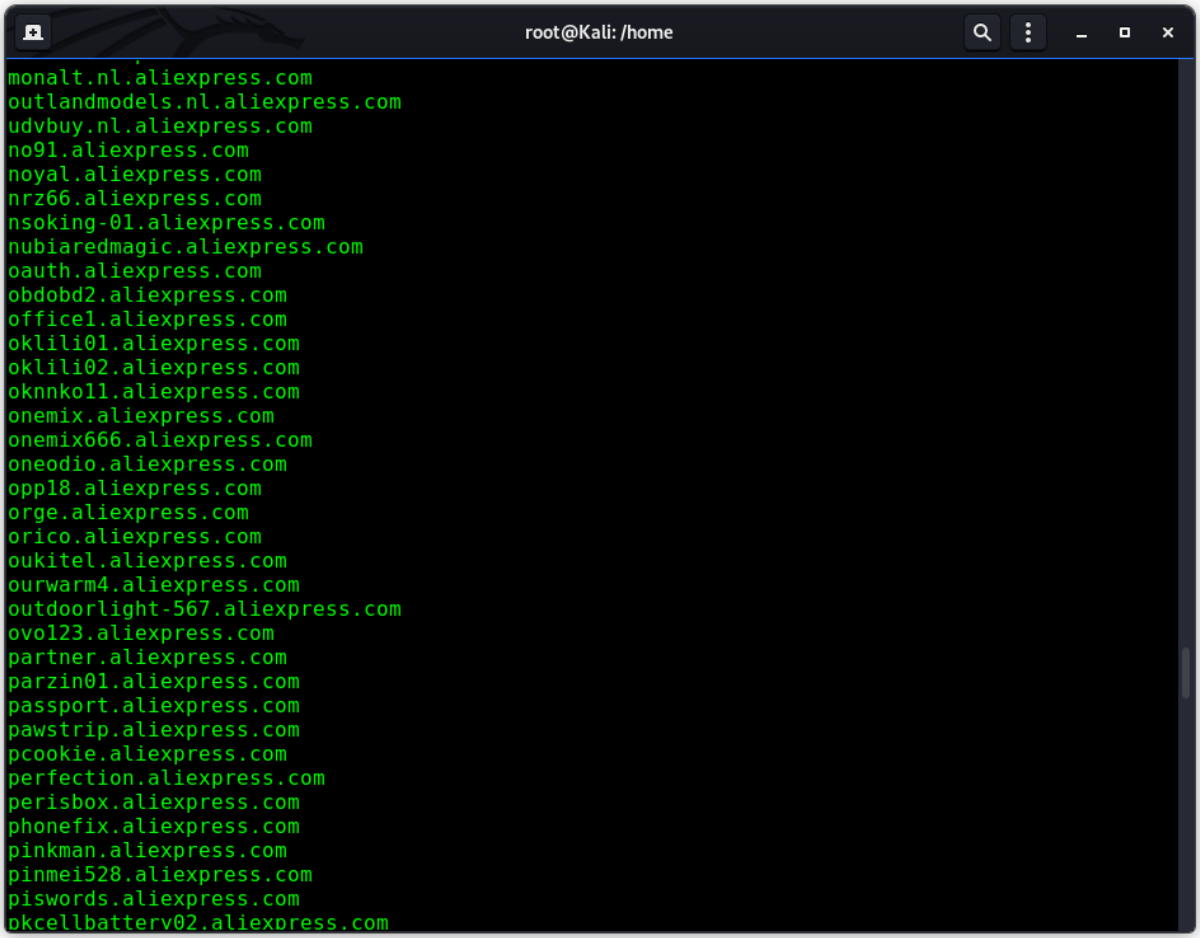

root@Kali: /home
vaggesportcycle360.aliexpress.com
veclan.aliexpress.com
venter.aliexpress.com
vention.aliexpress.com
vesonal1987.aliexpress.com
vi.aliexpress.com
h5.vi.aliexpress.com
m.vi.aliexpress.com
viltrox001.aliexpress.com
vip520.aliexpress.com
virtoba2016.aliexpress.com
viviansbridal2.aliexpress.com
vk21.aliexpress.com
voongsonsmt915.aliexpress.com
vstar2.aliexpress.com
vtear01.aliexpress.com
vvvv.aliexpress.com
walfos.aliexpress.com
wallpaper03.aliexpress.com
wansenda001.aliexpress.com
wansenda003.aliexpress.com
waveshare.aliexpress.com
waveshare-developmentkit.aliexpress.com
wavgat.aliexpress.com
web1064.aliexpress.com
web1097.aliexpress.com
web12452.aliexpress.com
web12456.aliexpress.com
web1311.aliexpress.com
web17024.aliexpress.com
web18823.aliexpress.com
web2416.aliexpress.com
web5453.aliexpress.com
web7437.aliexpress.com
wedoheatsink.aliexpress.com
weimostar365.aliexpress.com

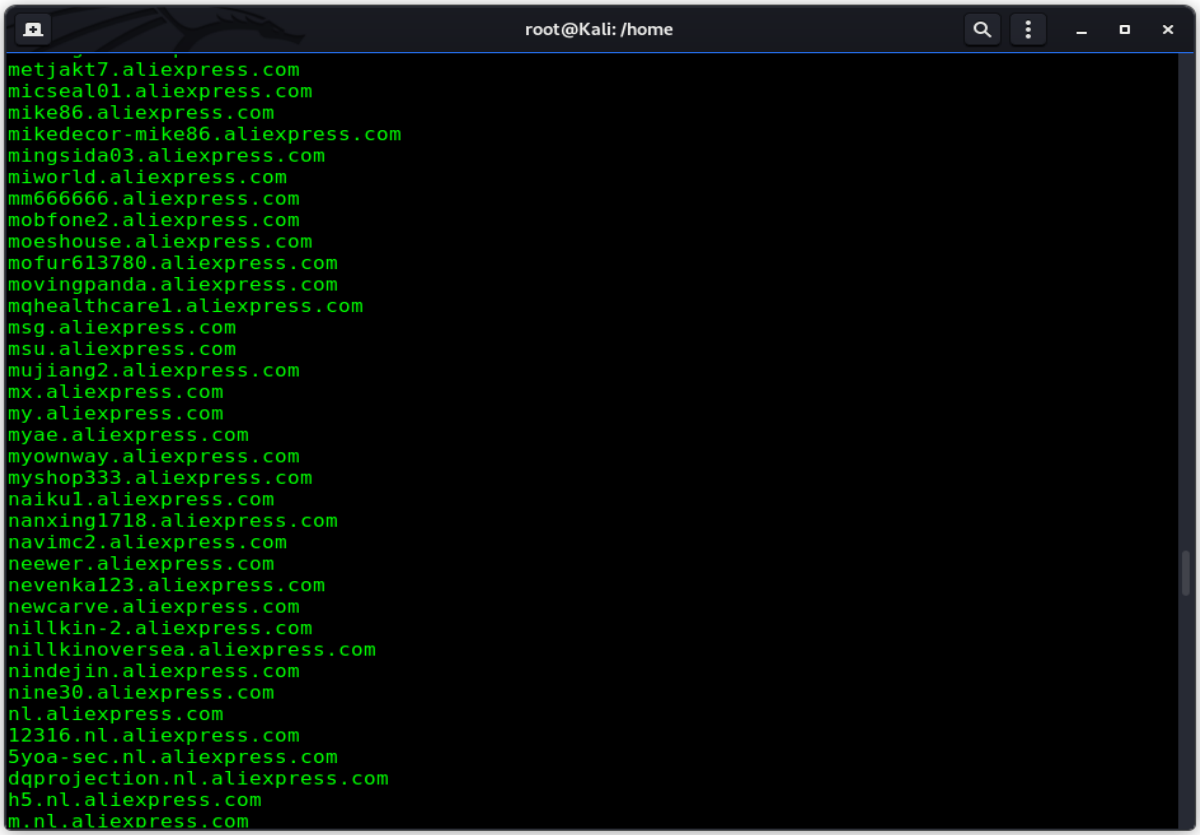

root@Kali: /home
sf0001.aliexpress.com
sg925.aliexpress.com
sgooway.aliexpress.com
sharrow123.aliexpress.com
shavingbrush.aliexpress.com
shinyk06.aliexpress.com
shipule1508070.aliexpress.com
shiyi0103.aliexpress.com
shopdesign.aliexpress.com
shopnews.aliexpress.com
shoppingcart.aliexpress.com
shoppingcart1.aliexpress.com
shoprenderview.aliexpress.com
shuangsheng1026.aliexpress.com
shunqian01.aliexpress.com
silver925.aliexpress.com
silverhoo.aliexpress.com
simplee.aliexpress.com
sincere.aliexpress.com
sinsimoon01.aliexpress.com
siteadmin.aliexpress.com
sky47.aliexpress.com
smarcctv.aliexpress.com
sonoff.aliexpress.com
soonyour2.aliexpress.com
soopiidirect.aliexpress.com
sopaka2017.aliexpress.com
soperwillton01.aliexpress.com
sorcerkeeper2013.aliexpress.com
soundpeats.aliexpress.com
spotpear.aliexpress.com
ss1.aliexpress.com
ssr.aliexpress.com
star.aliexpress.com
starshineguitars1987.aliexpress.com
steven6121.aliexpress.com

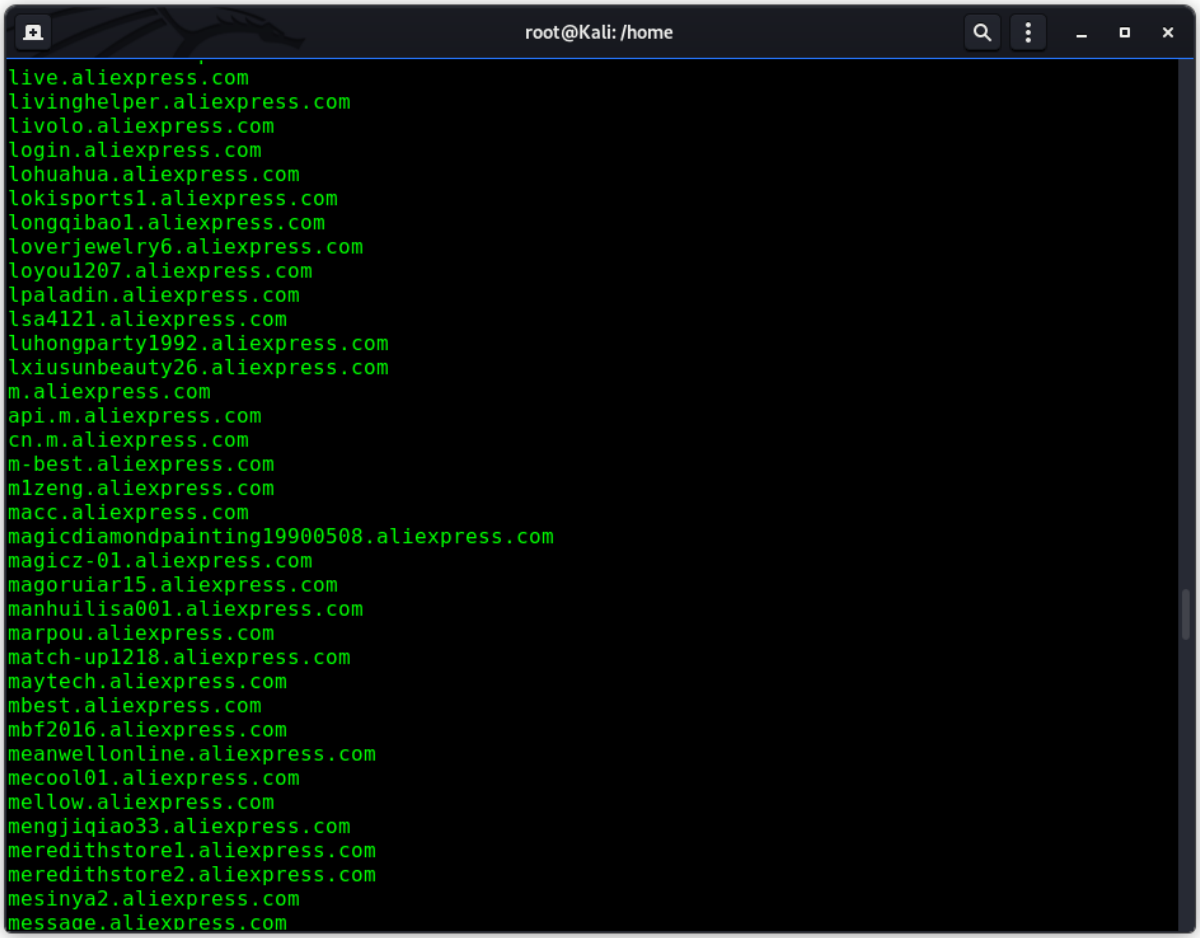

root@Kali: /home
stylessl.aliexpress.com
subscribe.aliexpress.com
sugess.aliexpress.com
sukiwml233.aliexpress.com
sumbulbs001.aliexpress.com
sumifundirecthealth.aliexpress.com
sunbeauty2012.aliexpress.com
suoque123.aliexpress.com
survey.aliexpress.com
survey-buyer.aliexpress.com
suyizn001.aliexpress.com
svbony.aliexpress.com
t.aliexpress.com
taddlee06.aliexpress.com
taohuayuantools.aliexpress.com
tech.aliexpress.com
teclast.aliexpress.com
temlaser001.aliexpress.com
temlaser01.aliexpress.com
tenstar.aliexpress.com
tfy28.aliexpress.com
th.aliexpress.com
m.th.aliexpress.com
thefirstoutdoor1.aliexpress.com
thirdparty.aliexpress.com
tiandirenhe01.aliexpress.com
ticwatch.aliexpress.com
tigertotem807710.aliexpress.com
tip7777777.aliexpress.com
titotitanium.aliexpress.com
toalice123.aliexpress.com
toonies147.aliexpress.com
top100.aliexpress.com
topfund.aliexpress.com
topfur7.aliexpress.com
topratedgolfsports.aliexpress.com

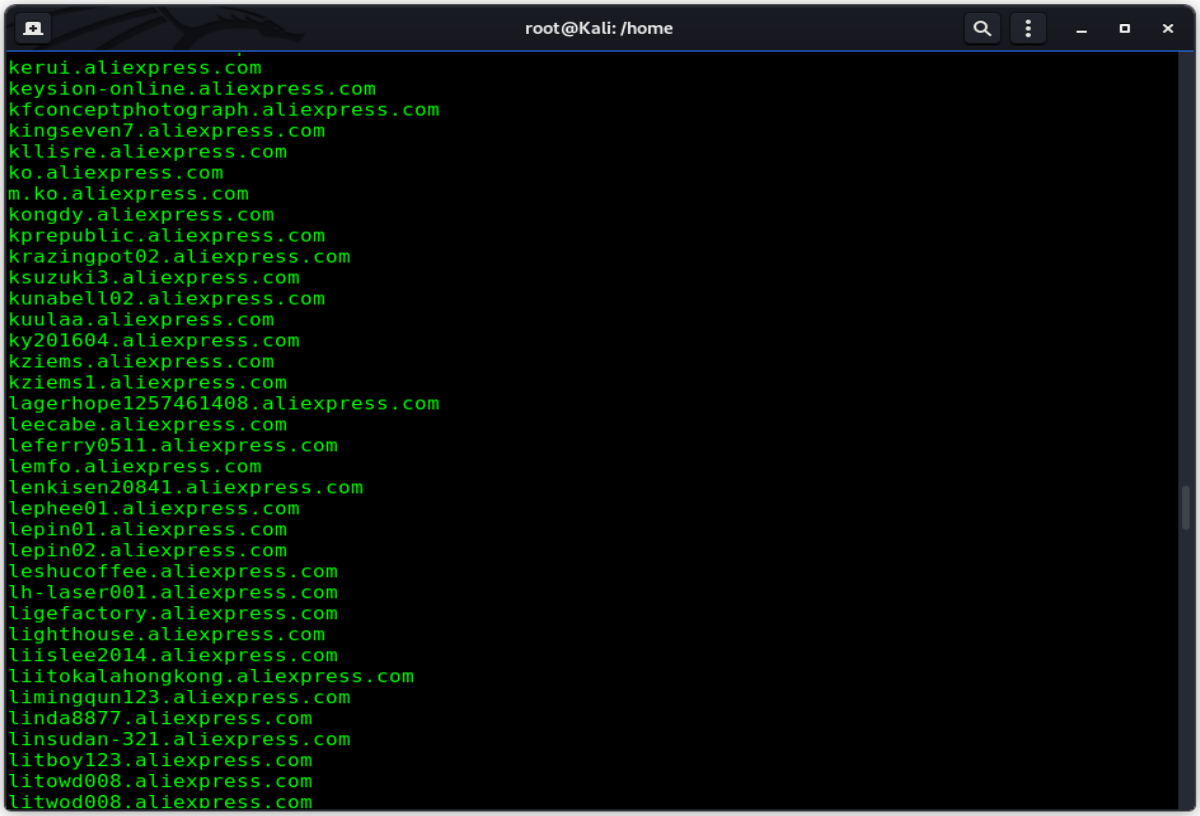

root@Kali: /home
qotom.aliexpress.com
qsks-ishow-10.aliexpress.com
qsks-ishow-54.aliexpress.com
racmmer-cycling.aliexpress.com
rainbowjewelry.aliexpress.com
rainiesean.aliexpress.com
raukube0001.aliexpress.com
rays-8865694.aliexpress.com
rdtech.aliexpress.com
reikinn.aliexpress.com
reolink.aliexpress.com
report.aliexpress.com
richtech.aliexpress.com
risingcam.aliexpress.com
rockbros.aliexpress.com
rockspace100.aliexpress.com
rozin.aliexpress.com
ru.aliexpress.com
hz.ru.aliexpress.com
m.ru.aliexpress.com
ruidong-mart.aliexpress.com
ruifan.aliexpress.com
s205.aliexpress.com
s4136.aliexpress.com
s925.aliexpress.com
sale.aliexpress.com
sbkwxc520.aliexpress.com
sbw1249006954.aliexpress.com
searide.aliexpress.com
securitycn.aliexpress.com
selebritee001.aliexpress.com
selection.aliexpress.com
sell.aliexpress.com
sellerjoin.aliexpress.com
service.aliexpress.com
servicehall.aliexpress.com

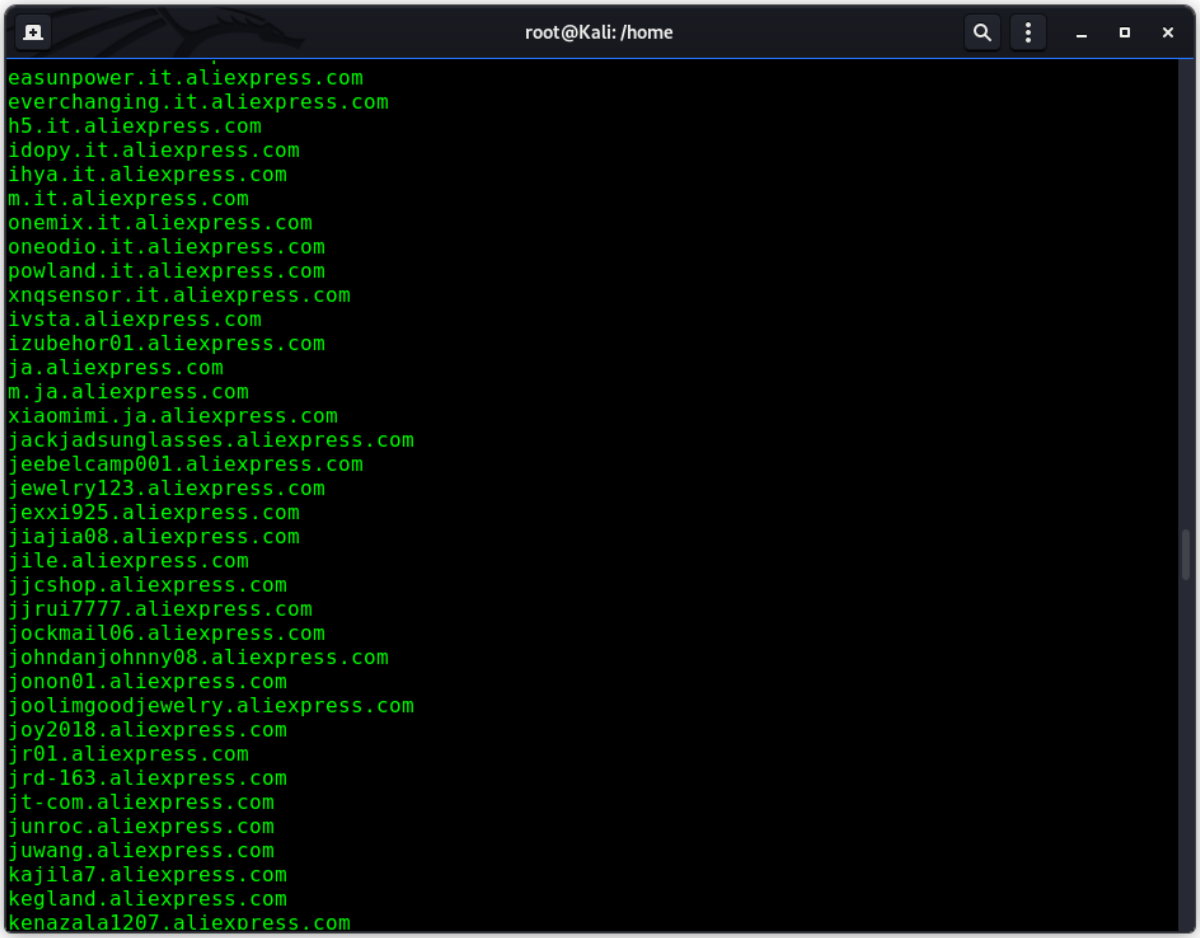

root@Kali: /home
pkcellbattery03.aliexpress.com
pl.aliexpress.com
agoal.pl.aliexpress.com
h5.pl.aliexpress.com
m.pl.aliexpress.com
plaza.aliexpress.com
plstarcosmos6.aliexpress.com
plus2.aliexpress.com
points.aliexpress.com
polyroyal.aliexpress.com
portal.aliexpress.com
portals.aliexpress.com
powland.aliexpress.com
promotion.aliexpress.com
prostormer.aliexpress.com
pt.aliexpress.com
amdcpu.pt.aliexpress.com
chenmansu.pt.aliexpress.com
eiechip.pt.aliexpress.com
h5.pt.aliexpress.com
kensbat.pt.aliexpress.com
livolo.pt.aliexpress.com
m.pt.aliexpress.com
merisihair.pt.aliexpress.com
miworld.pt.aliexpress.com
pinuslongaevachina.pt.aliexpress.com
realmeshop.pt.aliexpress.com
tintonlife.pt.aliexpress.com
xiaomi.pt.aliexpress.com
xiaomimi.pt.aliexpress.com
qcy100.aliexpress.com
qcy123.aliexpress.com
qdhammer04.aliexpress.com
qgeem.aliexpress.com
qiangupen1.aliexpress.com
qisha1178914.aliexpress.com

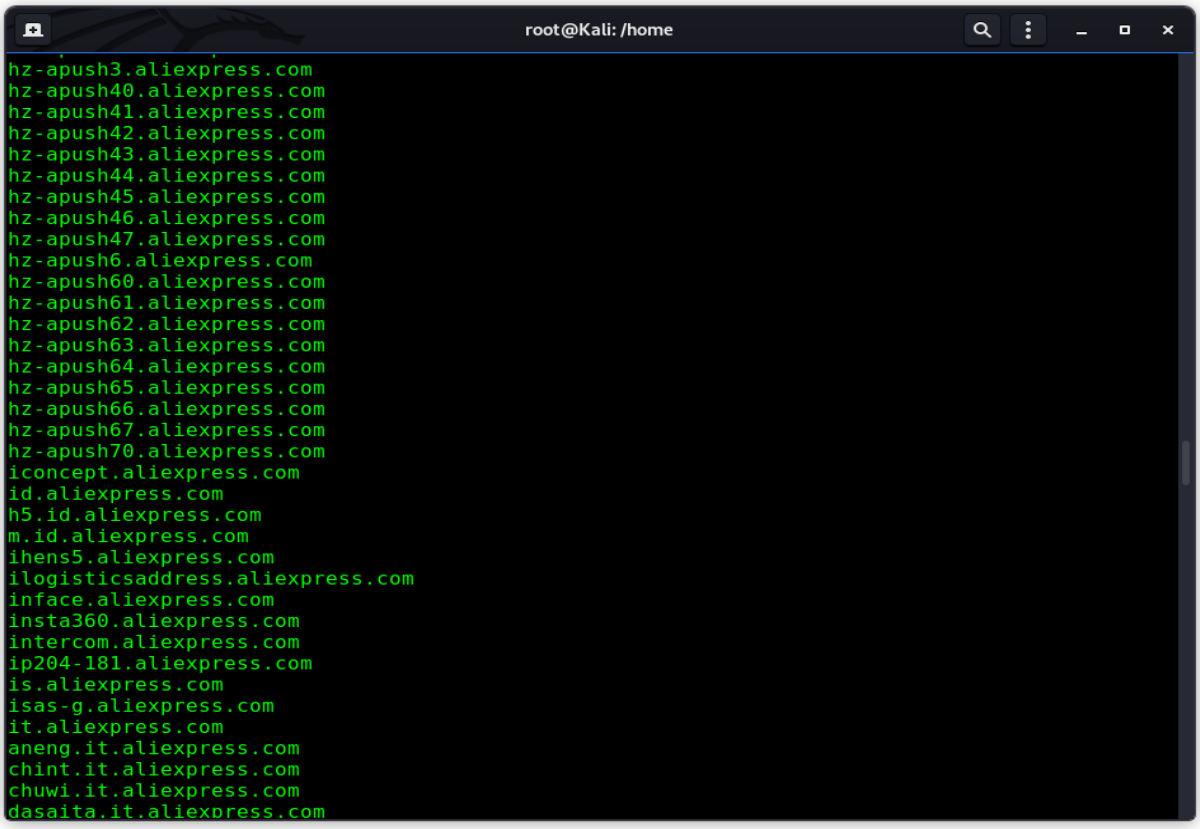

root@Kali: /home
monalt.nl.aliexpress.com
outlandmodels.nl.aliexpress.com
udvbuy.nl.aliexpress.com
no91.aliexpress.com
noyal.aliexpress.com
nrz66.aliexpress.com
nsoking-01.aliexpress.com
nubiaredmagic.aliexpress.com
oauth.aliexpress.com
obdobd2.aliexpress.com
office1.aliexpress.com
oklili01.aliexpress.com
oklili02.aliexpress.com
oknnko11.aliexpress.com
onemix.aliexpress.com
onemix666.aliexpress.com
oneodio.aliexpress.com
opp18.aliexpress.com
orge.aliexpress.com
orico.aliexpress.com
oukitel.aliexpress.com
ourwarm4.aliexpress.com
outdoorlight-567.aliexpress.com
ovo123.aliexpress.com
partner.aliexpress.com
parzin01.aliexpress.com
passport.aliexpress.com
pawstrip.aliexpress.com
pcookie.aliexpress.com
perfection.aliexpress.com
perisbox.aliexpress.com
phonefix.aliexpress.com
pinkman.aliexpress.com
pinmei528.aliexpress.com
piswords.aliexpress.com
pkcellbattery02.aliexpress.com

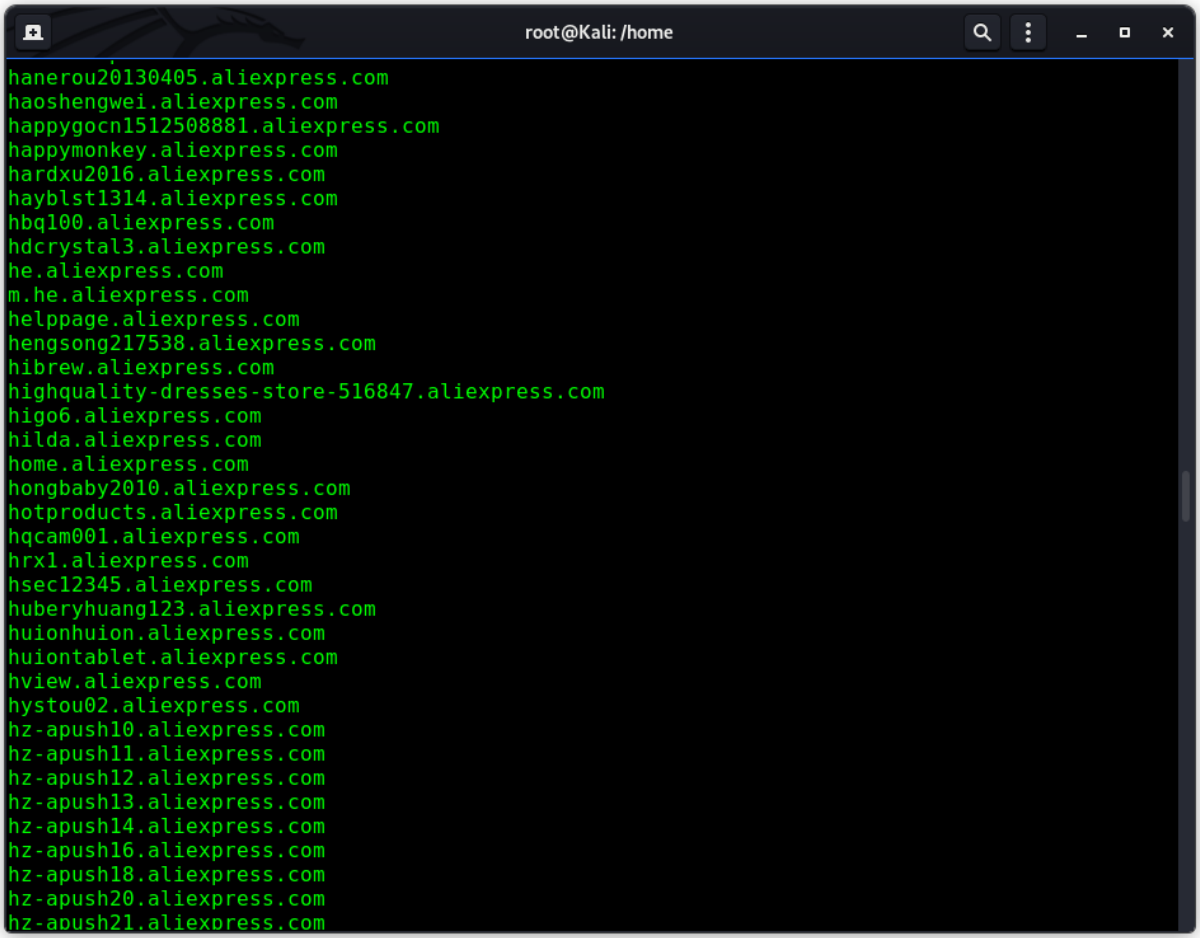

root@Kali: /home
metjakt7.aliexpress.com
micseal01.aliexpress.com
mike86.aliexpress.com
mikedecor-mike86.aliexpress.com
mingsida03.aliexpress.com
miworld.aliexpress.com
mm666666.aliexpress.com
mobfone2.aliexpress.com
moeshouse.aliexpress.com
mofur613780.aliexpress.com
movingpanda.aliexpress.com
mqhealthcare1.aliexpress.com
msg.aliexpress.com
msu.aliexpress.com
mujiang2.aliexpress.com
mx.aliexpress.com
my.aliexpress.com
myae.aliexpress.com
myownway.aliexpress.com
myshop333.aliexpress.com
naiku1.aliexpress.com
nanxing1718.aliexpress.com
navimc2.aliexpress.com
neewer.aliexpress.com
nevenka123.aliexpress.com
newcarve.aliexpress.com
nillkin-2.aliexpress.com
nillkinoversea.aliexpress.com
nindejin.aliexpress.com
nine30.aliexpress.com
nl.aliexpress.com
12316.nl.aliexpress.com
5yoa-sec.nl.aliexpress.com
dqprojection.nl.aliexpress.com
h5.nl.aliexpress.com
m.nl.aliexpress.com

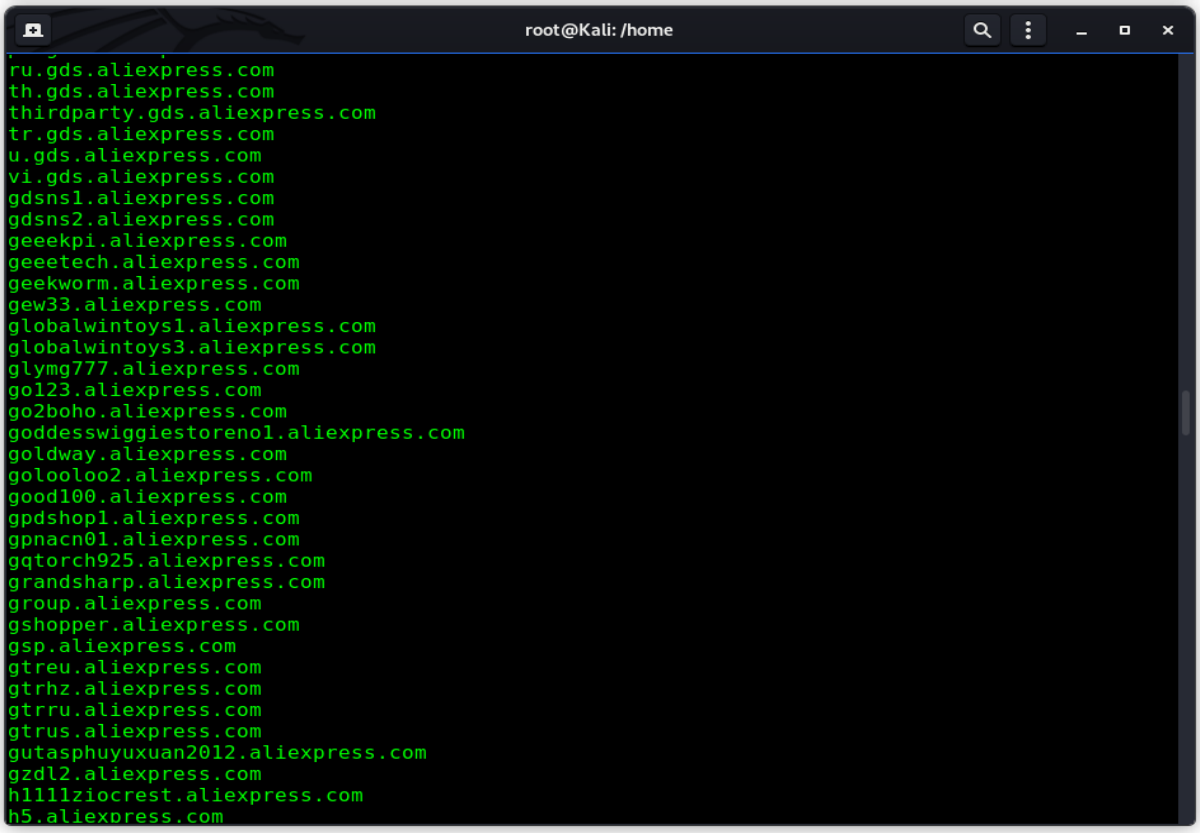

root@Kali: /home
live.aliexpress.com
livinghelper.aliexpress.com
livolo.aliexpress.com
login.aliexpress.com
lohuahua.aliexpress.com
lokisports1.aliexpress.com
longqibao1.aliexpress.com
loverjewelry6.aliexpress.com
loyou1207.aliexpress.com
lpaladin.aliexpress.com
lsa4121.aliexpress.com
luhongparty1992.aliexpress.com
lxiusunbeauty26.aliexpress.com
m.aliexpress.com
api.m.aliexpress.com
cn.m.aliexpress.com
m-best.aliexpress.com
m1zeng.aliexpress.com
macc.aliexpress.com
magicdiamondpainting19900508.aliexpress.com
magicz-01.aliexpress.com
magoruiar15.aliexpress.com
manhuilisa001.aliexpress.com
marpou.aliexpress.com
match-up1218.aliexpress.com
maytech.aliexpress.com
mbest.aliexpress.com
mbf2016.aliexpress.com
meanwellonline.aliexpress.com
mecool01.aliexpress.com
mellow.aliexpress.com
mengjiqiao33.aliexpress.com
meredithstore1.aliexpress.com
meredithstore2.aliexpress.com
mesinya2.aliexpress.com
message.aliexpress.com

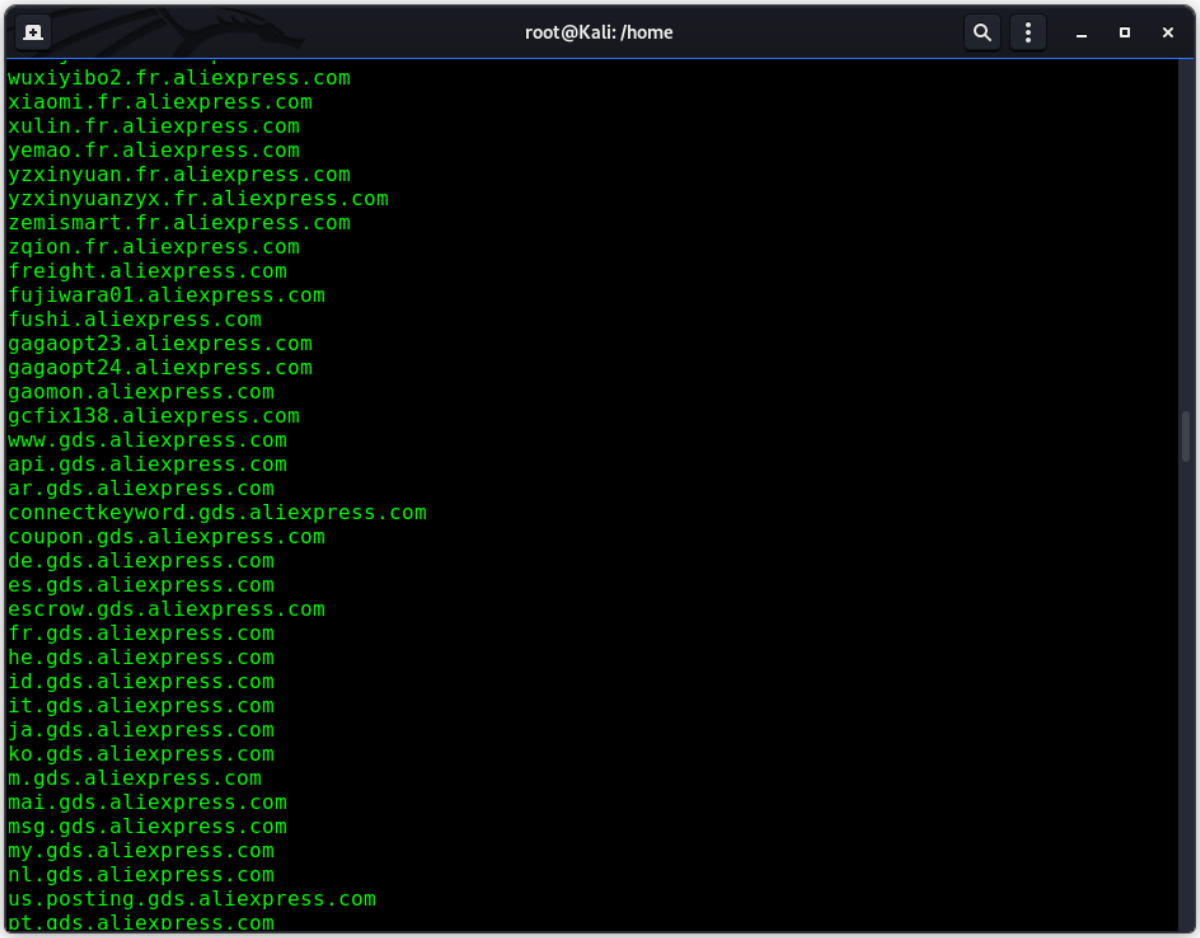

root@Kali: /home
kerui.aliexpress.com
keysion-online.aliexpress.com
kfconceptphotograph.aliexpress.com
kingseven7.aliexpress.com
kllisre.aliexpress.com
ko.aliexpress.com
m.ko.aliexpress.com
kongdy.aliexpress.com
kprepublic.aliexpress.com
krazingpot02.aliexpress.com
ksuzuki3.aliexpress.com
kunabell02.aliexpress.com
kuulaa.aliexpress.com
ky201604.aliexpress.com
kziems.aliexpress.com
kziems1.aliexpress.com
lagerhope1257461408.aliexpress.com
leecabe.aliexpress.com
leferry0511.aliexpress.com
lemfo.aliexpress.com
lenkisen20841.aliexpress.com
lephee01.aliexpress.com
lepin01.aliexpress.com
lepin02.aliexpress.com
leshucoffee.aliexpress.com
lh-laser001.aliexpress.com
ligefactory.aliexpress.com
lighthouse.aliexpress.com
liislee2014.aliexpress.com
liitokalahongkong.aliexpress.com
limingqun123.aliexpress.com
linda8877.aliexpress.com
linsudan-321.aliexpress.com
litboy123.aliexpress.com
litowd008.aliexpress.com
litwod008.aliexpress.com

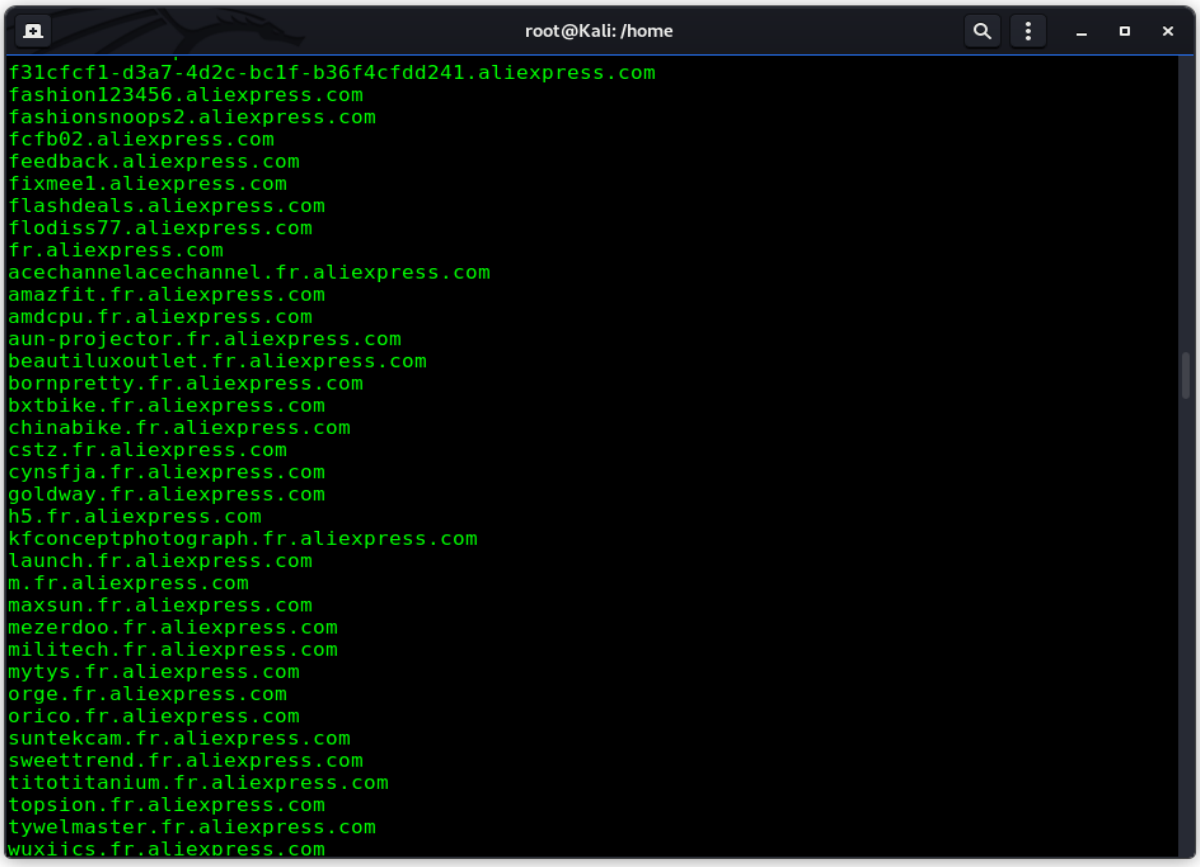

root@Kali: /home
easunpower.it.aliexpress.com
everchanging.it.aliexpress.com
h5.it.aliexpress.com
idopy.it.aliexpress.com
ihya.it.aliexpress.com
m.it.aliexpress.com
onemix.it.aliexpress.com
oneodio.it.aliexpress.com
powland.it.aliexpress.com
xnqsensor.it.aliexpress.com
ivsta.aliexpress.com
izubehor01.aliexpress.com
ja.aliexpress.com
m.ja.aliexpress.com
xiaomimi.ja.aliexpress.com
jackjadsunglasses.aliexpress.com
jeebelcamp001.aliexpress.com
jewelry123.aliexpress.com
jexxi925.aliexpress.com
jiajia08.aliexpress.com
jile.aliexpress.com
jjcshop.aliexpress.com
jjrui7777.aliexpress.com
jockmail06.aliexpress.com
johndanjohnny08.aliexpress.com
jonon01.aliexpress.com
joolimgoodjewelry.aliexpress.com
joy2018.aliexpress.com
jr01.aliexpress.com
jrd-163.aliexpress.com
jt-com.aliexpress.com
junroc.aliexpress.com
juwang.aliexpress.com
kajila7.aliexpress.com
kegland.aliexpress.com
kenazala1207.aliexpress.com

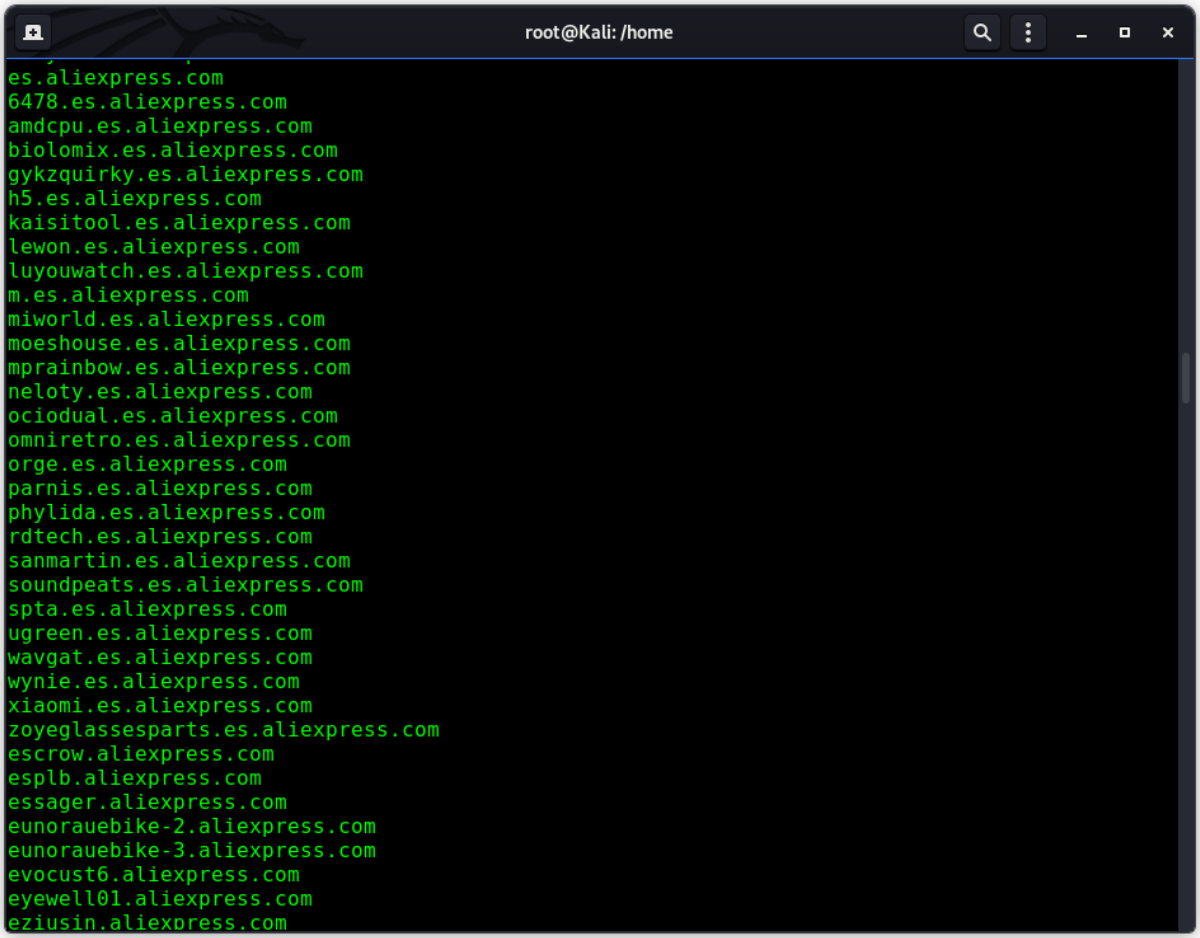

root@Kali: /home
hz-apush3.aliexpress.com
hz-apush40.aliexpress.com
hz-apush41.aliexpress.com
hz-apush42.aliexpress.com
hz-apush43.aliexpress.com
hz-apush44.aliexpress.com
hz-apush45.aliexpress.com
hz-apush46.aliexpress.com
hz-apush47.aliexpress.com
hz-apush6.aliexpress.com
hz-apush60.aliexpress.com
hz-apush61.aliexpress.com
hz-apush62.aliexpress.com
hz-apush63.aliexpress.com
hz-apush64.aliexpress.com
hz-apush65.aliexpress.com
hz-apush66.aliexpress.com
hz-apush67.aliexpress.com
hz-apush70.aliexpress.com
iconcept.aliexpress.com
id.aliexpress.com
h5.id.aliexpress.com
m.id.aliexpress.com
ihens5.aliexpress.com
ilogisticsaddress.aliexpress.com
inface.aliexpress.com
insta360.aliexpress.com
intercom.aliexpress.com
ip204-181.aliexpress.com
is.aliexpress.com
isas-g.aliexpress.com
it.aliexpress.com
aneng.it.aliexpress.com
chint.it.aliexpress.com
chuwi.it.aliexpress.com
dasaita.it.aliexpress.com

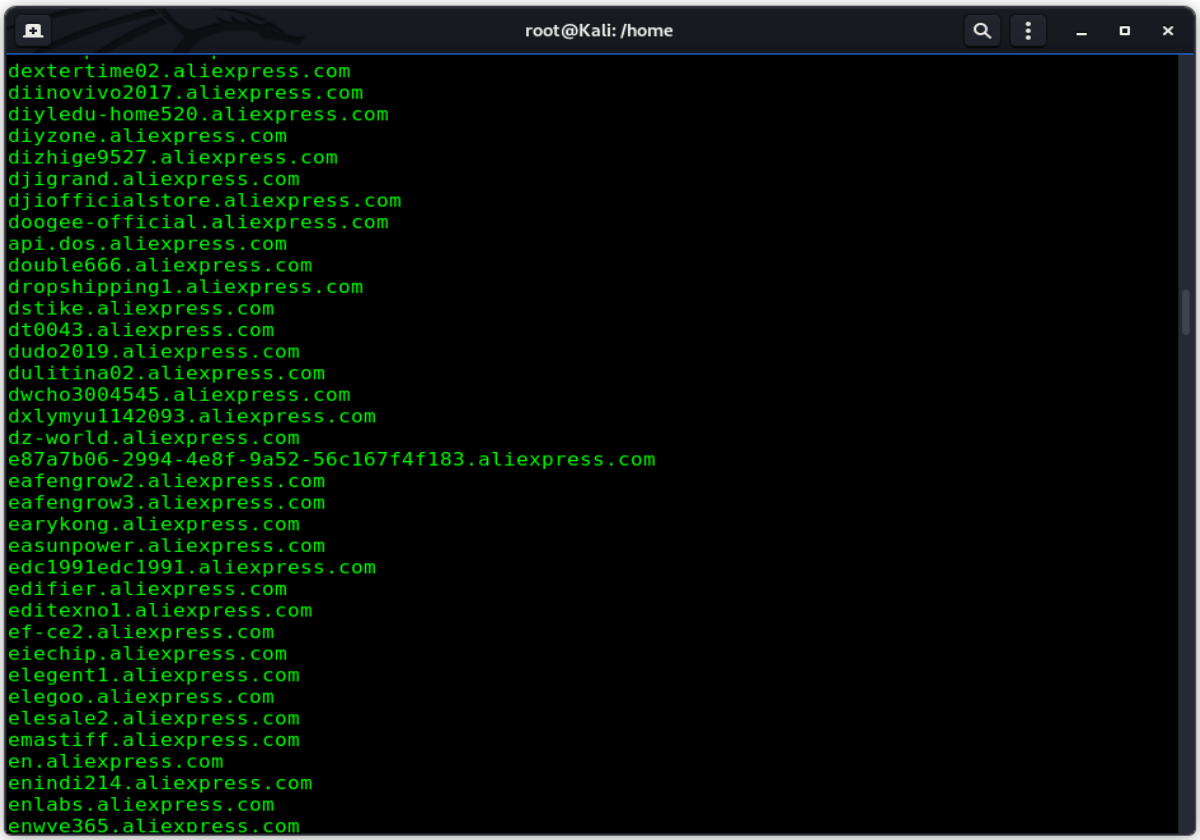

root@Kali: /home
hanerou20130405.aliexpress.com
haoshengwei.aliexpress.com
happygocn1512508881.aliexpress.com
happymonkey.aliexpress.com
hardxu2016.aliexpress.com
hayblst1314.aliexpress.com
hbq100.aliexpress.com
hdcrystal3.aliexpress.com
he.aliexpress.com
m.he.aliexpress.com
helppage.aliexpress.com
hengsong217538.aliexpress.com
hibrew.aliexpress.com
highquality-dresses-store-516847.aliexpress.com
higo6.aliexpress.com
hilda.aliexpress.com
home.aliexpress.com
hongbaby2010.aliexpress.com
hotproducts.aliexpress.com
hqcam001.aliexpress.com
hrx1.aliexpress.com
hsec12345.aliexpress.com
huberyhuang123.aliexpress.com
huionhuion.aliexpress.com
huiontablet.aliexpress.com
hview.aliexpress.com
hystou02.aliexpress.com
hz-apush10.aliexpress.com
hz-apush11.aliexpress.com
hz-apush12.aliexpress.com
hz-apush13.aliexpress.com
hz-apush14.aliexpress.com
hz-apush16.aliexpress.com
hz-apush18.aliexpress.com
hz-apush20.aliexpress.com
hz-apush21.aliexpress.com

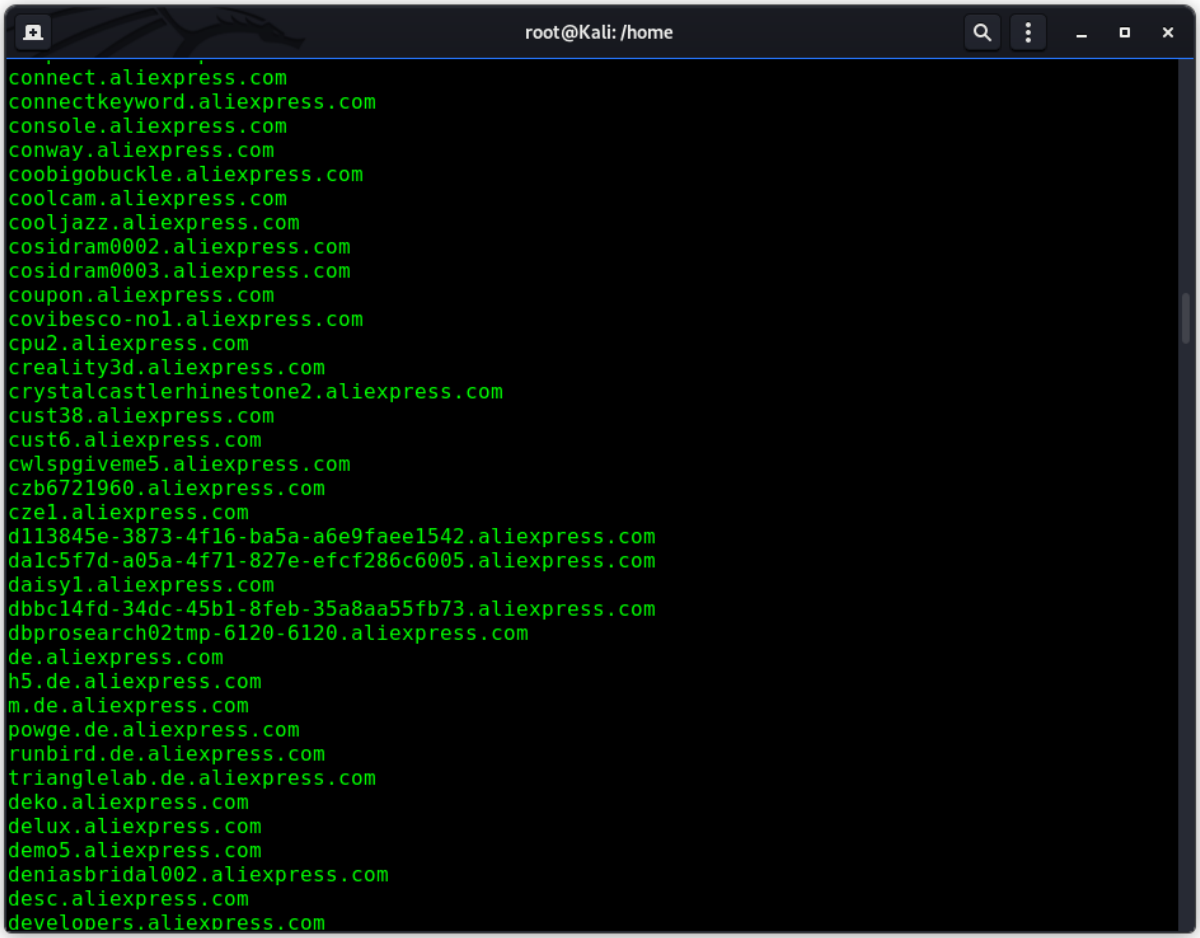

root@Kali: /home
ru.gds.aliexpress.com
th.gds.aliexpress.com
thirdparty.gds.aliexpress.com
tr.gds.aliexpress.com
u.gds.aliexpress.com
vi.gds.aliexpress.com
gdsns1.aliexpress.com
gdsns2.aliexpress.com
geeekpi.aliexpress.com
geeetech.aliexpress.com
geekworm.aliexpress.com
gew33.aliexpress.com
globalwintoys1.aliexpress.com
globalwintoys3.aliexpress.com
glymg777.aliexpress.com
go123.aliexpress.com
go2boho.aliexpress.com
goddesswiggiestoreno1.aliexpress.com
goldway.aliexpress.com
golooloo2.aliexpress.com
good100.aliexpress.com
gpdshop1.aliexpress.com
gpnacn01.aliexpress.com
gqtorch925.aliexpress.com
grandsharp.aliexpress.com
group.aliexpress.com
gshopper.aliexpress.com
gsp.aliexpress.com
gtreu.aliexpress.com
gtrhz.aliexpress.com
gtrru.aliexpress.com
gtrus.aliexpress.com
gutasphuyuxuan2012.aliexpress.com
gzdl2.aliexpress.com
h1111ziocrest.aliexpress.com
h5.aliexpress.com

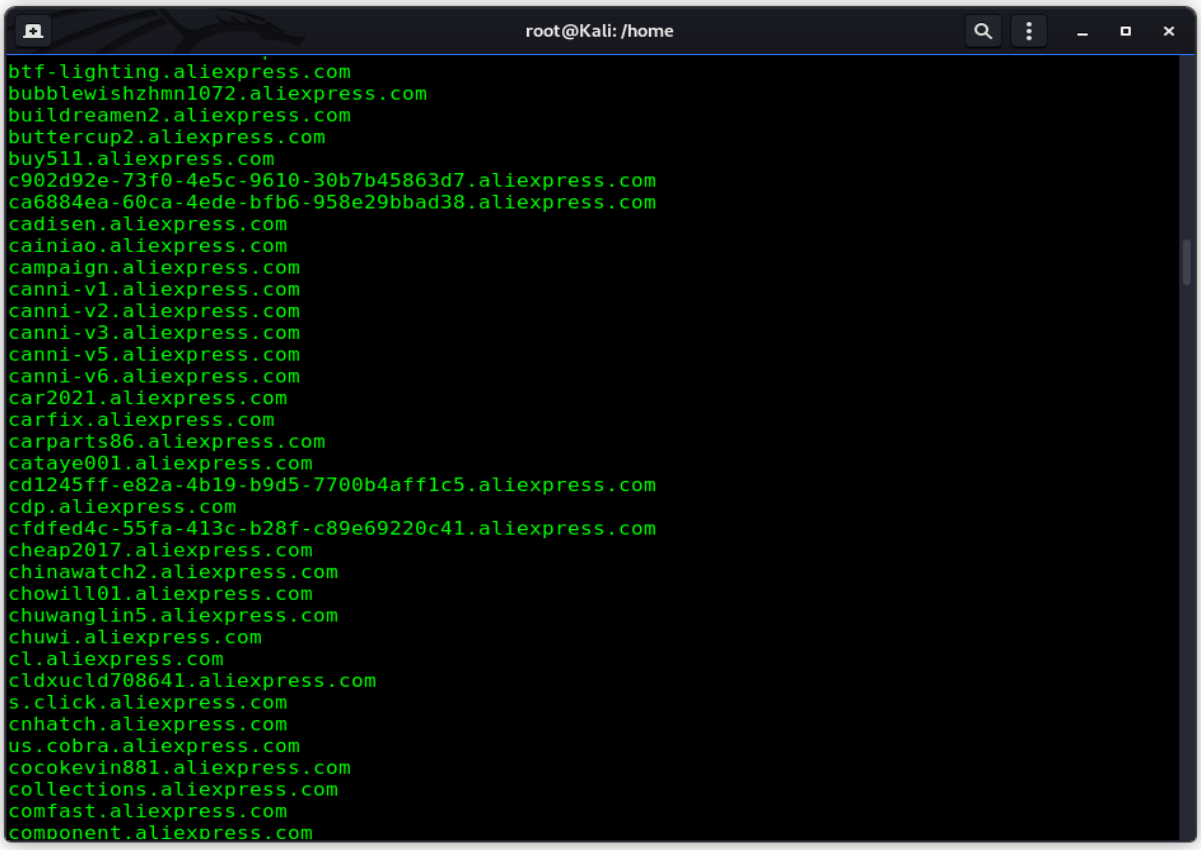

root@Kali: /home
wuxiyibo2.fr.aliexpress.com
xiaomi.fr.aliexpress.com
xulin.fr.aliexpress.com
yemao.fr.aliexpress.com
yzxinyuan.fr.aliexpress.com
yzxinyuanzyx.fr.aliexpress.com
zemismart.fr.aliexpress.com
zqion.fr.aliexpress.com
freight.aliexpress.com
fujiwara01.aliexpress.com
fushi.aliexpress.com
gagaopt23.aliexpress.com
gagaopt24.aliexpress.com
gaomon.aliexpress.com
gcfix138.aliexpress.com
www.gds.aliexpress.com
api.gds.aliexpress.com
ar.gds.aliexpress.com
connectkeyword.gds.aliexpress.com
coupon.gds.aliexpress.com
de.gds.aliexpress.com
es.gds.aliexpress.com
escrow.gds.aliexpress.com
fr.gds.aliexpress.com
he.gds.aliexpress.com
id.gds.aliexpress.com
it.gds.aliexpress.com
ja.gds.aliexpress.com
ko.gds.aliexpress.com
m.gds.aliexpress.com
mai.gds.aliexpress.com
msg.gds.aliexpress.com
my.gds.aliexpress.com
nl.gds.aliexpress.com
us.posting.gds.aliexpress.com
pt.gds.aliexpress.com

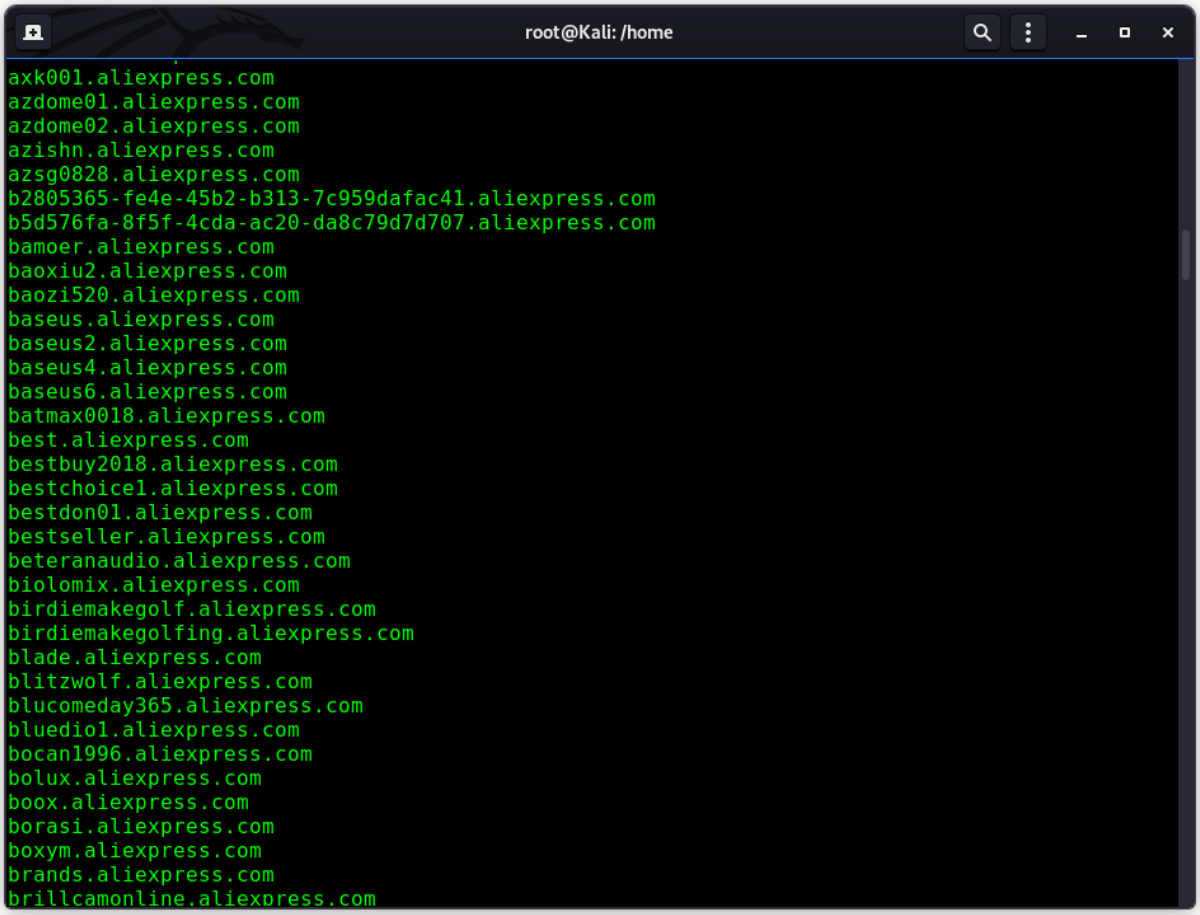

root@Kali: /home
f31cfcf1-d3a7-4d2c-bc1f-b36f4cfdd241.aliexpress.com
fashion123456.aliexpress.com
fashionsnoops2.aliexpress.com
fcfb02.aliexpress.com
feedback.aliexpress.com
fixmee1.aliexpress.com
flashdeals.aliexpress.com
flodiss77.aliexpress.com
fr.aliexpress.com
acechannelacechannel.fr.aliexpress.com
amazfit.fr.aliexpress.com
amdcpu.fr.aliexpress.com
aun-projector.fr.aliexpress.com
beautiluxoutlet.fr.aliexpress.com
bornpretty.fr.aliexpress.com
bxtbike.fr.aliexpress.com
chinabike.fr.aliexpress.com
cstz.fr.aliexpress.com
cynsfja.fr.aliexpress.com
goldway.fr.aliexpress.com
h5.fr.aliexpress.com
kfconceptphotograph.fr.aliexpress.com
launch.fr.aliexpress.com
m.fr.aliexpress.com
maxsun.fr.aliexpress.com
mezerdoo.fr.aliexpress.com
militech.fr.aliexpress.com
mytys.fr.aliexpress.com
orge.fr.aliexpress.com
orico.fr.aliexpress.com
suntekcam.fr.aliexpress.com
sweettrend.fr.aliexpress.com
titotitanium.fr.aliexpress.com
topsion.fr.aliexpress.com
tywelmaster.fr.aliexpress.com
wuxiics.fr.aliexpress.com

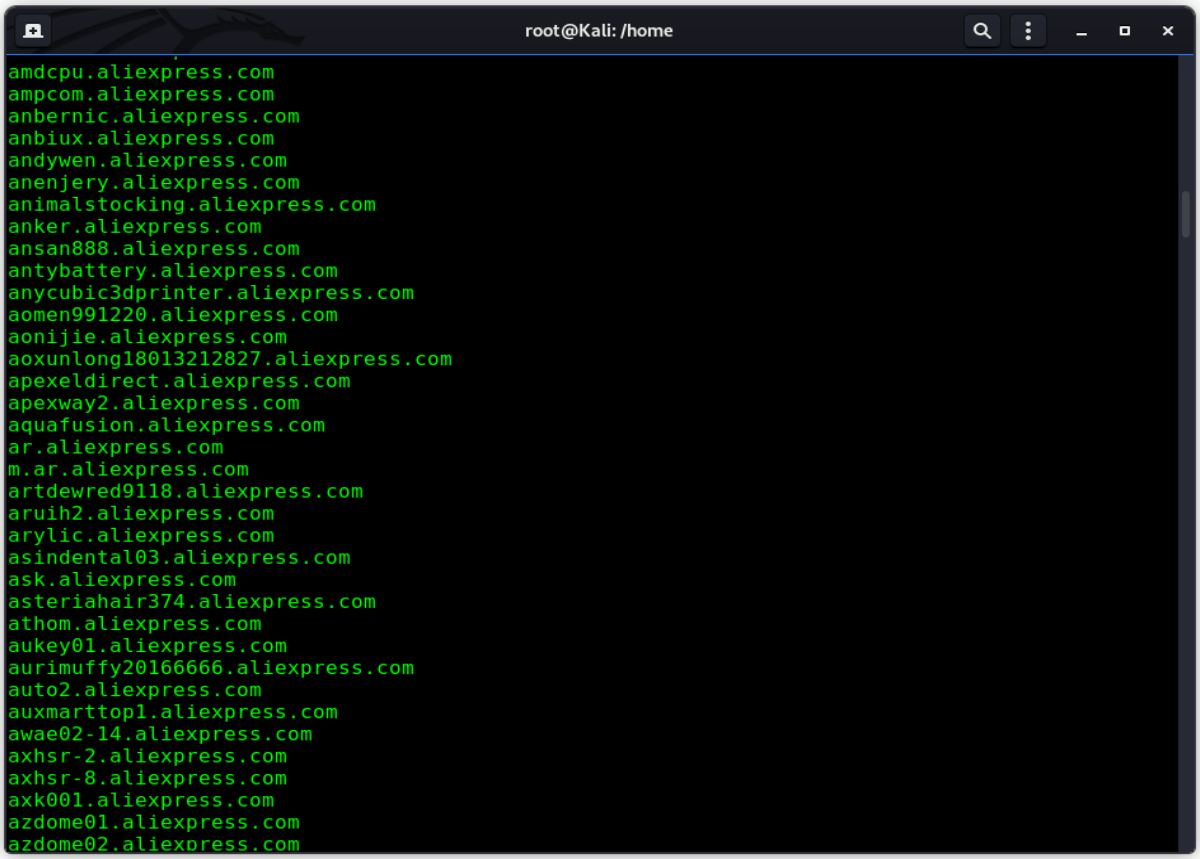

root@Kali: /home
es.aliexpress.com
6478.es.aliexpress.com
amdcpu.es.aliexpress.com
biolomix.es.aliexpress.com
gykzquirky.es.aliexpress.com
h5.es.aliexpress.com
kaisitool.es.aliexpress.com
lewon.es.aliexpress.com
luyouwatch.es.aliexpress.com
m.es.aliexpress.com
miworld.es.aliexpress.com
moeshouse.es.aliexpress.com
mprainbow.es.aliexpress.com
neloty.es.aliexpress.com
ociodual.es.aliexpress.com
omniretro.es.aliexpress.com
orge.es.aliexpress.com
parnis.es.aliexpress.com
phylida.es.aliexpress.com
rdtech.es.aliexpress.com
sanmartin.es.aliexpress.com
soundpeats.es.aliexpress.com
spta.es.aliexpress.com
ugreen.es.aliexpress.com
wavgat.es.aliexpress.com
wynie.es.aliexpress.com
xiaomi.es.aliexpress.com
zoyeglassesparts.es.aliexpress.com
escrow.aliexpress.com
esplb.aliexpress.com
essager.aliexpress.com
eunorauebike-2.aliexpress.com
eunorauebike-3.aliexpress.com
evocust6.aliexpress.com
eyewell01.aliexpress.com
eziusin.aliexpress.com

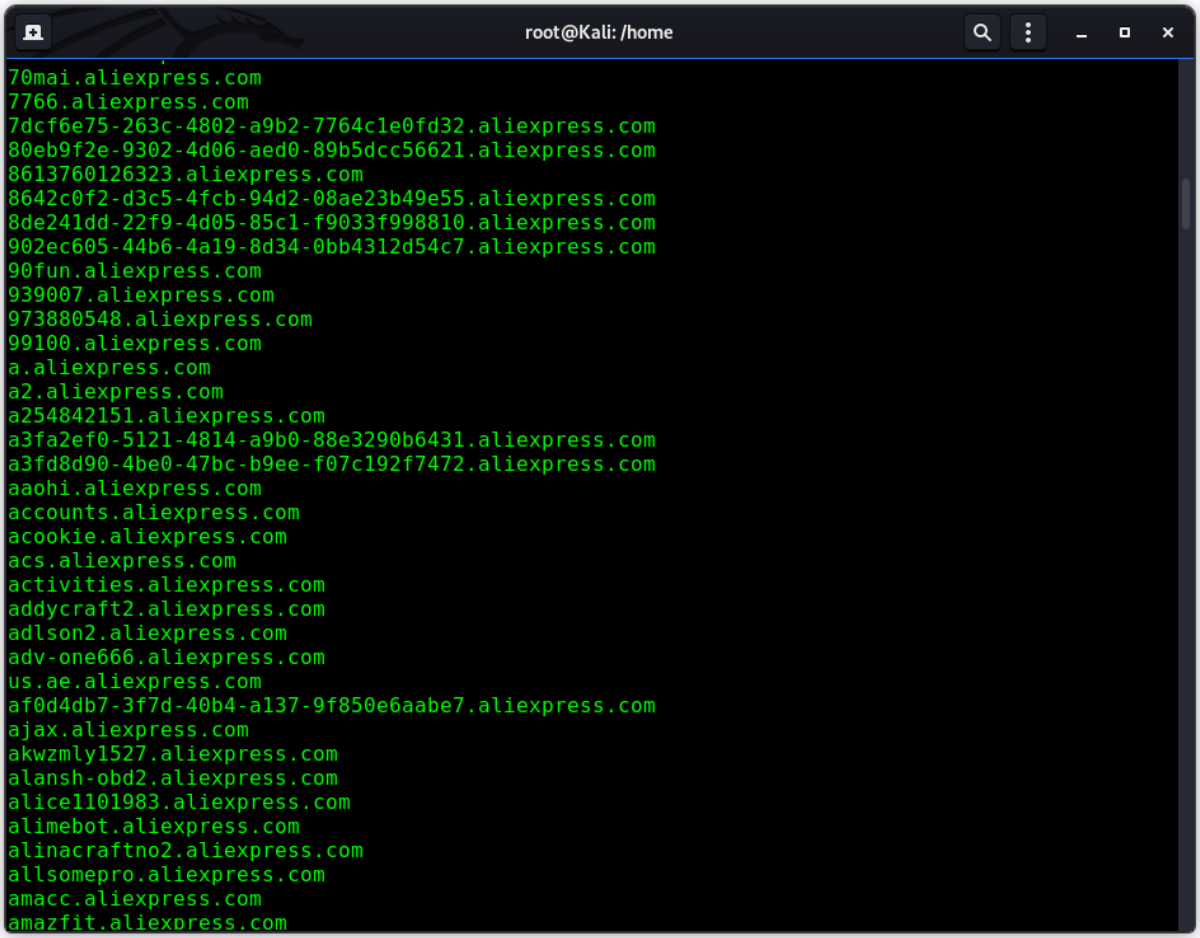

root@Kali: /home
dextertime02.aliexpress.com
diinovivo2017.aliexpress.com
diyledu-home520.aliexpress.com
diyzone.aliexpress.com
dizhige9527.aliexpress.com
djigrand.aliexpress.com
djiofficialstore.aliexpress.com
doogee-official.aliexpress.com
api.dos.aliexpress.com
double666.aliexpress.com
dropshipping1.aliexpress.com
dstike.aliexpress.com
dt0043.aliexpress.com
dudo2019.aliexpress.com
dulitina02.aliexpress.com
dwcho3004545.aliexpress.com
dxlymyu1142093.aliexpress.com
dz-world.aliexpress.com
e87a7b06-2994-4e8f-9a52-56c167f4f183.aliexpress.com
eafengrow2.aliexpress.com
eafengrow3.aliexpress.com
earykong.aliexpress.com
easunpower.aliexpress.com
edc1991edc1991.aliexpress.com
edifier.aliexpress.com
editexno1.aliexpress.com
ef-ce2.aliexpress.com
eiechip.aliexpress.com
elegent1.aliexpress.com
elegoo.aliexpress.com
elesale2.aliexpress.com
emastiff.aliexpress.com
en.aliexpress.com
enindi214.aliexpress.com
enlabs.aliexpress.com
enwve365.aliexpress.com

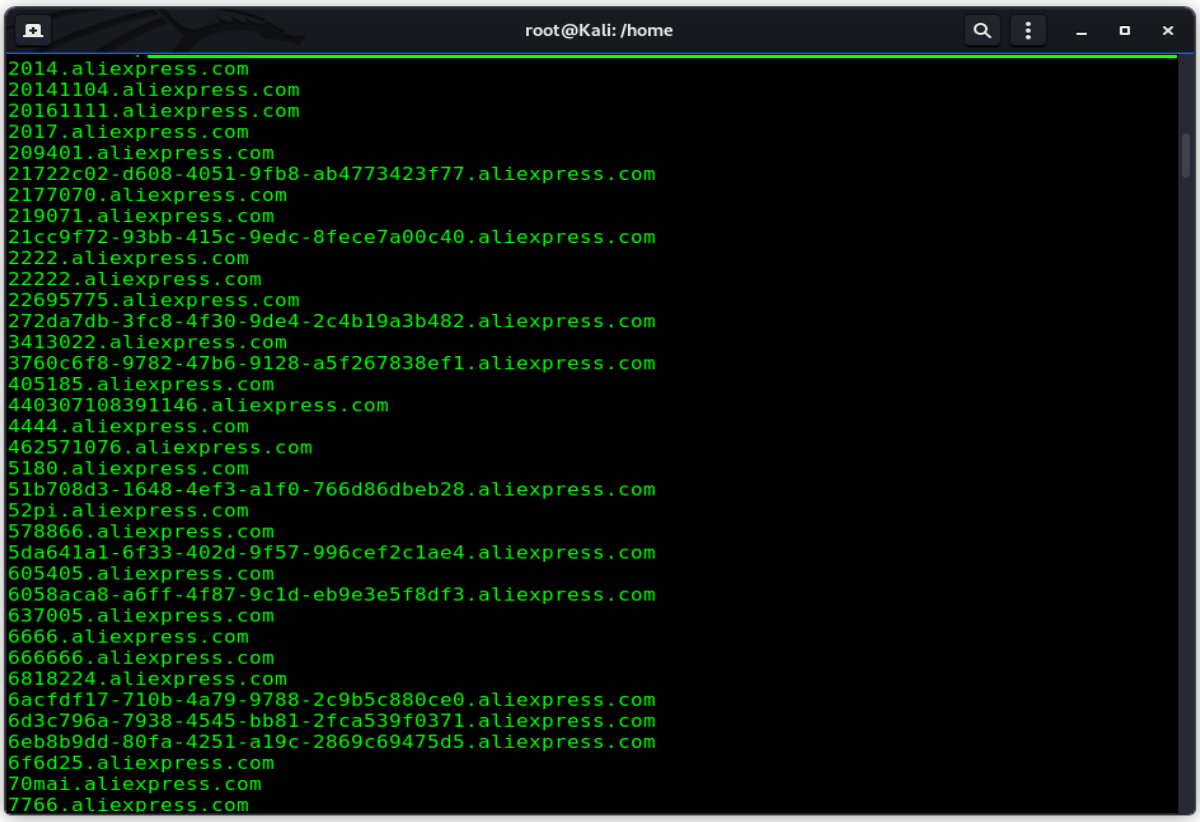

root@Kali: /home
connect.aliexpress.com
connectkeyword.aliexpress.com
console.aliexpress.com
conway.aliexpress.com
coobigobuckle.aliexpress.com
coolcam.aliexpress.com
cooljazz.aliexpress.com
cosidram0002.aliexpress.com
cosidram0003.aliexpress.com
coupon.aliexpress.com
covibesco-no1.aliexpress.com
cpu2.aliexpress.com
creality3d.aliexpress.com
crystalcastlerhinestone2.aliexpress.com
cust38.aliexpress.com
cust6.aliexpress.com
cwlspgiveme5.aliexpress.com
czb6721960.aliexpress.com
cze1.aliexpress.com
d113845e-3873-4f16-ba5a-a6e9faee1542.aliexpress.com
da1c5f7d-a05a-4f71-827e-efcf286c6005.aliexpress.com
daisy1.aliexpress.com
dbbc14fd-34dc-45b1-8feb-35a8aa55fb73.aliexpress.com
dbprosearch02tmp-6120-6120.aliexpress.com
de.aliexpress.com
h5.de.aliexpress.com
m.de.aliexpress.com
powge.de.aliexpress.com
runbird.de.aliexpress.com
trianglelab.de.aliexpress.com
deko.aliexpress.com
delux.aliexpress.com
demo5.aliexpress.com
deniasbridal002.aliexpress.com
desc.aliexpress.com
developers.aliexpress.com

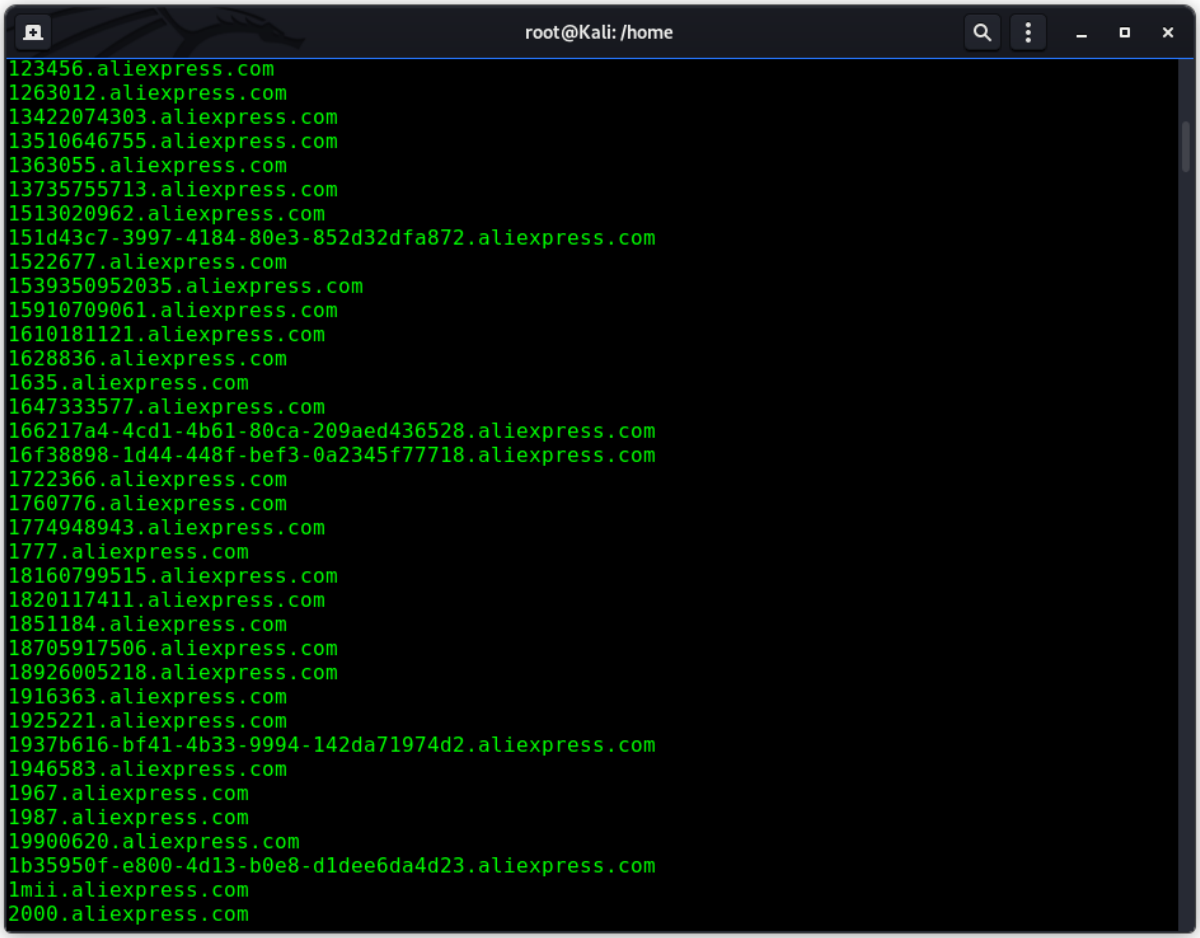

root@Kali: /home
btf-lighting.aliexpress.com
bubblewishzhmn1072.aliexpress.com
buildreamen2.aliexpress.com
buttercup2.aliexpress.com
buy511.aliexpress.com
c902d92e-73f0-4e5c-9610-30b7b45863d7.aliexpress.com
ca6884ea-60ca-4ede-bfb6-958e29bbad38.aliexpress.com
cadisen.aliexpress.com
cainiao.aliexpress.com
campaign.aliexpress.com
canni-v1.aliexpress.com
canni-v2.aliexpress.com
canni-v3.aliexpress.com
canni-v5.aliexpress.com
canni-v6.aliexpress.com
car2021.aliexpress.com
carfix.aliexpress.com
carparts86.aliexpress.com
cataye001.aliexpress.com
cd1245ff-e82a-4b19-b9d5-7700b4aff1c5.aliexpress.com
cdp.aliexpress.com
cfdfed4c-55fa-413c-b28f-c89e69220c41.aliexpress.com
cheap2017.aliexpress.com
chinawatch2.aliexpress.com
chowill01.aliexpress.com
chuwanglin5.aliexpress.com
chuwi.aliexpress.com
cl.aliexpress.com
cldxucld708641.aliexpress.com
s.click.aliexpress.com
cnhatch.aliexpress.com
us.cobra.aliexpress.com
cocokevin881.aliexpress.com
collections.aliexpress.com
comfast.aliexpress.com
component.aliexpress.com

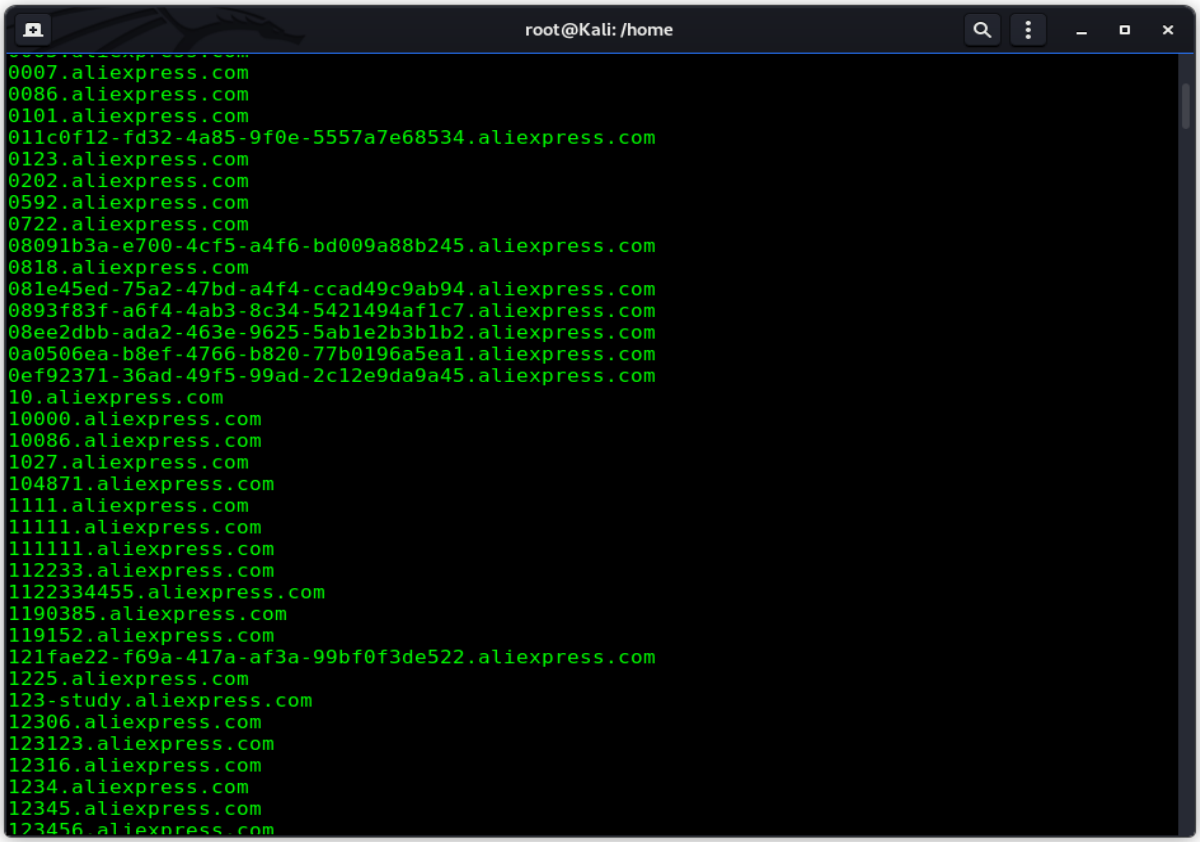

root@Kali: /home
axk001.aliexpress.com
azdome01.aliexpress.com
azdome02.aliexpress.com
azishn.aliexpress.com
azsg0828.aliexpress.com
b2805365-fe4e-45b2-b313-7c959dafac41.aliexpress.com
b5d576fa-8f5f-4cda-ac20-da8c79d7d707.aliexpress.com
bamoer.aliexpress.com
baoxiu2.aliexpress.com
baozi520.aliexpress.com
baseus.aliexpress.com
baseus2.aliexpress.com
baseus4.aliexpress.com
baseus6.aliexpress.com
batmax0018.aliexpress.com
best.aliexpress.com
bestbuy2018.aliexpress.com
bestchoice1.aliexpress.com
bestdon01.aliexpress.com
bestseller.aliexpress.com
beteranaudio.aliexpress.com
biolomix.aliexpress.com
birdiemakegolf.aliexpress.com
birdiemakegolfing.aliexpress.com
blade.aliexpress.com
blitzwolf.aliexpress.com
blucomeday365.aliexpress.com
bluedio1.aliexpress.com
bocan1996.aliexpress.com
bolux.aliexpress.com
boox.aliexpress.com
borasi.aliexpress.com
boxym.aliexpress.com
brands.aliexpress.com
brillcamonline.aliexpress.com

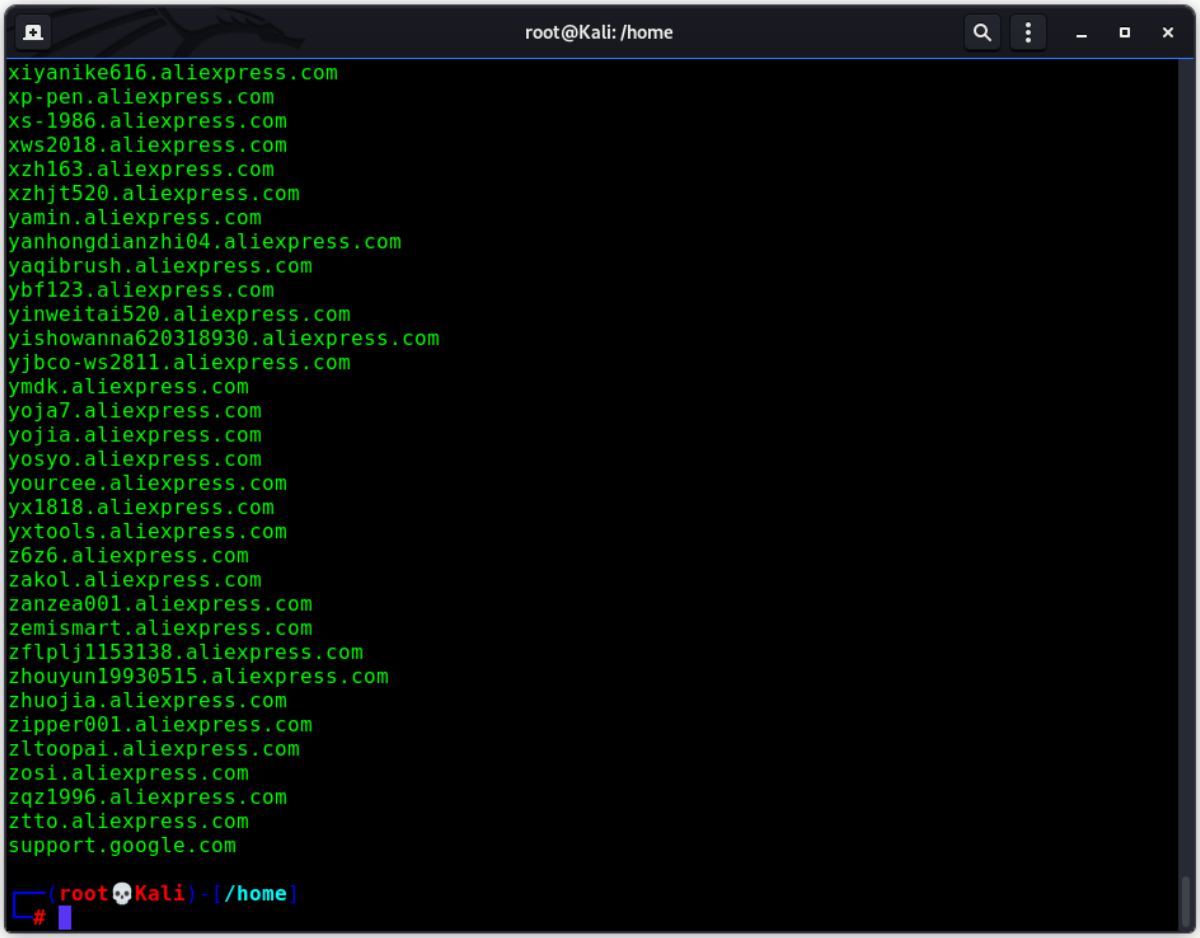

root@Kali: /home
amdcpu.aliexpress.com
ampcom.aliexpress.com
anbernic.aliexpress.com
anbiux.aliexpress.com
andywen.aliexpress.com
anenjery.aliexpress.com
animalstocking.aliexpress.com
anker.aliexpress.com
ansan888.aliexpress.com
antybattery.aliexpress.com
anycubic3dprinter.aliexpress.com
aomen991220.aliexpress.com
aonijie.aliexpress.com
aoxunlong18013212827.aliexpress.com
apexeldirect.aliexpress.com
apexway2.aliexpress.com
aquafusion.aliexpress.com
ar.aliexpress.com
m.ar.aliexpress.com
artdewred9118.aliexpress.com
aruih2.aliexpress.com
arylic.aliexpress.com
asindental03.aliexpress.com
ask.aliexpress.com
asteriahair374.aliexpress.com
athom.aliexpress.com
aukey01.aliexpress.com
aurimuffy20166666.aliexpress.com
auto2.aliexpress.com
auxmarttop1.aliexpress.com
awae02-14.aliexpress.com
axhsr-2.aliexpress.com
axhsr-8.aliexpress.com
axk001.aliexpress.com
azdome01.aliexpress.com
azdome02.aliexpress.com


root@Kali: /home
70mai.aliexpress.com
7766.aliexpress.com
7dcf6e75-263c-4802-a9b2-7764c1e0fd32.aliexpress.com
80eb9f2e-9302-4d06-aed0-89b5dcc56621.aliexpress.com
8613760126323.aliexpress.com
8642c0f2-d3c5-4fcb-94d2-08ae23b49e55.aliexpress.com
8de241dd-22f9-4d05-85c1-f9033f998810.aliexpress.com
902ec605-44b6-4a19-8d34-0bb4312d54c7.aliexpress.com
90fun.aliexpress.com
939007.aliexpress.com
973880548.aliexpress.com
99100.aliexpress.com
a.aliexpress.com
a2.aliexpress.com
a254842151.aliexpress.com
a3fa2ef0-5121-4814-a9b0-88e3290b6431.aliexpress.com
a3fd8d90-4be0-47bc-b9ee-f07c192f7472.aliexpress.com
aaohi.aliexpress.com
accounts.aliexpress.com
acookie.aliexpress.com
acs.aliexpress.com
activities.aliexpress.com
addycraft2.aliexpress.com
adlson2.aliexpress.com
adv-one666.aliexpress.com
us.ae.aliexpress.com
af0d4db7-3f7d-40b4-a137-9f850e6aabe7.aliexpress.com
ajax.aliexpress.com
akwzmly1527.aliexpress.com
alansh-obd2.aliexpress.com
alice1101983.aliexpress.com
alimebot.aliexpress.com
alinacraftno2.aliexpress.com
allsomepro.aliexpress.com
amacc.aliexpress.com
amazfit.aliexpress.com


root@Kali: /home
2014.aliexpress.com
20141104.aliexpress.com
20161111.aliexpress.com
2017.aliexpress.com
209401.aliexpress.com
21722c02-d608-4051-9fb8-ab4773423f77.aliexpress.com
2177070.aliexpress.com
219071.aliexpress.com
21cc9f72-93bb-415c-9edc-8fece7a00c40.aliexpress.com
2222.aliexpress.com
22222.aliexpress.com
22695775.aliexpress.com
272da7db-3fc8-4f30-9de4-2c4b19a3b482.aliexpress.com
3413022.aliexpress.com
3760c6f8-9782-47b6-9128-a5f267838ef1.aliexpress.com
405185.aliexpress.com
440307108391146.aliexpress.com
4444.aliexpress.com
462571076.aliexpress.com
5180.aliexpress.com
51b708d3-1648-4ef3-a1f0-766d86dbeb28.aliexpress.com
52pi.aliexpress.com
578866.aliexpress.com
5da641a1-6f33-402d-9f57-996cef2c1ae4.aliexpress.com
605405.aliexpress.com
6058aca8-a6ff-4f87-9c1d-eb9e3e5f8df3.aliexpress.com
637005.aliexpress.com
6666.aliexpress.com
666666.aliexpress.com
6818224.aliexpress.com
6acfdf17-710b-4a79-9788-2c9b5c880ce0.aliexpress.com
6d3c796a-7938-4545-bb81-2fca539f0371.aliexpress.com
6eb8b9dd-80fa-4251-a19c-2869c69475d5.aliexpress.com
6f6d25.aliexpress.com
70mai.aliexpress.com
7766.aliexpress.com

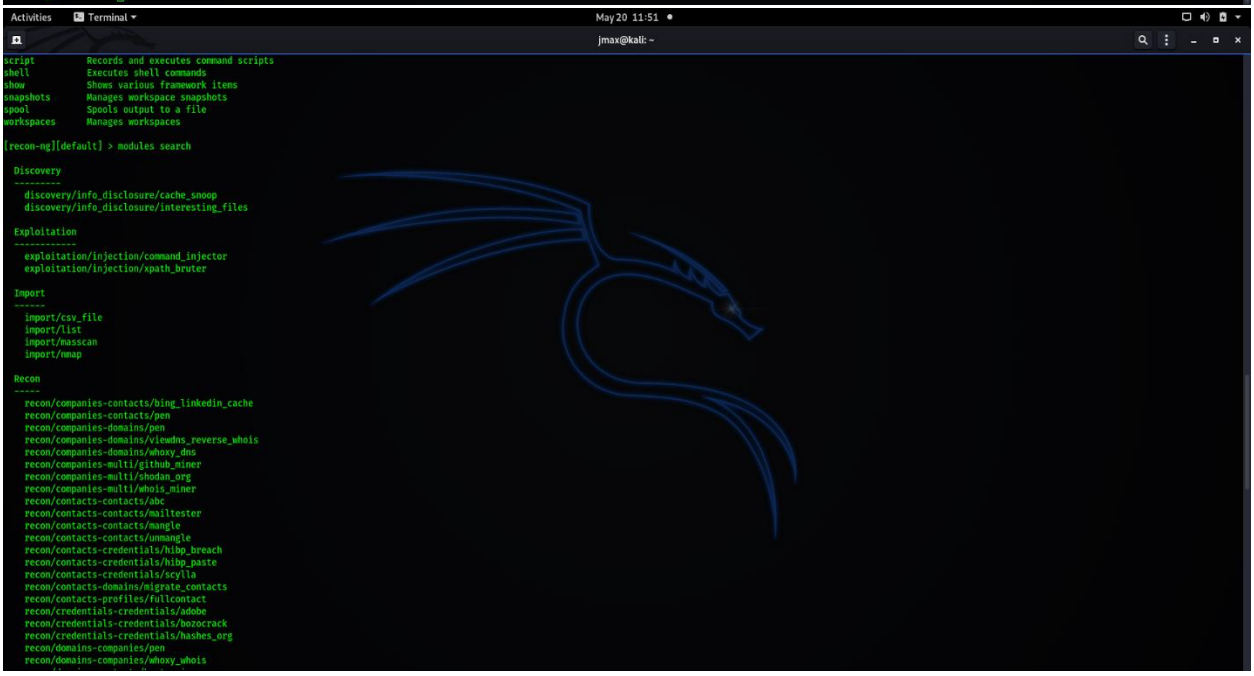

root@Kali: /home
123456.aliexpress.com
1263012.aliexpress.com
13422074303.aliexpress.com
13510646755.aliexpress.com
1363055.aliexpress.com
13735755713.aliexpress.com
1513020962.aliexpress.com
151d43c7-3997-4184-80e3-852d32dfa872.aliexpress.com
1522677.aliexpress.com
1539350952035.aliexpress.com
15910709061.aliexpress.com
1610181121.aliexpress.com
1628836.aliexpress.com
1635.aliexpress.com
1647333577.aliexpress.com
166217a4-4cd1-4b61-80ca-209aed436528.aliexpress.com
16f38898-1d44-448f-bef3-0a2345f77718.aliexpress.com
1722366.aliexpress.com
1760776.aliexpress.com
1774948943.aliexpress.com
1777.aliexpress.com
18160799515.aliexpress.com
1820117411.aliexpress.com
1851184.aliexpress.com
18705917506.aliexpress.com
18926005218.aliexpress.com
1916363.aliexpress.com
1925221.aliexpress.com
1937b616-bf41-4b33-9994-142da71974d2.aliexpress.com
1946583.aliexpress.com
1967.aliexpress.com
1987.aliexpress.com
19900620.aliexpress.com
1b35950f-e800-4d13-b0e8-d1dee6da4d23.aliexpress.com
1mii.aliexpress.com
2000.aliexpress.com

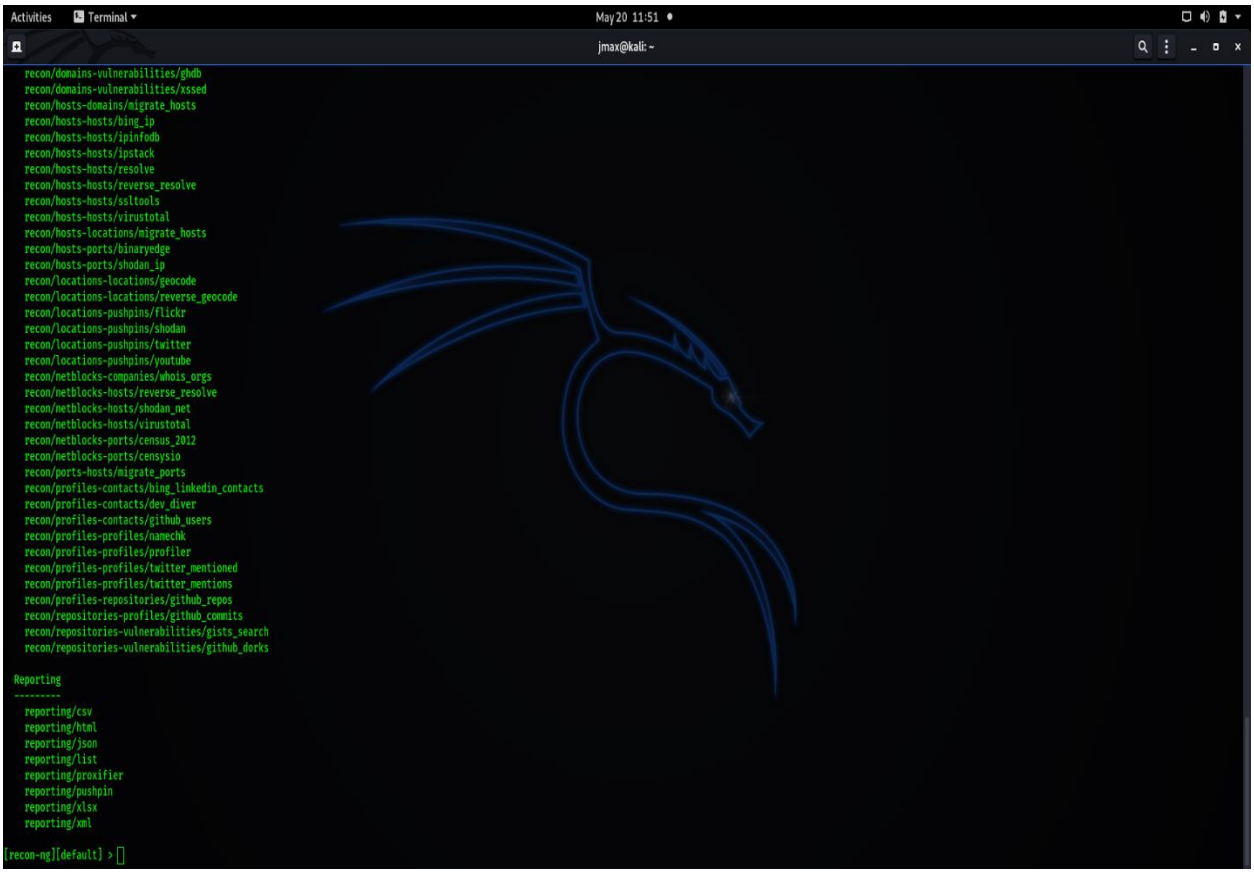

root@Kali: /home
0007.aliexpress.com
0086.aliexpress.com
0101.aliexpress.com
011c0f12-fd32-4a85-9f0e-5557a7e68534.aliexpress.com
0123.aliexpress.com
0202.aliexpress.com
0592.aliexpress.com
0722.aliexpress.com
08091b3a-e700-4cf5-a4f6-bd009a88b245.aliexpress.com
0818.aliexpress.com
081e45ed-75a2-47bd-a4f4-ccad49c9ab94.aliexpress.com
0893f83f-a6f4-4ab3-8c34-5421494af1c7.aliexpress.com
08ee2dbb-ada2-463e-9625-5ab1e2b3b1b2.aliexpress.com
0a0506ea-b8ef-4766-b820-77b0196a5ea1.aliexpress.com
0ef92371-36ad-49f5-99ad-2c12e9da9a45.aliexpress.com
10.aliexpress.com
10000.aliexpress.com
10086.aliexpress.com
1027.aliexpress.com
104871.aliexpress.com
1111.aliexpress.com
11111.aliexpress.com
111111.aliexpress.com
112233.aliexpress.com
1122334455.aliexpress.com
1190385.aliexpress.com
119152.aliexpress.com
121fae22-f69a-417a-af3a-99bf0f3de522.aliexpress.com
1225.aliexpress.com
123-study.aliexpress.com
12306.aliexpress.com
123123.aliexpress.com
12316.aliexpress.com
1234.aliexpress.com
12345.aliexpress.com

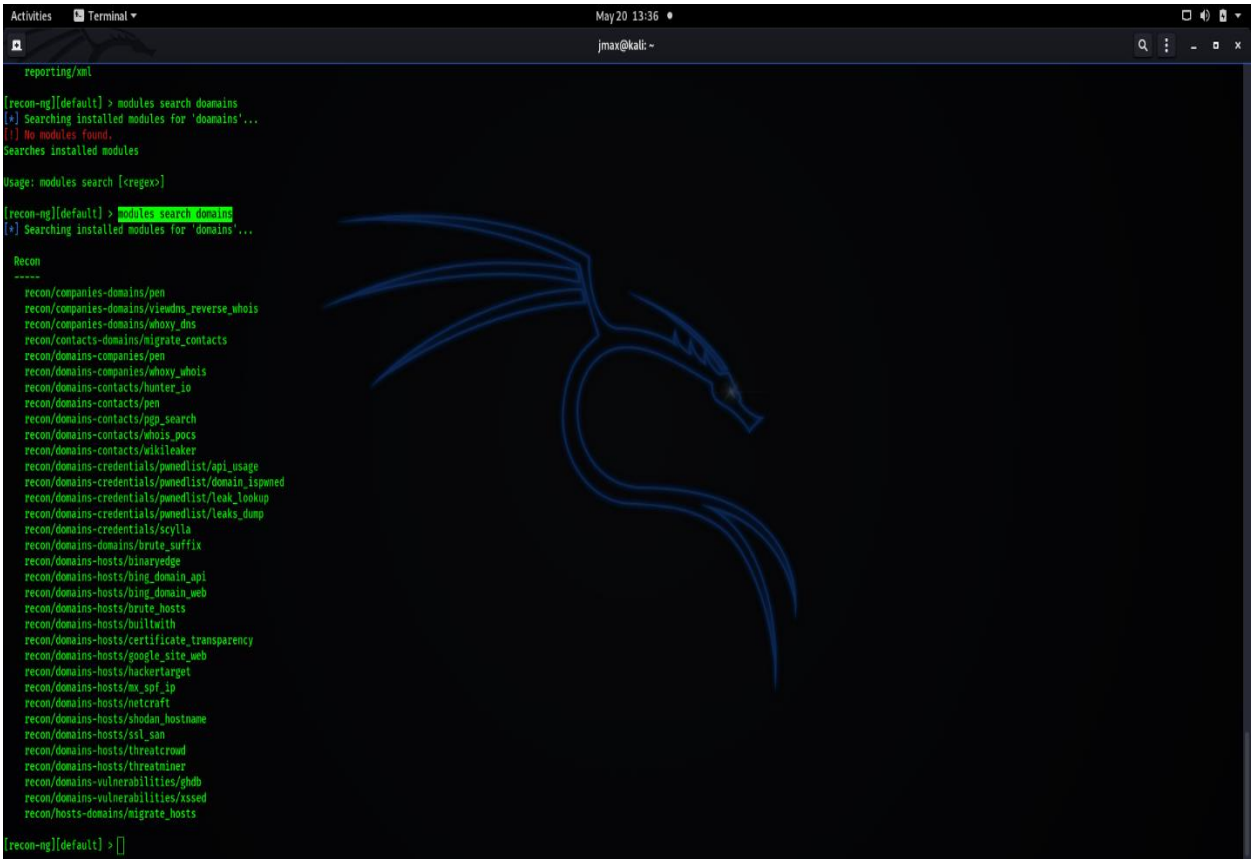

root@Kali: /home
xiyanike616.aliexpress.com
xp-pen.aliexpress.com
xs-1986.aliexpress.com
xws2018.aliexpress.com
xzh163.aliexpress.com
xzhjt520.aliexpress.com
yamin.aliexpress.com
yanhongdianzhi04.aliexpress.com
yaqibrush.aliexpress.com
ybf123.aliexpress.com
yinweitai520.aliexpress.com
yishowanna620318930.aliexpress.com
yjbco-ws2811.aliexpress.com
ymdk.aliexpress.com
yoja7.aliexpress.com
yojia.aliexpress.com
yosyo.aliexpress.com
yourcee.aliexpress.com
yx1818.aliexpress.com
yxtools.aliexpress.com
z6z6.aliexpress.com
zakol.aliexpress.com
zanzea001.aliexpress.com
zemismart.aliexpress.com
zflplj1153138.aliexpress.com
zhouyun19930515.aliexpress.com
zhuojia.aliexpress.com
zipper001.aliexpress.com
zltoopai.aliexpress.com
zosi.aliexpress.com
zqz1996.aliexpress.com
ztto.aliexpress.com
support.google.com
(root Kali)-[/home]
#

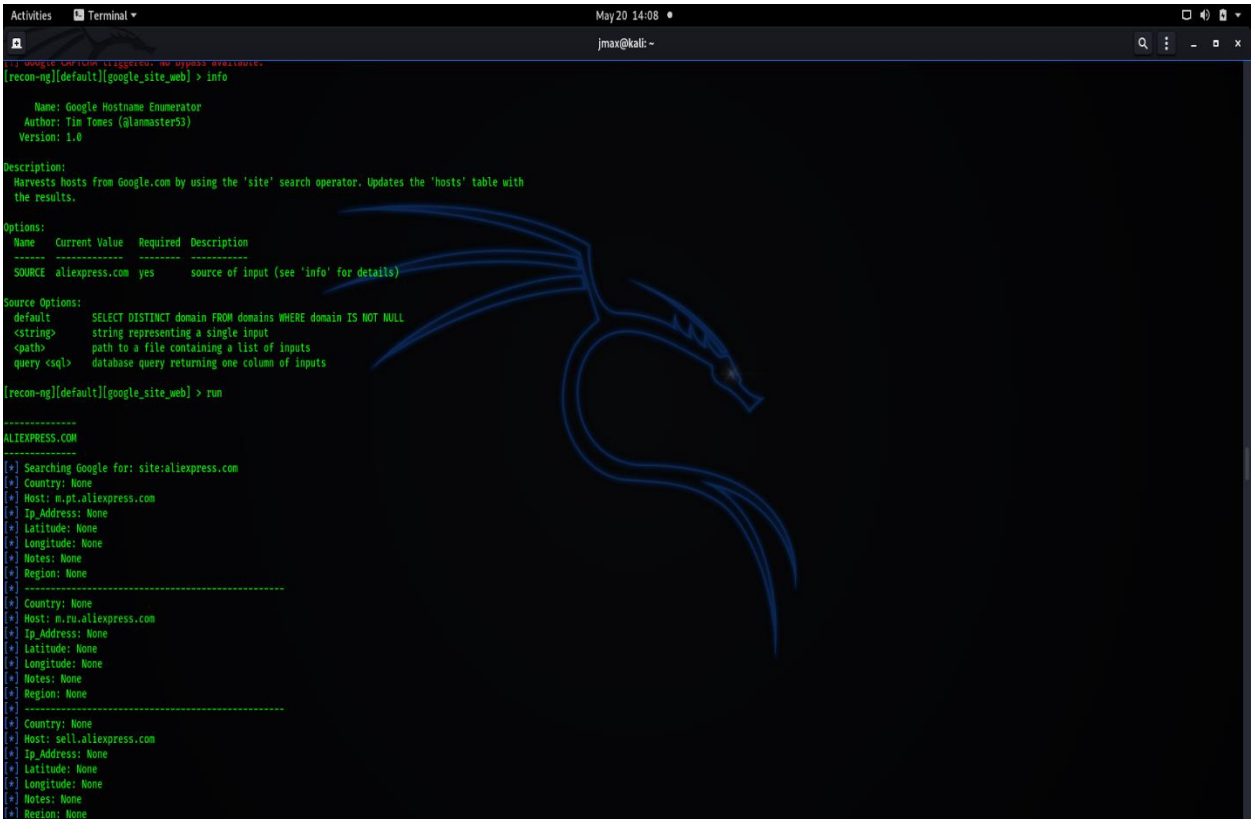
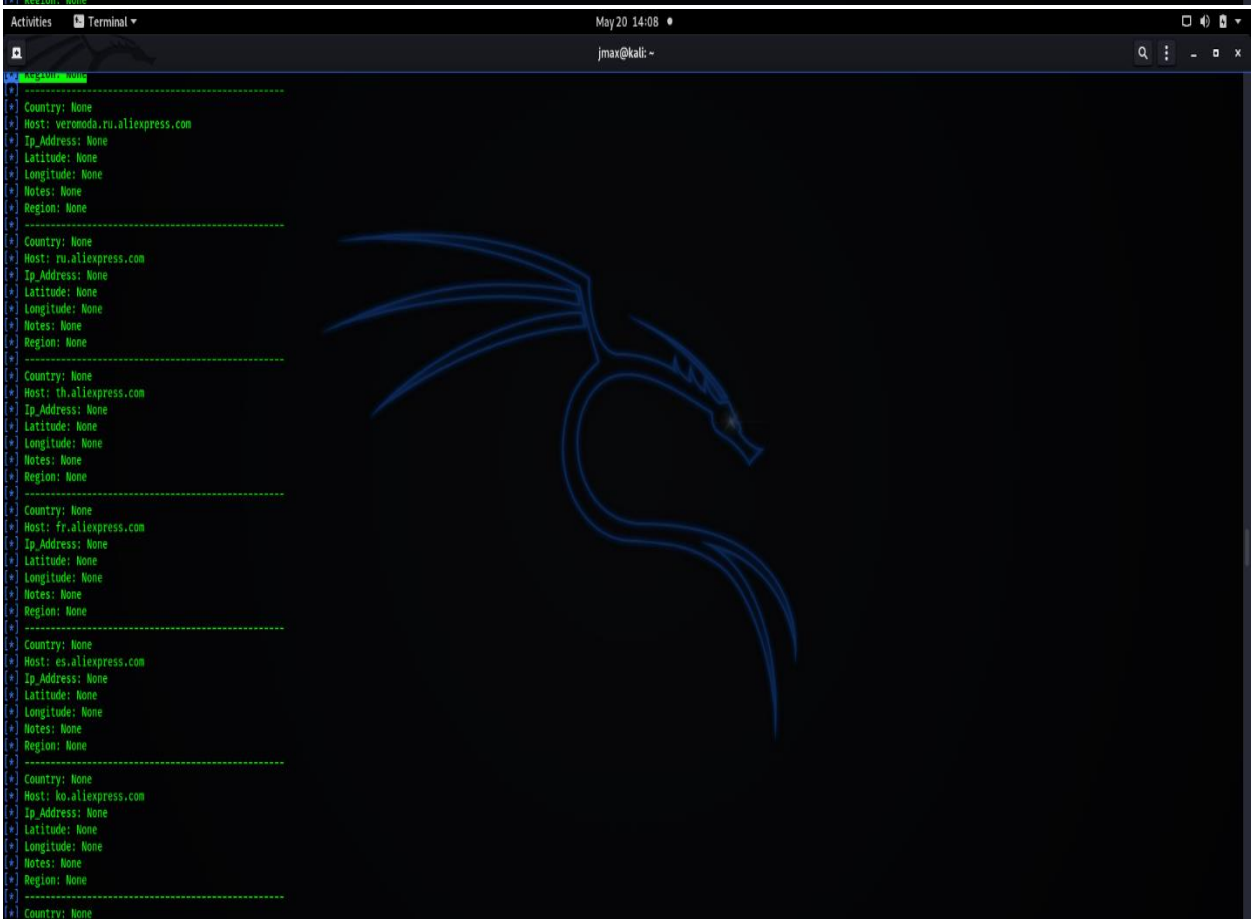
2. Recon-ng Tool

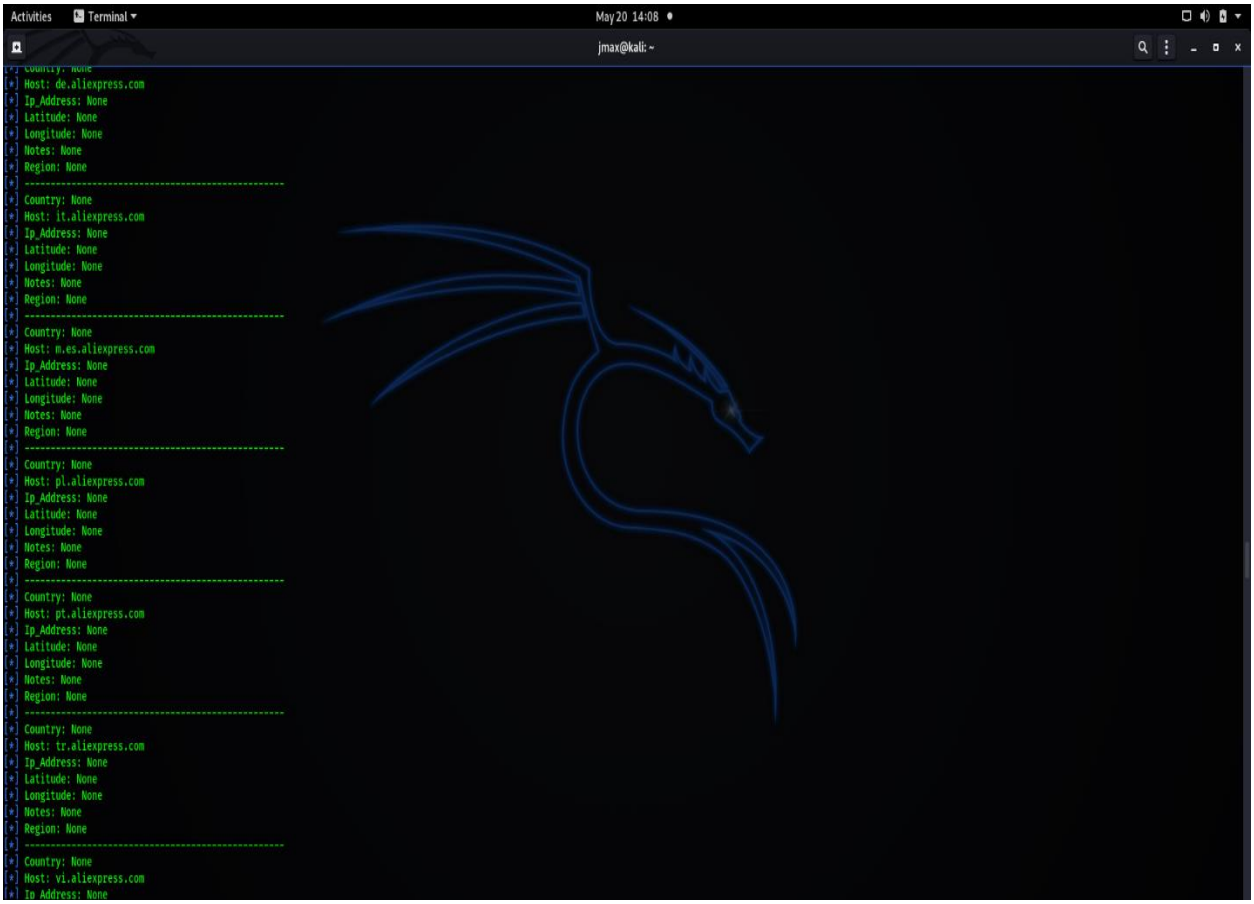
Recon-ng is a Python-based Web Reconnaissance framework with a lot of features. Recon-ng is a completely modular framework that allows even the most inexperienced Python programmers to contribute. The “module” class is subclassed by each module.

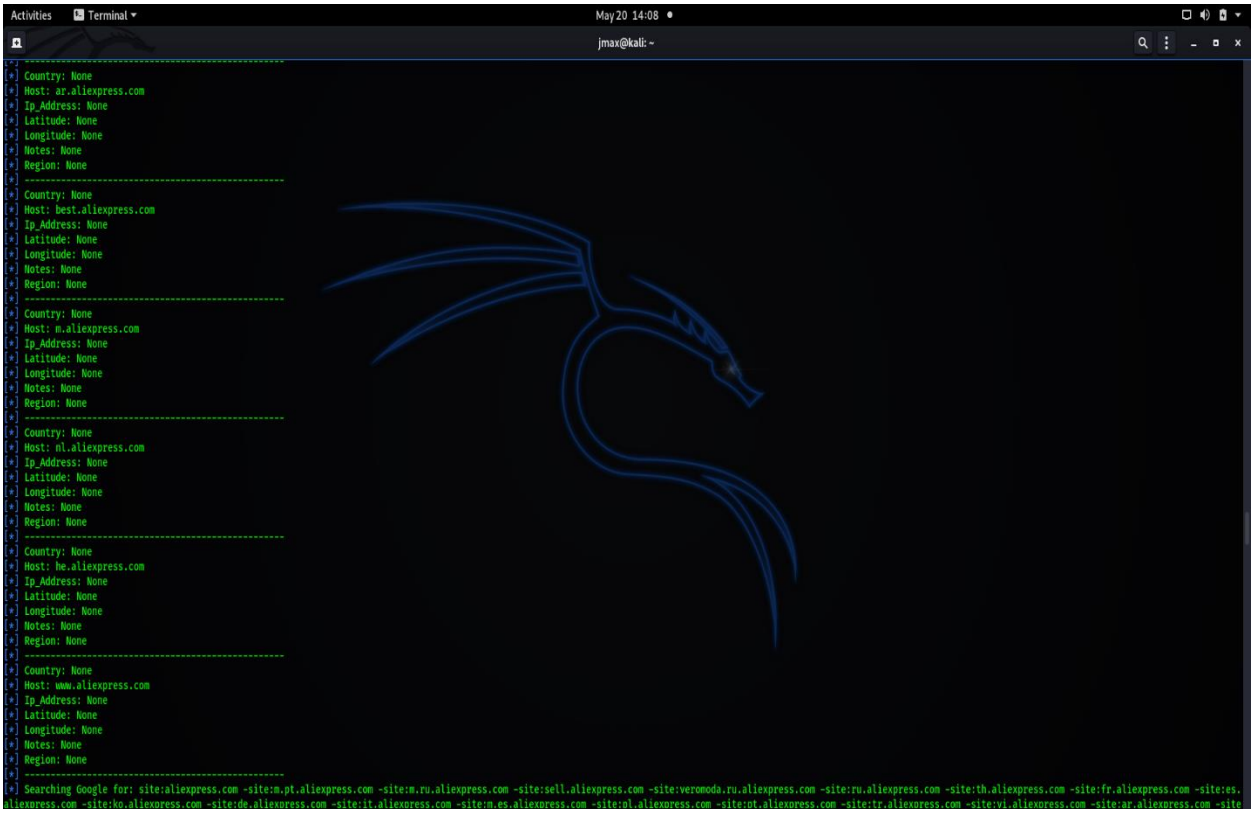


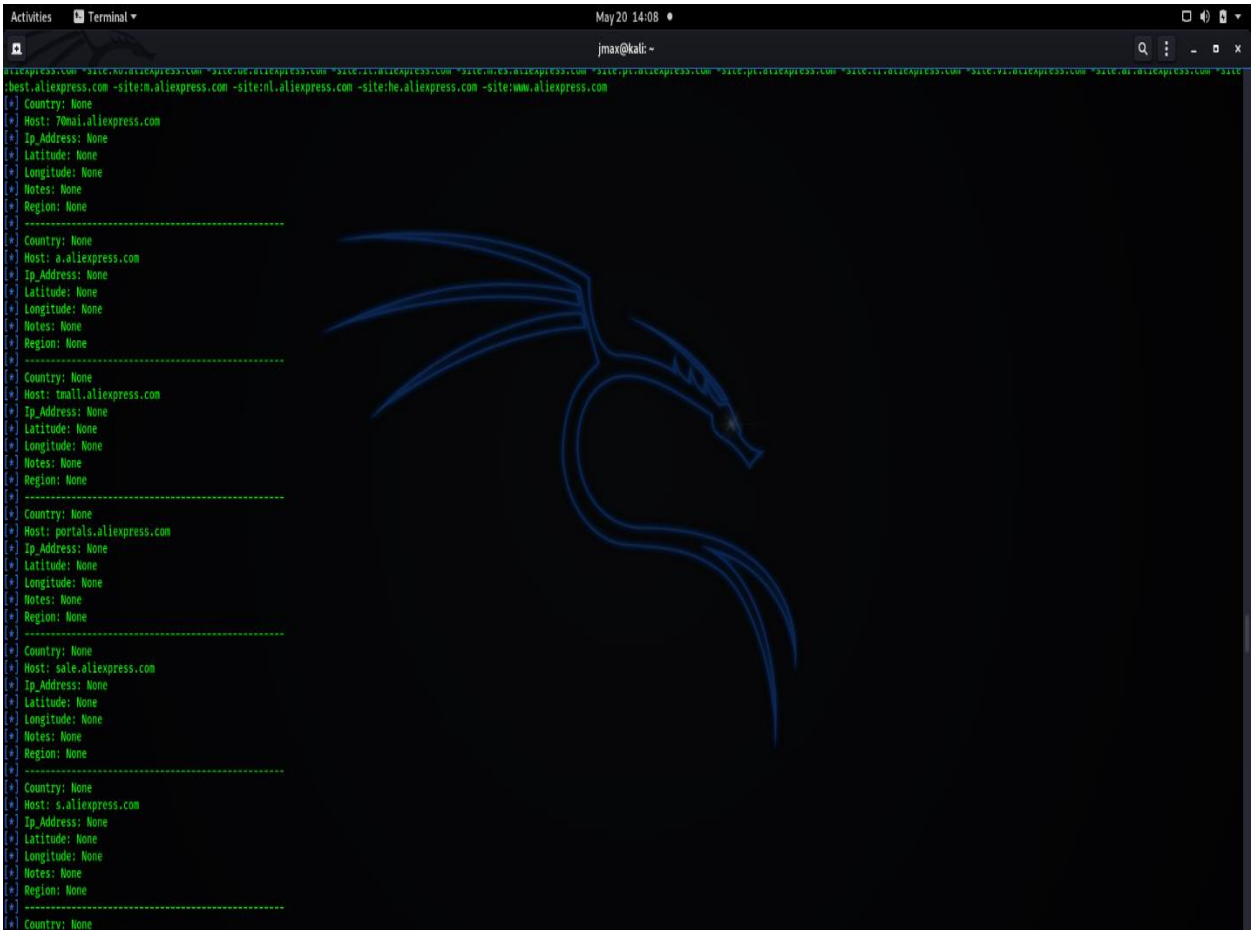

Activities
Terminal
May 20 11:51
jmax@kali: ~
recon/domains-vulnerabilities/ghdb
recon/domains-vulnerabilities/xssed
recon/hosts-domains/migrate_hosts
recon/hosts-hosts/bing_ip
recon/hosts-hosts/ipinfodb
recon/hosts-hosts/ipstack
recon/hosts-hosts/resolve
recon/hosts-hosts/reverse_resolve
recon/hosts-hosts/ssltools
recon/hosts-hosts/virustotal
recon/hosts-locations/migrate_hosts
recon/hosts-ports/binaryedge
recon/hosts-ports/shodan_ip
recon/locations-locations/geocode
recon/locations-locations/reverse_geocode
recon/locations-pushpins/flickr
recon/locations-pushpins/shodan
recon/locations-pushpins/twitter
recon/locations-pushpins/youtube
recon/netblocks-companies/whois_orgs
recon/netblocks-hosts/reverse_resolve
recon/netblocks-hosts/shodan_net
recon/netblocks-hosts/virustotal
recon/netblocks-ports/census_2012
recon/netblocks-ports/censysio
recon/ports-hosts/migrate_ports
recon/profiles-contacts/bing_linkedin_contacts
recon/profiles-contacts/dev_diver
recon/profiles-contacts/github_users
recon/profiles-profiles/namechk
recon/profiles-profiles/profiler
recon/profiles-profiles/twitter_mentioned
recon/profiles-profiles/twitter_mentions
recon/profiles-repositories/github_repos
recon/repositories-profiles/github_commits
recon/repositories-vulnerabilities/gists_search
recon/repositories-vulnerabilities/github_dorks
Reporting
reporting/csv
reporting/html
reporting/json
reporting/list
reporting/proxifier
reporting/pushpin
reporting/xlsx
reporting/xml
[recon-ng][default] >

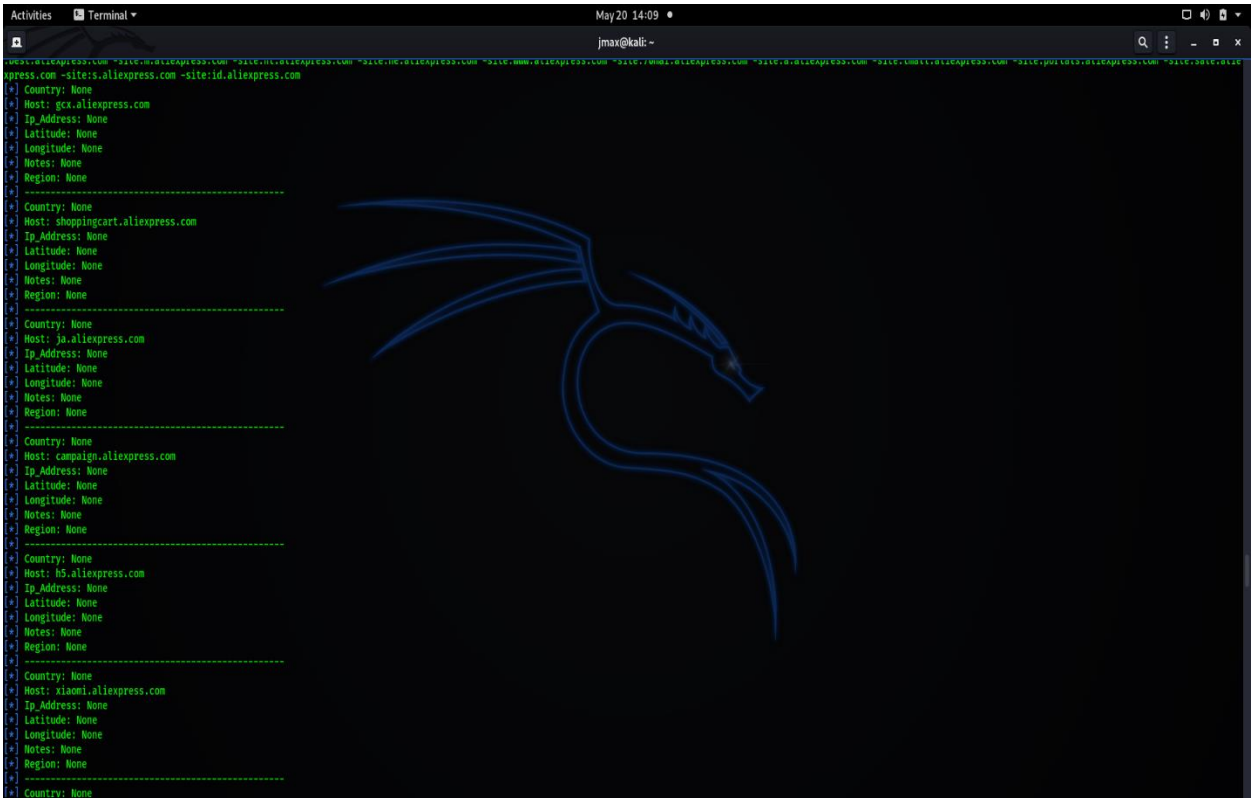

Activities
Terminal
May 20 13:36
jmax@kali: ~
reporting/xml
[recon-ng][default] > modules search doamains
[*] Searching installed modules for 'doamains'...
[!] No modules found.
Searches installed modules
Usage: modules search [<regex>]
[recon-ng][default] > modules search domains
[*] Searching installed modules for 'domains'...
Recon
recon/companies-domains/pen
recon/companies-domains/viewdns_reverse_whois
recon/companies-domains/whoxy_dns
recon/contacts-domains/migrate_contacts
recon/domains-companies/pen
recon/domains-companies/whoxy_whois
recon/domains-contacts/hunter_io
recon/domains-contacts/pen
recon/domains-contacts/pgp_search
recon/domains-contacts/whois_pocs
recon/domains-contacts/wikileaker
recon/domains-credentials/pwnedlist/api_usage
recon/domains-credentials/pwnedlist/domain_ispwned
recon/domains-credentials/pwnedlist/leak_lookup
recon/domains-credentials/pwnedlist/leaks_dump
recon/domains-credentials/scylla
recon/domains-domains/brute_suffix
recon/domains-hosts/binaryedge
recon/domains-hosts/bing_domain_api
recon/domains-hosts/bing_domain_web
recon/domains-hosts/brute_hosts
recon/domains-hosts/builtwith
recon/domains-hosts/certificate_transparency
recon/domains-hosts/google_site_web
recon/domains-hosts/hackertarget
recon/domains-hosts/mx_spf_ip
recon/domains-hosts/netcraft
recon/domains-hosts/shodan_hostname
recon/domains-hosts/ssl_san
recon/domains-hosts/threatcrowd
recon/domains-hosts/threatminer
recon/domains-vulnerabilities/ghdb
recon/domains-vulnerabilities/xssed
recon/hosts-domains/migrate_hosts
[recon-ng][default] >


Activities
Terminal
May 20 14:08
jmax@kali: ~
[recon-ng][default][google_site_web] > info
Name: Google Hostname Enumerator
Author: Tim Tomes (@lanmaster53)
Version: 1.0
Description:
Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with
the results.
Options:
Name Current Value Required Description
SOURCE aliexpress.com yes source of input (see 'info' for details)
Source Options:
default SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
<string> string representing a single input
<path> path to a file containing a list of inputs
query <sql> database query returning one column of inputs
[recon-ng][default][google_site_web] > run
ALIEXPRESS.COM
[*] Searching Google for: site:aliexpress.com
[*] Country: None
[*] Host: m.pt.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: m.ru.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: sell.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None

Activities
Terminal
May 20 14:08
jmax@kali: ~
[*] Country: None
[*] Host: veromoda.ru.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: ru.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: th.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: fr.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: es.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: ko.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None


Activities
Terminal
May 20 14:08
jmax@kali: ~
[*] Country: None
[*] Host: de.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] Country: None
[*] Host: it.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] Country: None
[*] Host: m.es.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] Country: None
[*] Host: pl.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] Country: None
[*] Host: pt.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] Country: None
[*] Host: tr.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] Country: None
[*] Host: vi.aliexpress.com
[*] Ip_Address: None


Activities
Terminal
May 20 14:08
jmax@kali: ~
[*] ----------
[*] Country: None
[*] Host: ar.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] Country: None
[*] Host: best.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] Country: None
[*] Host: m.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] Country: None
[*] Host: nl.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] Country: None
[*] Host: he.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] Country: None
[*] Host: www.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
aliexpress.com -site:ko.aliexpress.com -site:de.aliexpress.com -site:it.aliexpress.com -site:m.es.aliexpress.com -site:pl.aliexpress.com -site:pt.aliexpress.com -site:tr.aliexpress.com -site:vi.aliexpress.com -site:ar.aliexpress.com -site


Activities
Terminal
May 20 14:08
jmax@kali: ~
best.aliexpress.com -site:m.aliexpress.com -site:nl.aliexpress.com -site:he.aliexpress.com -site:www.aliexpress.com
[*] Country: None
[*] Host: 70mai.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---
[*] Country: None
[*] Host: a.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---
[*] Country: None
[*] Host: tmall.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---
[*] Country: None
[*] Host: portals.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---
[*] Country: None
[*] Host: sale.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---
[*] Country: None
[*] Host: s.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---
[*] Country: None


Activities
Terminal
May 20 14:09
jmax@kali: ~
press.com -site:s.aliexpress.com -site:id.aliexpress.com
[*] Country: None
[*] Host: gcx.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---
[*] Country: None
[*] Host: shoppingcart.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---
[*] Country: None
[*] Host: ja.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---
[*] Country: None
[*] Host: campaign.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---
[*] Country: None
[*] Host: h5.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---
[*] Country: None
[*] Host: xiaomi.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---
[*] Country: None

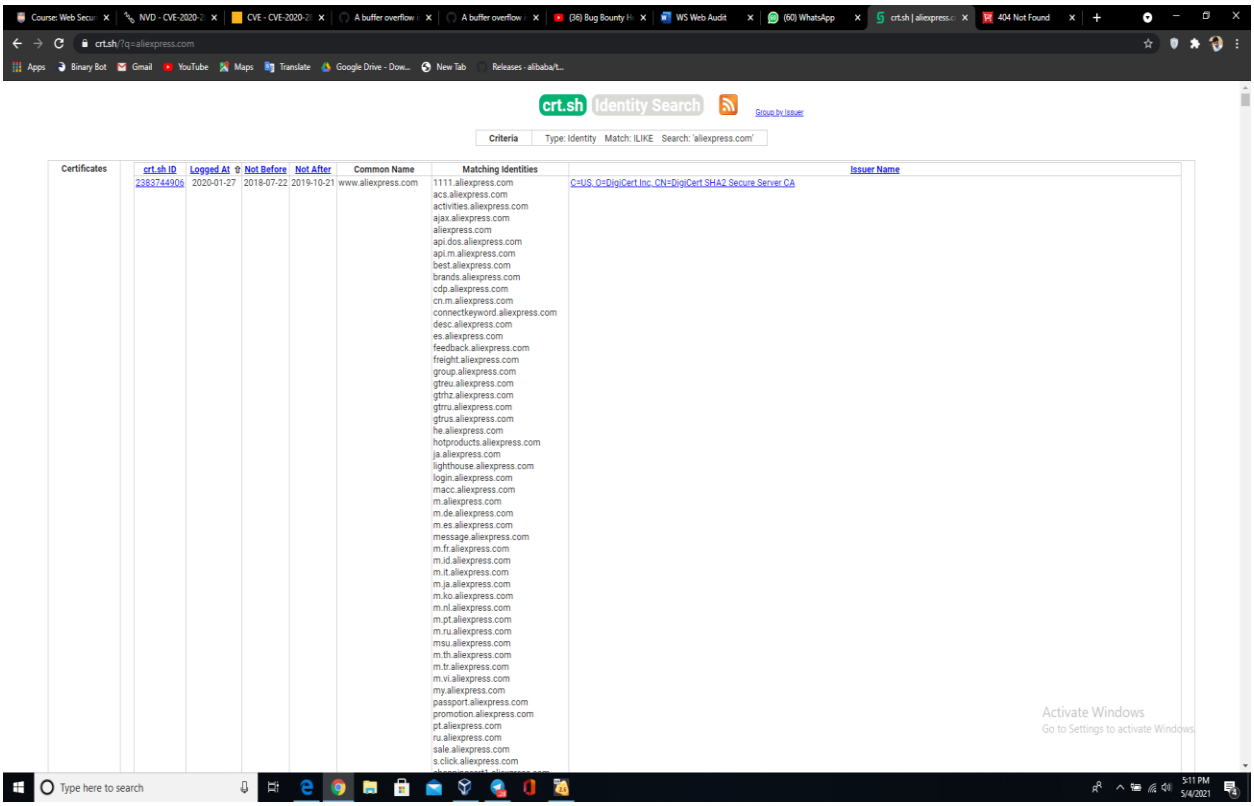

Activities
Terminal
May 20 14:09
jmax@kali: ~
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: passport.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: kpytomoa.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: ugreen.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: baseus.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: login.aliexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
aliexpress.com -site:ko.aliexpress.com -site:de.aliexpress.com -site:it.aliexpress.com -site:m.es.aliexpress.com -site:pl.aliexpress.com -site:pt.aliexpress.com -site:tr.aliexpress.com -site:vi.aliexpress.com -site:ar.aliexpress.com -site
:best.aliexpress.com -site:m.aliexpress.com -site:nl.aliexpress.com -site:he.aliexpress.com -site:www.aliexpress.com -site:70mai.aliexpress.com -site:a.aliexpress.com -site:tmall.aliexpress.com -site:portals.aliexpress.com -site:sale.alie
xpress.com -site:s.aliexpress.com -site:id.aliexpress.com -site:gcx.aliexpress.com -site:shoppingcart.aliexpress.com -site:ja.aliexpress.com -site:campaign.aliexpress.com -site:h5.aliexpress.com -site:xiaomi.aliexpress.com -site:motermsho
p.aliexpress.com -site:service.aliexpress.com -site:kziems.aliexpress.com -site:developers.aliexpress.com -site:passport.aliexpress.com -site:kpytomoa.aliexpress.com -site:ugreen.aliexpress.com -site:baseus.aliexpress.com -site:login.alie
xpress.com -site:idoingexpert.aliexpress.com -site:u7-jewellery.aliexpress.com -site:jianwu.aliexpress.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1601.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
aliexpress.com -site:ko.aliexpress.com -site:de.aliexpress.com -site:it.aliexpress.com -site:m.es.aliexpress.com -site:pl.aliexpress.com -site:pt.aliexpress.com -site:tr.aliexpress.com -site:vi.aliexpress.com -site:ar.aliexpress.com -site
:best.aliexpress.com -site:m.aliexpress.com -site:nl.aliexpress.com -site:he.aliexpress.com -site:www.aliexpress.com -site:70mai.aliexpress.com -site:a.aliexpress.com -site:tmall.aliexpress.com -site:portals.aliexpress.com -site:sale.alie
xpress.com -site:s.aliexpress.com -site:id.aliexpress.com -site:gcx.aliexpress.com -site:shoppingcart.aliexpress.com -site:ja.aliexpress.com -site:campaign.aliexpress.com -site:h5.aliexpress.com -site:xiaomi.aliexpress.com -site:motermsho
p.aliexpress.com -site:service.aliexpress.com -site:kziems.aliexpress.com -site:developers.aliexpress.com -site:passport.aliexpress.com -site:kpytomoa.aliexpress.com -site:ugreen.aliexpress.com -site:baseus.aliexpress.com -site:login.alie
xpress.com -site:idoingexpert.aliexpress.com -site:u7-jewellery.aliexpress.com -site:jianwu.aliexpress.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1701.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
aliexpress.com -site:ko.aliexpress.com -site:de.aliexpress.com -site:it.aliexpress.com -site:m.es.aliexpress.com -site:pl.aliexpress.com -site:pt.aliexpress.com -site:tr.aliexpress.com -site:vi.aliexpress.com -site:ar.aliexpress.com -site
:best.aliexpress.com -site:m.aliexpress.com -site:nl.aliexpress.com -site:he.aliexpress.com -site:www.aliexpress.com -site:70mai.aliexpress.com -site:a.aliexpress.com -site:tmall.aliexpress.com -site:portals.aliexpress.com -site:sale.alie
xpress.com -site:s.aliexpress.com -site:id.aliexpress.com -site:gcx.aliexpress.com -site:shoppingcart.aliexpress.com -site:ja.aliexpress.com -site:campaign.aliexpress.com -site:h5.aliexpress.com -site:xiaomi.aliexpress.com -site:motermsho
p.aliexpress.com -site:service.aliexpress.com -site:kziems.aliexpress.com -site:developers.aliexpress.com -site:passport.aliexpress.com -site:kpytomoa.aliexpress.com -site:ugreen.aliexpress.com -site:baseus.aliexpress.com -site:login.alie
xpress.com -site:idoingexpert.aliexpress.com -site:u7-jewellery.aliexpress.com -site:jianwu.aliexpress.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1801.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
aliexpress.com -site:ko.aliexpress.com -site:de.aliexpress.com -site:it.aliexpress.com -site:m.es.aliexpress.com -site:pl.aliexpress.com -site:pt.aliexpress.com -site:tr.aliexpress.com -site:vi.aliexpress.com -site:ar.aliexpress.com -site
:best.aliexpress.com -site:m.aliexpress.com -site:nl.aliexpress.com -site:he.aliexpress.com -site:www.aliexpress.com -site:70mai.aliexpress.com -site:a.aliexpress.com -site:tmall.aliexpress.com -site:portals.aliexpress.com -site:sale.alie
xpress.com -site:s.aliexpress.com -site:id.aliexpress.com -site:gcx.aliexpress.com -site:shoppingcart.aliexpress.com -site:ja.aliexpress.com -site:campaign.aliexpress.com -site:h5.aliexpress.com -site:xiaomi.aliexpress.com -site:motermsho
p.aliexpress.com -site:service.aliexpress.com -site:kziems.aliexpress.com -site:developers.aliexpress.com -site:passport.aliexpress.com -site:kpytomoa.aliexpress.com -site:ugreen.aliexpress.com -site:baseus.aliexpress.com -site:login.alie
xpress.com -site:idoingexpert.aliexpress.com -site:u7-jewellery.aliexpress.com -site:jianwu.aliexpress.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1901.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
aliexpress.com -site:ko.aliexpress.com -site:de.aliexpress.com -site:it.aliexpress.com -site:m.es.aliexpress.com -site:pl.aliexpress.com -site:pt.aliexpress.com -site:tr.aliexpress.com -site:vi.aliexpress.com -site:ar.aliexpress.com -site
:best.aliexpress.com -site:m.aliexpress.com -site:nl.aliexpress.com -site:he.aliexpress.com -site:www.aliexpress.com -site:70mai.aliexpress.com -site:a.aliexpress.com -site:tmall.aliexpress.com -site:portals.aliexpress.com -site:sale.alie
xpress.com -site:s.aliexpress.com -site:id.aliexpress.com -site:gcx.aliexpress.com -site:shoppingcart.aliexpress.com -site:ja.aliexpress.com -site:campaign.aliexpress.com -site:h5.aliexpress.com -site:xiaomi.aliexpress.com -site:motermsho
p.aliexpress.com -site:service.aliexpress.com -site:kziems.aliexpress.com -site:developers.aliexpress.com -site:passport.aliexpress.com -site:kpytomoa.aliexpress.com -site:ugreen.aliexpress.com -site:baseus.aliexpress.com -site:login.alie
xpress.com -site:idoingexpert.aliexpress.com -site:u7-jewellery.aliexpress.com -site:jianwu.aliexpress.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 2001.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
aliexpress.com -site:ko.aliexpress.com -site:de.aliexpress.com -site:it.aliexpress.com -site:m.es.aliexpress.com -site:pl.aliexpress.com -site:pt.aliexpress.com -site:tr.aliexpress.com -site:vi.aliexpress.com -site:ar.aliexpress.com -site
:best.aliexpress.com -site:m.aliexpress.com -site:nl.aliexpress.com -site:he.aliexpress.com -site:www.aliexpress.com -site:70mai.aliexpress.com -site:a.aliexpress.com -site:tmall.aliexpress.com -site:portals.aliexpress.com -site:sale.alie
xpress.com -site:s.aliexpress.com -site:id.aliexpress.com -site:gcx.aliexpress.com -site:shoppingcart.aliexpress.com -site:ja.aliexpress.com -site:campaign.aliexpress.com -site:h5.aliexpress.com -site:xiaomi.aliexpress.com -site:motermsho
p.aliexpress.com -site:service.aliexpress.com -site:kziems.aliexpress.com -site:developers.aliexpress.com -site:passport.aliexpress.com -site:kpytomoa.aliexpress.com -site:ugreen.aliexpress.com -site:baseus.aliexpress.com -site:login.alie
xpress.com -site:idoingexpert.aliexpress.com -site:u7-jewellery.aliexpress.com -site:jianwu.aliexpress.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 2101.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
aliexpress.com -site:ko.aliexpress.com -site:de.aliexpress.com -site:it.aliexpress.com -site:m.es.aliexpress.com -site:pl.aliexpress.com -site:pt.aliexpress.com -site:tr.aliexpress.com -site:vi.aliexpress.com -site:ar.aliexpress.com -site
:best.aliexpress.com -site:m.aliexpress.com -site:nl.aliexpress.com -site:he.aliexpress.com -site:www.aliexpress.com -site:70mai.aliexpress.com -site:a.aliexpress.com -site:tmall.aliexpress.com -site:portals.aliexpress.com -site:sale.alie
xpress.com -site:s.aliexpress.com -site:id.aliexpress.com -site:gcx.aliexpress.com -site:shoppingcart.aliexpress.com -site:ja.aliexpress.com -site:campaign.aliexpress.com -site:h5.aliexpress.com -site:xiaomi.aliexpress.com -site:motermsho
p.aliexpress.com -site:service.aliexpress.com -site:kziems.aliexpress.com -site:developers.aliexpress.com -site:passport.aliexpress.com -site:kpytomoa.aliexpress.com -site:ugreen.aliexpress.com -site:baseus.aliexpress.com -site:login.alie
xpress.com -site:idoingexpert.aliexpress.com -site:u7-jewellery.aliexpress.com -site:jianwu.aliexpress.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 2201.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.

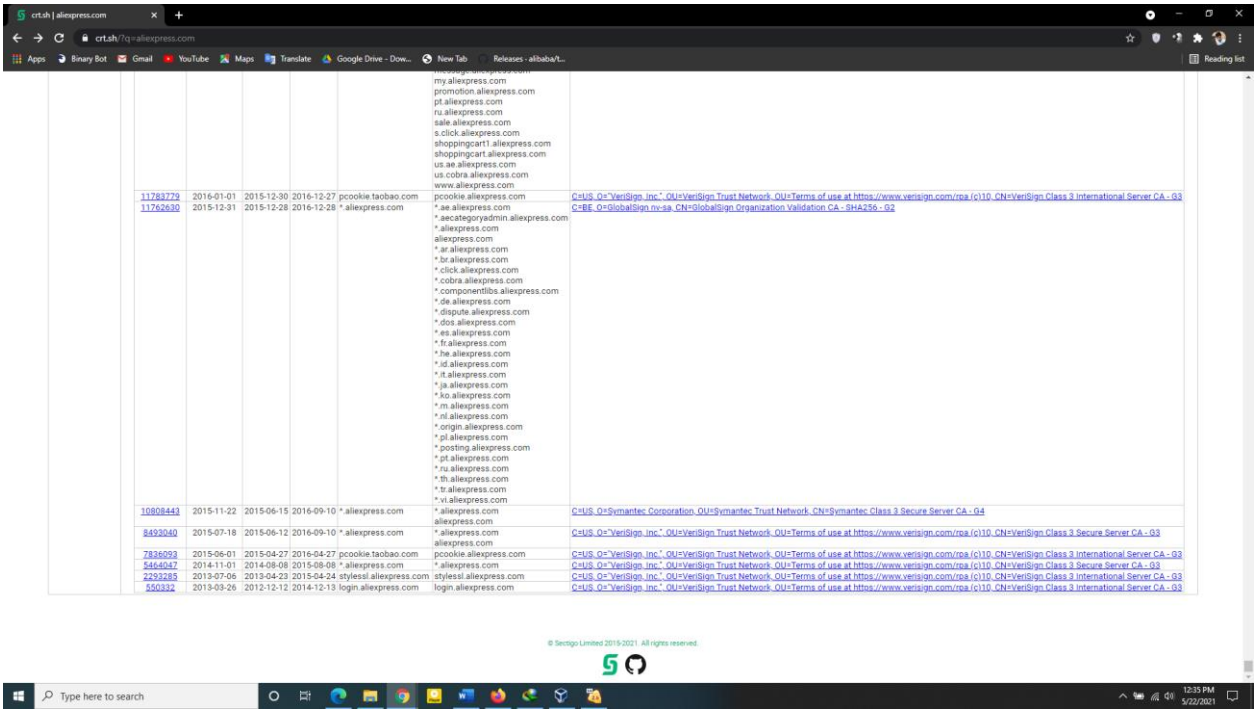

Activities
Terminal
May 20 14:09
jmax@kali: ~
[*] No New Subdomains Found on the Current Page. Jumping to Result 2601.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
[*] No New Subdomains Found on the Current Page. Jumping to Result 2701.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
[*] No New Subdomains Found on the Current Page. Jumping to Result 2801.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
[*] No New Subdomains Found on the Current Page. Jumping to Result 2901.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
[*] No New Subdomains Found on the Current Page. Jumping to Result 3001.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
[*] No New Subdomains Found on the Current Page. Jumping to Result 3101.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
[*] No New Subdomains Found on the Current Page. Jumping to Result 3201.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.


Activities
Terminal
May 20 14:09
jmax@kali: ~
[*] No New Subdomains Found on the Current Page. Jumping to Result 4301.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
[*] No New Subdomains Found on the Current Page. Jumping to Result 4401.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
[*] No New Subdomains Found on the Current Page. Jumping to Result 4501.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
[*] No New Subdomains Found on the Current Page. Jumping to Result 4601.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
[*] No New Subdomains Found on the Current Page. Jumping to Result 4701.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
[*] No New Subdomains Found on the Current Page. Jumping to Result 4801.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.
[*] No New Subdomains Found on the Current Page. Jumping to Result 4901.
[*] Searching Google for: site:aliexpress.com -site:m.pt.aliexpress.com -site:m.ru.aliexpress.com -site:sell.aliexpress.com -site:veromoda.ru.aliexpress.com -site:ru.aliexpress.com -site:th.aliexpress.com -site:fr.aliexpress.com -site:es.


Activities
Terminal
May 20 14:10
jmax@kali: ~
[*] No New Subdomains Found on the Current Page. Jumping to Result 4501.
[*] No New Subdomains Found on the Current Page. Jumping to Result 4601.
[*] No New Subdomains Found on the Current Page. Jumping to Result 4701.
[*] No New Subdomains Found on the Current Page. Jumping to Result 4801.
[*] No New Subdomains Found on the Current Page. Jumping to Result 4901.
[*] No New Subdomains Found on the Current Page. Jumping to Result 5001.
[!] Google CAPTCHA triggered. No bypass available.
SUMMARY
[*] 47 total (3 new) hosts found.

3. Crt.sh


crt.sh Identity Search
Group by Issuer
Criteria
Type: Identity Match: ILIKE Search: 'aliexpress.com'
Certificates
crt.sh ID
Logged At
Not Before
Not After
Common Name
Matching Identities
Issuer Name
2383744906
2020-01-27
2018-07-22
2019-10-21
www.aliexpress.com
1111.aliexpress.com
acs.aliexpress.com
activities.aliexpress.com
ajax.aliexpress.com
aliexpress.com
api.dos.aliexpress.com
api.m.aliexpress.com
best.aliexpress.com
brands.aliexpress.com
cdp.aliexpress.com
cn.m.aliexpress.com
connectkeyword.aliexpress.com
desc.aliexpress.com
es.aliexpress.com
feedback.aliexpress.com
freight.aliexpress.com
group.aliexpress.com
gtreu.aliexpress.com
gtrhz.aliexpress.com
gtrru.aliexpress.com
gtrus.aliexpress.com
he.aliexpress.com
hotproducts.aliexpress.com
ja.aliexpress.com
lighthouse.aliexpress.com
login.aliexpress.com
macc.aliexpress.com
m.aliexpress.com
m.de.aliexpress.com
m.es.aliexpress.com
message.aliexpress.com
m.fr.aliexpress.com
m.id.aliexpress.com
m.it.aliexpress.com
m.ja.aliexpress.com
m.ko.aliexpress.com
m.nl.aliexpress.com
m.pt.aliexpress.com
m.ru.aliexpress.com
msu.aliexpress.com
m.th.aliexpress.com
m.tr.aliexpress.com
m.vi.aliexpress.com
my.aliexpress.com
passport.aliexpress.com
promotion.aliexpress.com
pt.aliexpress.com
ru.aliexpress.com
sale.aliexpress.com
s.click.aliexpress.com
C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
Activate Windows
Go to Settings to activate Windows.
Type here to search
5:11 PM
5/4/2021


crt.sh | aliexpress.com
crt.sh/?q=aliexpress.com
my.aliexpress.com
promotion.aliexpress.com
pt.aliexpress.com
ru.aliexpress.com
sale.aliexpress.com
s.click.aliexpress.com
shoppingcart1.aliexpress.com
shoppingcart.aliexpress.com
us.ae.aliexpress.com
us.cobra.aliexpress.com
www.aliexpress.com
11783779 2016-01-01 2015-12-30 2016-12-27 pcookie.taobao.com pcookie.aliexpress.com C=US, O="VeriSign, Inc.", OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 International Server CA - G3
11762630 2015-12-31 2015-12-28 2016-12-28 *.aliexpress.com C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation CA - SHA256 - G2
*.ae.aliexpress.com
*.aecategoryadmin.aliexpress.com
*.aliexpress.com
aliexpress.com
*.ar.aliexpress.com
*.br.aliexpress.com
*.click.aliexpress.com
*.cobra.aliexpress.com
*.componentlibs.aliexpress.com
*.de.aliexpress.com
*.dispute.aliexpress.com
*.dos.aliexpress.com
*.es.aliexpress.com
*.fr.aliexpress.com
*.he.aliexpress.com
*.id.aliexpress.com
*.it.aliexpress.com
*.ja.aliexpress.com
*.ko.aliexpress.com
*.m.aliexpress.com
*.nl.aliexpress.com
*.origin.aliexpress.com
*.pl.aliexpress.com
*.posting.aliexpress.com
*.pt.aliexpress.com
*.ru.aliexpress.com
*.th.aliexpress.com
*.tr.aliexpress.com
*.vi.aliexpress.com
10808443 2015-11-22 2015-06-15 2016-09-10 *.aliexpress.com *.aliexpress.com C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4
8493040 2015-07-18 2015-06-12 2016-09-10 *.aliexpress.com aliexpress.com C=US, O="VeriSign, Inc.", OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 Secure Server CA - G3
7836093 2015-06-01 2015-04-27 2016-04-27 pcookie.taobao.com pcookie.aliexpress.com C=US, O="VeriSign, Inc.", OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 International Server CA - G3
5464047 2014-11-01 2014-08-08 2015-08-08 *.aliexpress.com *.aliexpress.com C=US, O="VeriSign, Inc.", OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 Secure Server CA - G3
2293285 2013-07-06 2013-04-23 2015-04-24 stylessl.aliexpress.com stylessl.aliexpress.com C=US, O="VeriSign, Inc.", OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 International Server CA - G3
150332 2013-03-26 2012-12-12 2014-12-13 login.aliexpress.com login.aliexpress.com C=US, O="VeriSign, Inc.", OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 International Server CA - G3
© Sectigo Limited 2015-2021. All rights reserved.
Type here to search
12:35 PM
5/22/2021

Website Vulnerability Enumeration

Nikto

Nikto is a website vulnerability tool that is widely used in penetration testing and is considered an industry standard. Nikto's main function is to evaluate websites and webapps and report any vulnerabilities that can be used to attack or exploit the site back to the tester**.**

In according to my selected domain,I perform the scan using nikto tool(2.1.6).

jmax@kali:~$ nikto -h aliexpress.com

- Nikto v2.1.6

+ Target IP: 47.254.177.101

+ Target Hostname: aliexpress.com

+ Target Port: 80

+ Start Time: 2021-05-03 12:18:47 (GMT5.5)

+ Server: Tengine/Aserver

+ Cookie ali_apache_id created without the httponly flag

+ IP address found in the 'ali_apache_id' cookie. The IP is "33.0.189.215".

+ IP address found in the 'set-cookie' header. The IP is "33.0.189.215".

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ Uncommon header 'eagleeye-traceid' found, with contents: 2100bdd716200245275748323e8f7d

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ Root page / redirects to: https://www.aliexpress.com/

+ Uncommon header 'bxpunish' found, with contents: 1

+ Retrieved via header: aebridge033000189215.de81[web,302]

+ /cgi-bin/cart32.exe: request cart32.exe/cart32clientlist

+ /cgi-bin/classified.cgi: Check Phrack 55 for info by RFP

+ /cgi-bin/download.cgi: v1 by Matt Wright; check info in Phrack 55 by RFP

+ /cgi-bin/flexform.cgi: Check Phrack 55 for info by RFP, allows to append info to writable files.

+ /cgi-bin/flexform: Check Phrack 55 for info by RFP, allows to append info to writable files.

+ /cgi-bin/lwgate.cgi: Check Phrack 55 for info by RFP, http://www.phrack.com/show.php?p=55&a=7

+ /cgi-bin/LWGate.cgi: Check Phrack 55 for info by RFP, http://www.phrack.com/show.php?p=55&a=7

+ /cgi-bin/lwgate: Check Phrack 55 for info by RFP

+ /cgi-bin/LWGate: Check Phrack 55 for info by RFP

+ /cgi-bin/perlshop.cgi: v3.1 by ARPAnet.com; check info in Phrack 55 by RFP

+ OSVDB-396: /_vti_bin/shtml.exe: Attackers may be able to crash FrontPage by requesting a DOS device, like shtml.exe/aux.htm -- a DoS was not attempted.

+ /cgi-bin/handler.cgi: Variation of Irix Handler? Has been seen from other CGI scanners.

+ /cgi-bin/finger: finger other users, may be other commands?

+ /cgi-bin/finger.pl: finger other users, may be other commands?

+ /cgi-bin/get32.exe: This can allow attackers to execute arbitrary commands remotely.

+ /cgi-bin/gm-authors.cgi: GreyMatter 'password' file, that controls who can post. This contains login and password information and is installed mode 666 by default.

+ OSVDB-3093: /cgi-bin/nph-exploitscanget.cgi: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/nph-maillist.pl: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/parse-file: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/php-cgi: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/pollssi.cgi: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/postcards.cgi: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/profile.cgi: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/quikstore.cfg: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/register.cgi: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/replicator/webpage.cgi/: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/rightfax/fuwww.dll/?: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/rmp_query: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/robpoll.cgi: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/scripts/*%0a.pl: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/simplestguest.cgi: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/simplestmail.cgi: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/statusconfig.pl: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/sws/manager.pl: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/texis/phine: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/Upload.pl: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/utm/admin: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/utm/utm_stat: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/_vti_bin/fpcount.exe?Page=default.htm|Image=3|Digits=15: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/_vti_pvt/doctodep.btr: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/cfgwiz.exe: cfgwiz.exe is a Norton Anti-Virus file and should not be available via the web site.

+ OSVDB-3093: /cgi-bin/Cgitest.exe: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/mailform.exe: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/ms_proxy_auth_query/: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/post16.exe: This might be interesting... has been seen in web logs from an unknown scanner.

+ OSVDB-3093: /cgi-bin/.htaccess: Contains authorization information

+ OSVDB-3093: /cgi-bin/.htaccess.old: Backup/Old copy of .htaccess - Contains authorization information

+ OSVDB-3093: /cgi-bin/.htaccess.save: Backup/Old copy of .htaccess - Contains authorization information

+ OSVDB-3093: /cgi-bin/.htaccess~: Backup/Old copy of .htaccess - Contains authorization information

+ OSVDB-3093: /cgi-bin/.htpasswd: Contains authorization information

+ OSVDB-3093: /cgi-bin/.passwd: Contains authorization information

+ OSVDB-3093: /cgi-bin/.wwwacl: Contains authorization information

+ OSVDB-3093: /cgi-bin/.www_acl: Contains authorization information

+ OSVDB-3093: /.htpasswd: Contains authorization information

+ OSVDB-3093: /.bashrc: User home dir was found with a shell rc file. This may reveal file and path information.

+ OSVDB-3093: /.htaccess: Contains configuration and/or authorization information

+ OSVDB-3233: /_vti_bin/shtml.exe/_vti_rpc: FrontPage may be installed.

+ OSVDB-3233: /cgi-bin/test-cgi.bat: This is an Apache for Win default. If Apache is lower than 1.3.23, this can be exploited as in test-cgi.bat?|dir+c:+>..\htdocs\listing.txt, but may not allow data sent back to the browser.

+ OSVDB-3233: /cgi-bin/admin.pl: Default FrontPage CGI found.

+ OSVDB-3233: /cgi-bin/cfgwiz.exe: Default FrontPage CGI found.

+ OSVDB-3233: /cgi-bin/CGImail.exe: Default FrontPage CGI found.

+ OSVDB-3233: /cgi-bin/contents.htm: Default FrontPage CGI found.

+ OSVDB-3233: /cgi-bin/fpadmin.htm: Default FrontPage CGI found.

+ OSVDB-3233: /cgi-bin/fpremadm.exe: Default FrontPage CGI found.

+ OSVDB-3233: /cgi-bin/fpsrvadm.exe: Default FrontPage CGI found.

+ OSVDB-3233: /_vti_bin/cfgwiz.exe: Default FrontPage CGI found.

+ OSVDB-3233: /_vti_bin/CGImail.exe: Default FrontPage CGI found.

+ OSVDB-3233: /_vti_bin/fpremadm.exe: Default FrontPage CGI found.

+ OSVDB-3233: /_vti_bin/fpsrvadm.exe: Default FrontPage CGI found.

+ OSVDB-3233: /_vti_pvt/administrators.pwd: Default FrontPage file found, may be a password file.

+ OSVDB-3233: /_vti_pvt/authors.pwd: Default FrontPage file found, may be a password file.

+ OSVDB-3233: /_vti_pvt/service.pwd: Default FrontPage file found, may be a password file.

+ OSVDB-3233: /_vti_pvt/users.pwd: Default FrontPage file found, may be a password file.

+ OSVDB-3233: /cgi-bin/cgi-test.exe: Default CGI found

+ OSVDB-3380: /cgi-bin/imagemap: imagemap.exe was found. Many versions from different vendors contain flaws.

+ OSVDB-3380: /cgi-bin/imagemap.exe: imagemap.exe was found. Many versions from different vendors contain flaws.

+ OSVDB-3384: /cgi-bin/htimage.exe: htimage.exe may be vulnerable to a buffer overflow in the mapname portion. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2000/MS00-028. http://www.securityfocus.com/bid/1117

+ OSVDB-3514: /cgi-bin/vote.cgi: Mike's Vote CGI contained a bug which allowed arbitrary command execution (version 1.2), see http://freshmeat.net/projects/mikessurveycgi/

+ OSVDB-3515: /cgi-bin/quizme.cgi: Mike's Quiz Me! CGI contained a bug which allowed arbitrary command execution (version 0.5), see http://freshmeat.net/users/mikespice/

+ OSVDB-3568: /cgi-bin/sendform.cgi: This CGI by Rod Clark (v1.4.4 and below) may allow arbitrary file reading via email or allow spam to be sent. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0710. http://www.securityfocus.com/bid/5286.

+ OSVDB-4171: /ASP/cart/database/metacart.mdb: MetaCart2 is an ASP shopping cart. The database of customers is available via the web.

+ OSVDB-4171: /database/metacart.mdb: MetaCart2 is an ASP shopping cart. The database of customers is available via the web.

+ OSVDB-4171: /mcartfree/database/metacart.mdb: MetaCart2 is an ASP shopping cart. The database of customers is available via the web.

+ OSVDB-4171: /metacart/database/metacart.mdb: MetaCart2 is an ASP shopping cart. The database of customers is available via the web.

+ OSVDB-4171: /shop/database/metacart.mdb: MetaCart2 is an ASP shopping cart. The database of customers is available via the web.

+ OSVDB-4171: /shoponline/fpdb/shop.mdb: MetaCart2 is an ASP shopping cart. The database of customers is available via the web.

+ OSVDB-4171: /shopping/database/metacart.mdb: MetaCart2 is an ASP shopping cart. The database of customers is available via the web.

+ OSVDB-4192: /cgi-bin/gettransbitmap: Sun Answerbook2 is vulnerable to a buffer overflow in the gettransbitmap CGI. All default CGIs should be disabled or removed, and Answerbook2 should be disabled if not being used.

+ OSVDB-4237: /ban.bak: Bannermatic versions 1-3 reveal sensitive information from unprotected files. These files should be protected.

+ OSVDB-4261: /cgi-bin/VsSetCookie.exe?: A flaw in VsSetCookie.exe may allow attackers to guess a correct user name & gain access to the Lucent system.

+ OSVDB-4301: /cgi-bin/Webnews.exe: Some versions of WebNews are vulnerable to a buffer overflow. See http://www.nextgenss.com/advisories/netwinnews.txt for more info.

+ OSVDB-4301: /cgi-bin/webnews.pl: WebNews may contain some default users in the binary: testweb/newstest, alwn3845/imaptest, alwi3845/wtest3452, testweb2/wtest4879

+ OSVDB-436: /cgi-bin/sensepost.exe?/c+dir: The presence of sensepost.exe indicates the system is/was vulnerable to a Unicode flaw and was compromised with a test script from SensePost. The sensepost.exe allows command execution (it is a copy of cmd.exe), as did the original unicode exploit (see ht

+ OSVDB-4360: /acart2_0/acart2_0.mdb: Alan Ward A-Cart 2.0 allows remote user to read customer database file which may contain usernames, passwords, credit cards and more.

+ OSVDB-5689: /cgi-bin/namazu.cgi: Namazu search engine found. Vulnerable to XSS attacks (fixed 2001-11-25). Attacker could write arbitrary files outside docroot (fixed 2000-01-26). http://www.cert.org/advisories/CA-2000-02.html.

+ OSVDB-5709: /cgi-bin/.nsconfig: Contains authorization information

+ OSVDB-6666: /cgi-bin/hpnst.exe?c=p+i=SrvSystemInfo.html: HP Instant TopTools GoAhead WebServer hpnst.exe may be vulnerable to a DoS.

+ OSVDB-6695: /cgi-bin/rwcgi60: Oracle report server reveals system information without authorization. See Oracle note 133957.1 - Restricting Access to the Reports Server Environment and Output

+ OSVDB-6695: /cgi-bin/rwcgi60/showenv: Oracle report server reveals system information without authorization. See Oracle note 133957.1 - Restricting Access to the Reports Server Environment and Output

+ OSVDB-6698: /cgi-bin/classifieds/classifieds.cgi: Mike's Classifieds CGI contains a bug that allows arbitrary command execution on the server (untested), see http://freshmeat.net/projects/myclassifieds/

+ OSVDB-6699: /cgi-bin/calendar/index.cgi: Mike's Calendar CGI contains a bug that allows arbitrary command execution (version 1.4), see http://freshmeat.net/projects/mycalendar/

+ OSVDB-721: /..%252f..%252f..%252f..%252f..%252f../windows/repair/sam: BadBlue server is vulnerable to multiple remote exploits. See http://www.securiteam.com/exploits/5HP0M2A60G.html for more information.

+ OSVDB-721: /..%252f..%252f..%252f..%252f..%252f../winnt/repair/sam: BadBlue server is vulnerable to multiple remote exploits. See http://www.securiteam.com/exploits/5HP0M2A60G.html for more information.

+ OSVDB-721: /..%252f..%252f..%252f..%252f..%252f../winnt/repair/sam._: BadBlue server is vulnerable to multiple remote exploits. See http://www.securiteam.com/exploits/5HP0M2A60G.html for more information.

+ OSVDB-721: /..%255c..%255c..%255c..%255c..%255c../windows/repair/sam: BadBlue server is vulnerable to multiple remote exploits. See http://www.securiteam.com/exploits/5HP0M2A60G.html for more information.

+ OSVDB-721: /..%255c..%255c..%255c..%255c..%255c../winnt/repair/sam: BadBlue server is vulnerable to multiple remote exploits. See http://www.securiteam.com/exploits/5HP0M2A60G.html for more information.

+ OSVDB-721: /..%255c..%255c..%255c..%255c..%255c../winnt/repair/sam._: BadBlue server is vulnerable to multiple remote exploits. See http://www.securiteam.com/exploits/5HP0M2A60G.html for more information.

+ OSVDB-38580: /cgi-bin/c32web.exe/GetImage?ImageName=CustomerEmail.txt%00.pdf : Cart32 contains a null byte directory traversal in the ImageName variable.

- STATUS: Completed 4750 requests (~69% complete, 9.4 minutes left): currently in plugin 'Nikto Tests'

- STATUS: Running average: 100 requests: 0.22429 sec, 10 requests: 0.2250 sec.

+ /cgi-bin/awredir.pl: AWStats redirection file.

+ OSVDB-3092: /.svn/entries: Subversion Entries file may contain directory listing information.

+ /_vti_bin/_vti_adm/admin.exe: FrontPage/Sharepointfile available.

+ /_vti_bin/_vti_aut/author.exe: FrontPage/Sharepointfile available.

+ /server-manager/: Mitel Audio and Web Conferencing server manager identified.

+ /web.txt: This might be interesting...

+ /loleaflet/dist/admin/admin.html: LibreOffice Online Admin interface found (pass protected)

+ /dist/admin/admin.html: LibreOffice Online Admin interface found (pass protected)

+ /wls-wsat/CoordinatorPortType: This application may be vulnerable to http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271.

+ /wls-wsat/RegistrationPortTypeRPC: This application may be vulnerable to http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271.

+ /wls-wsat/ParticipantPortType: This application may be vulnerable to http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271.

+ /wls-wsat/RegistrationRequesterPortType: This application may be vulnerable to http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271.

+ /wls-wsat/CoordinatorPortType11: This application may be vulnerable to http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271.

+ /wls-wsat/RegistrationPortTypeRPC11: This application may be vulnerable to http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271.

+ /wls-wsat/ParticipantPortType11: This application may be vulnerable to http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10271.

+ /master.xml: This might be interesting...

+ /masters.xml: This might be interesting...

+ /connections.xml: This might be interesting...

+ /connection.xml: This might be interesting...

+ /passwords.xml: This might be interesting...

+ /PasswordsData.xml: This might be interesting...

+ /users.xml: This might be interesting...

+ /conndb.xml: This might be interesting...

+ /conn.xml: This might be interesting...

+ /security.xml: This might be interesting...

+ /accounts.xml: This might be interesting...

+ /db.json: This might be interesting...

+ /userdata.json: This might be interesting...

+ /login.json: This might be interesting...

+ /master.json: This might be interesting...

+ /masters.json: This might be interesting...

+ /connections.json: This might be interesting...

+ /connection.json: This might be interesting...

+ /passwords.json: This might be interesting...

+ /PasswordsData.json: This might be interesting...

+ /users.json: This might be interesting...

+ /conndb.json: This might be interesting...

+ /conn.json: This might be interesting...

+ /accounts.json: This might be interesting...

+ /.gitignore: .gitignore file found. It is possible to grasp the directory structure.

+ /.hgignore: .hgignore file found. It is possible to grasp the directory structure.

+ /.env: .env file found. The .env file may contain credentials.

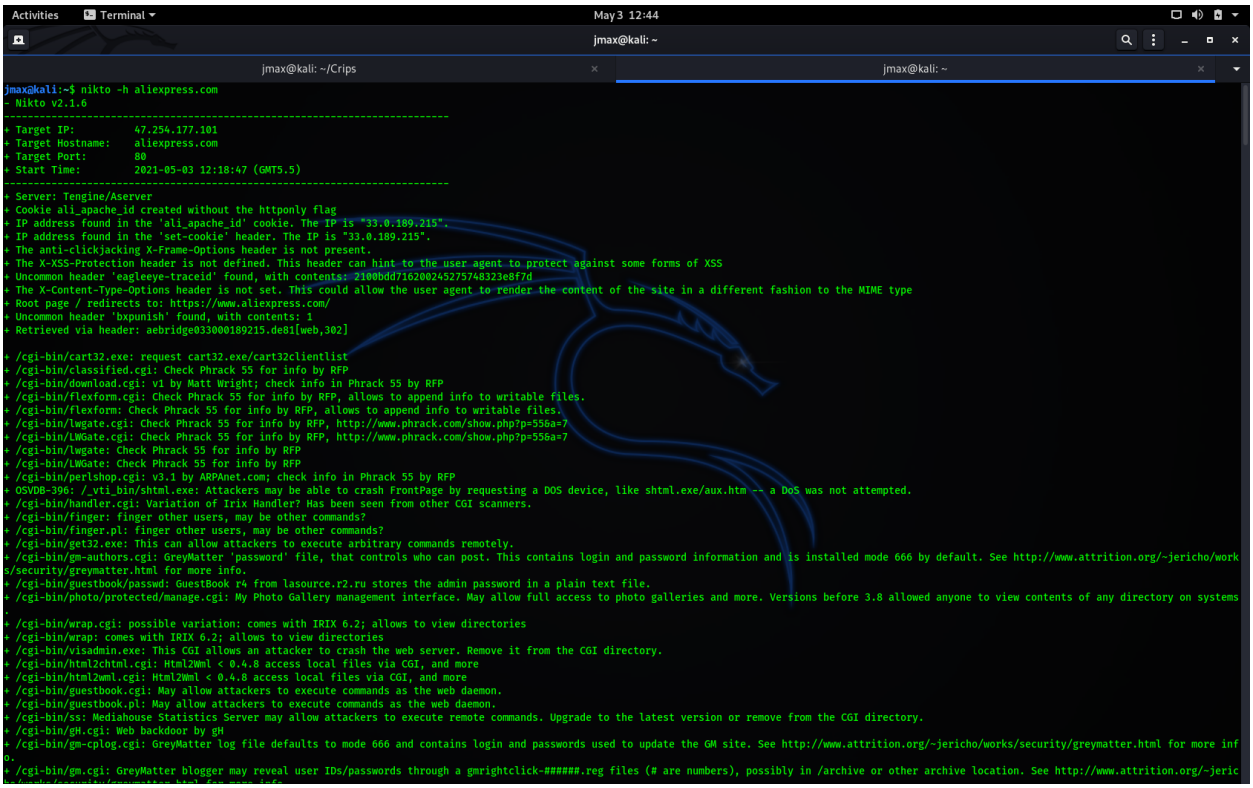
+ 8596 requests: 1 error(s) and 559 item(s) reported on remote host

+ End Time: 2021-05-03 12:55:01 (GMT5.5) (2174 seconds)

+ 1 host(s) tested

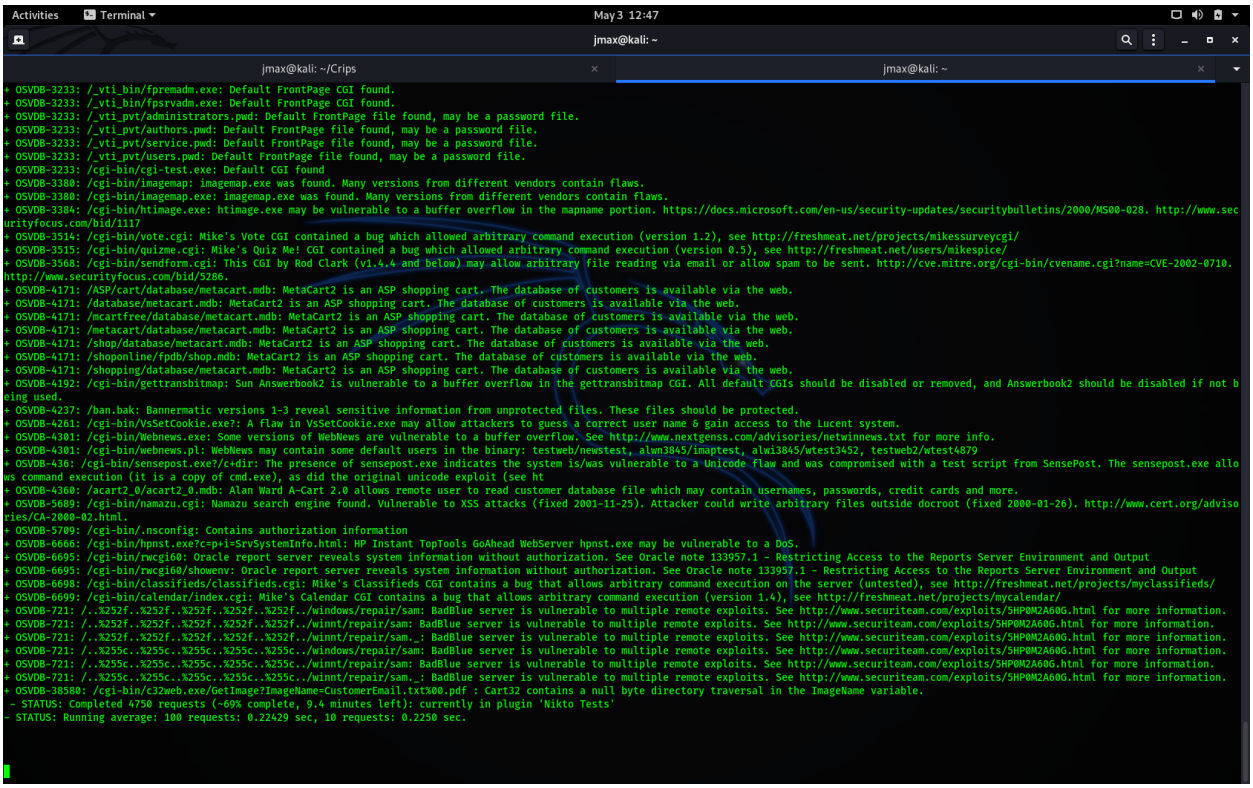
After the scanning I could find some interesting stuffs.

Firstly, I got the IP address of my domain and then I found the server of the domain. Then I could find lots of previously fixed vulnerabilities and existing vulnerabilities as well.



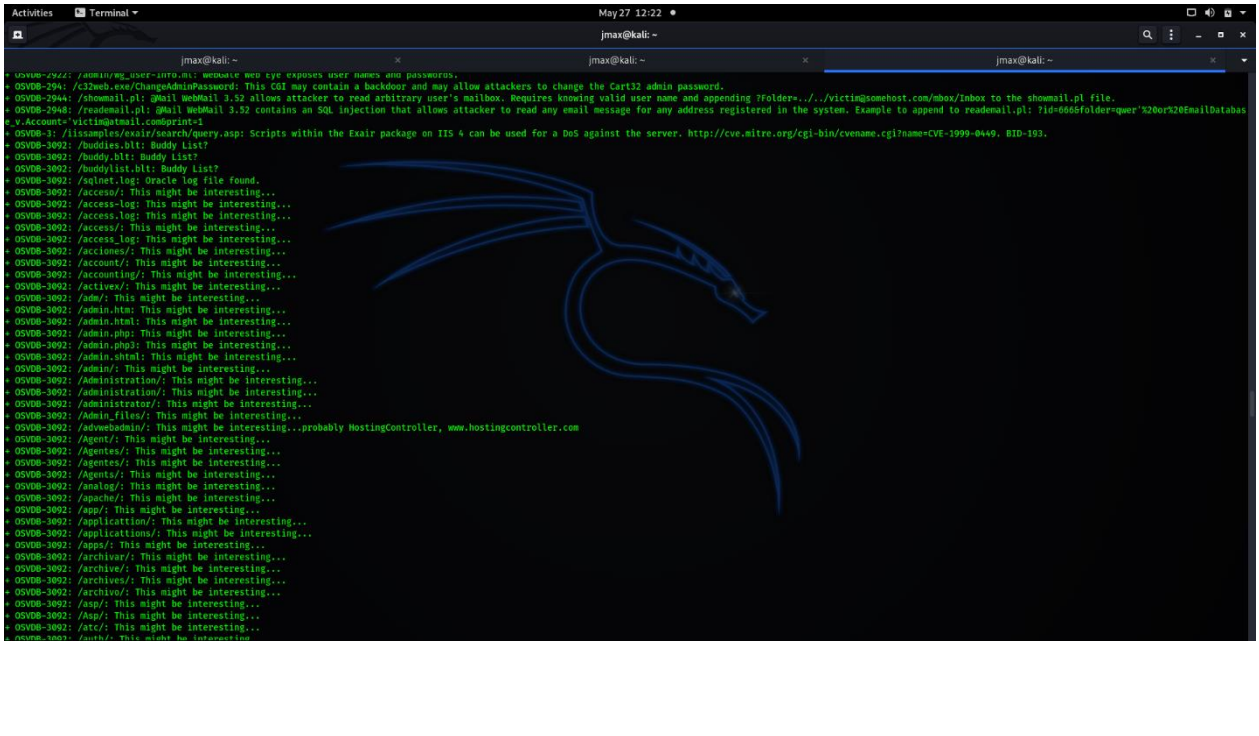
After I could find some hidden directories and files.

During the result, I really excited about below results like password files etc.

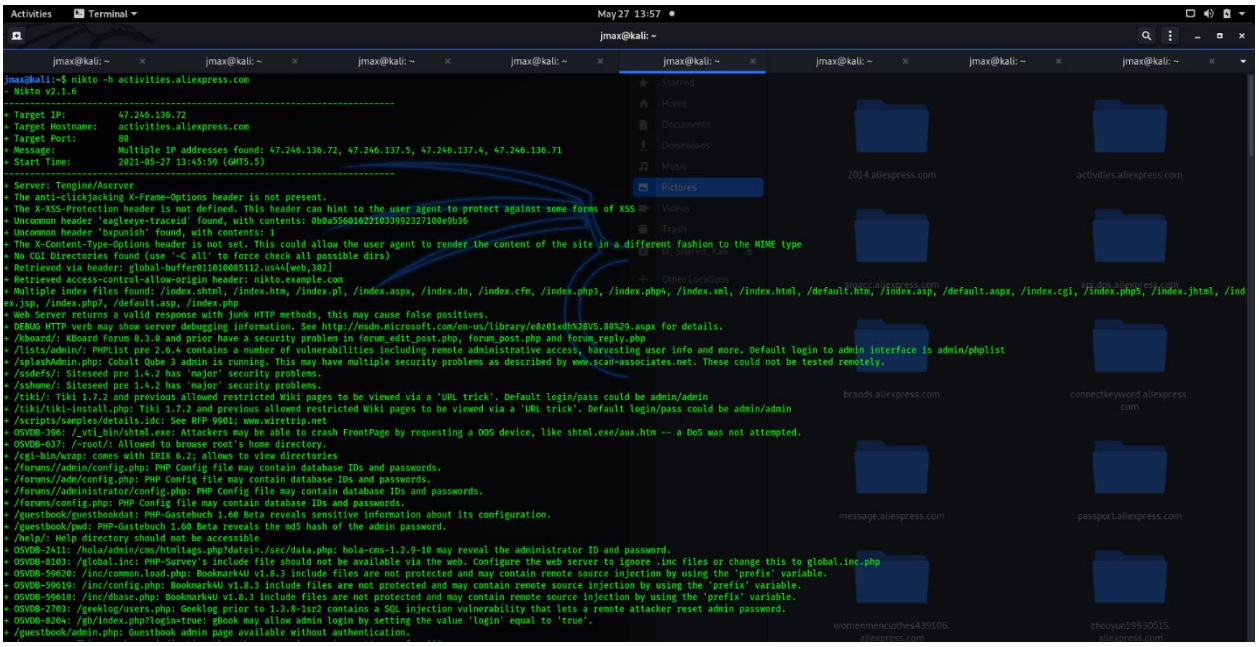


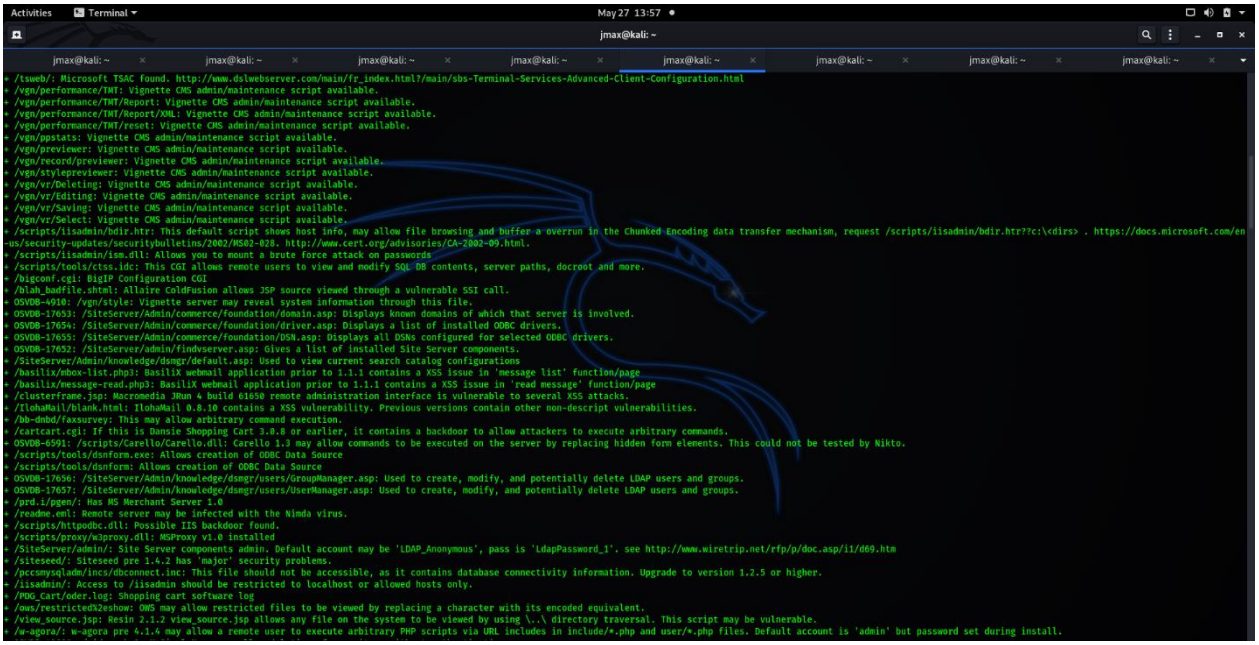
Then I tried to enumerate the vulnerabilities of my target subdomains.

1. **2014.aliexpress.com**

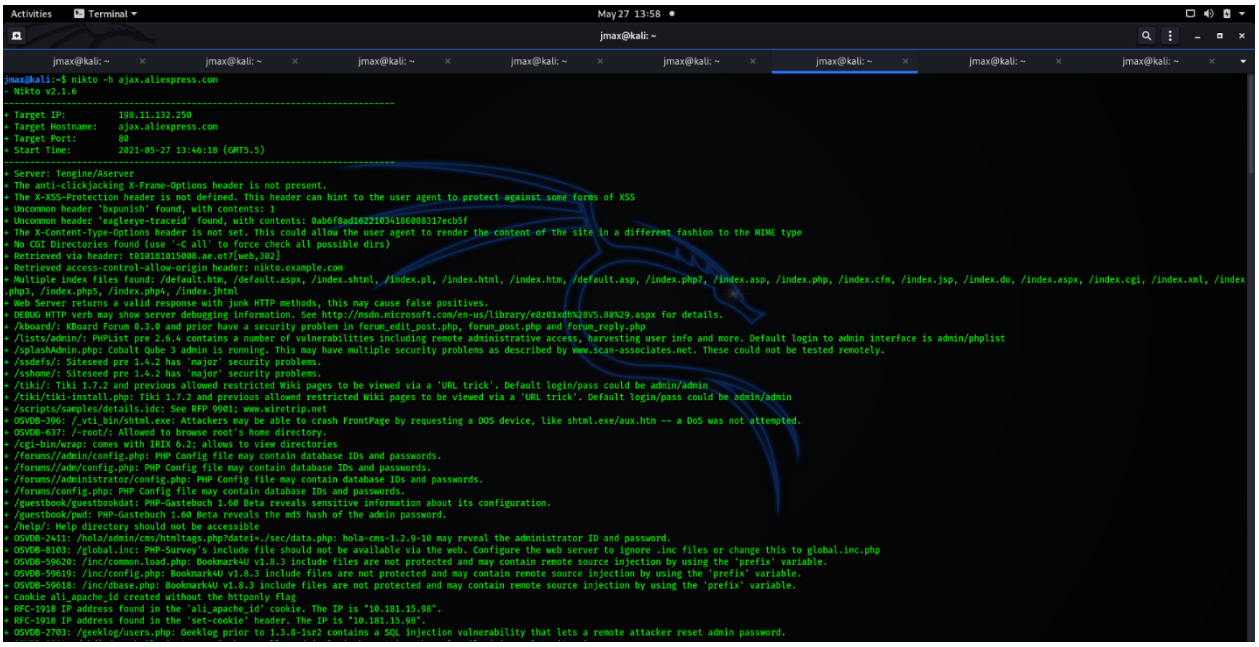


2. activities.aliexpress.com

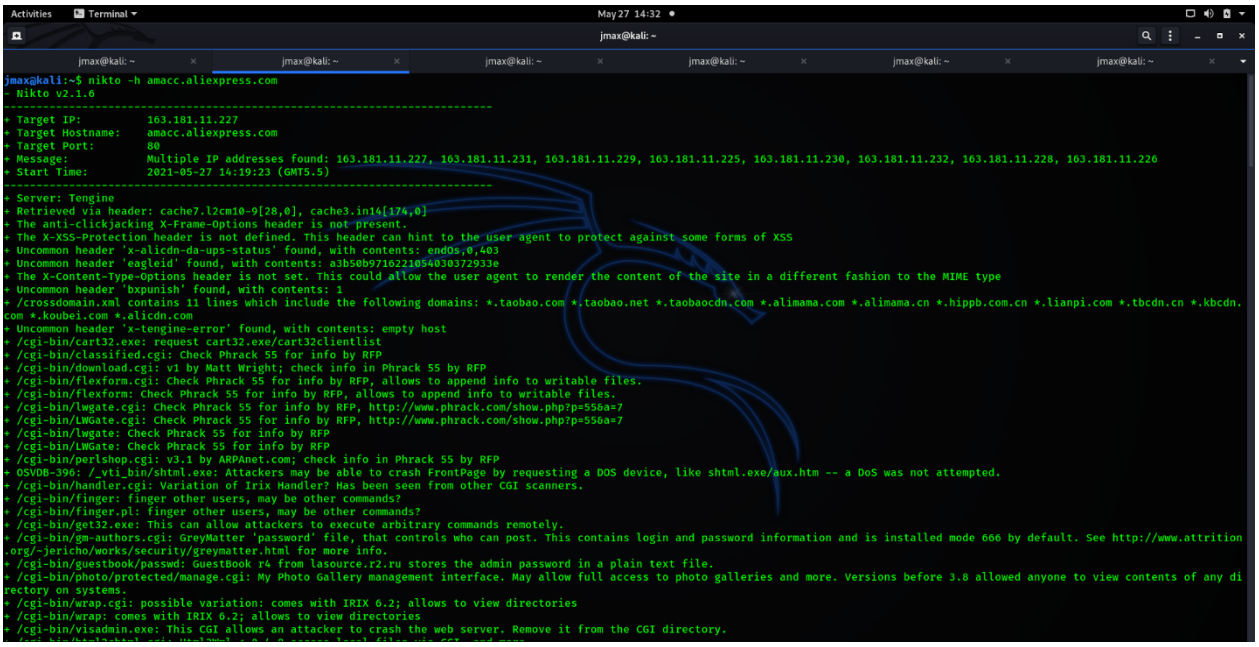


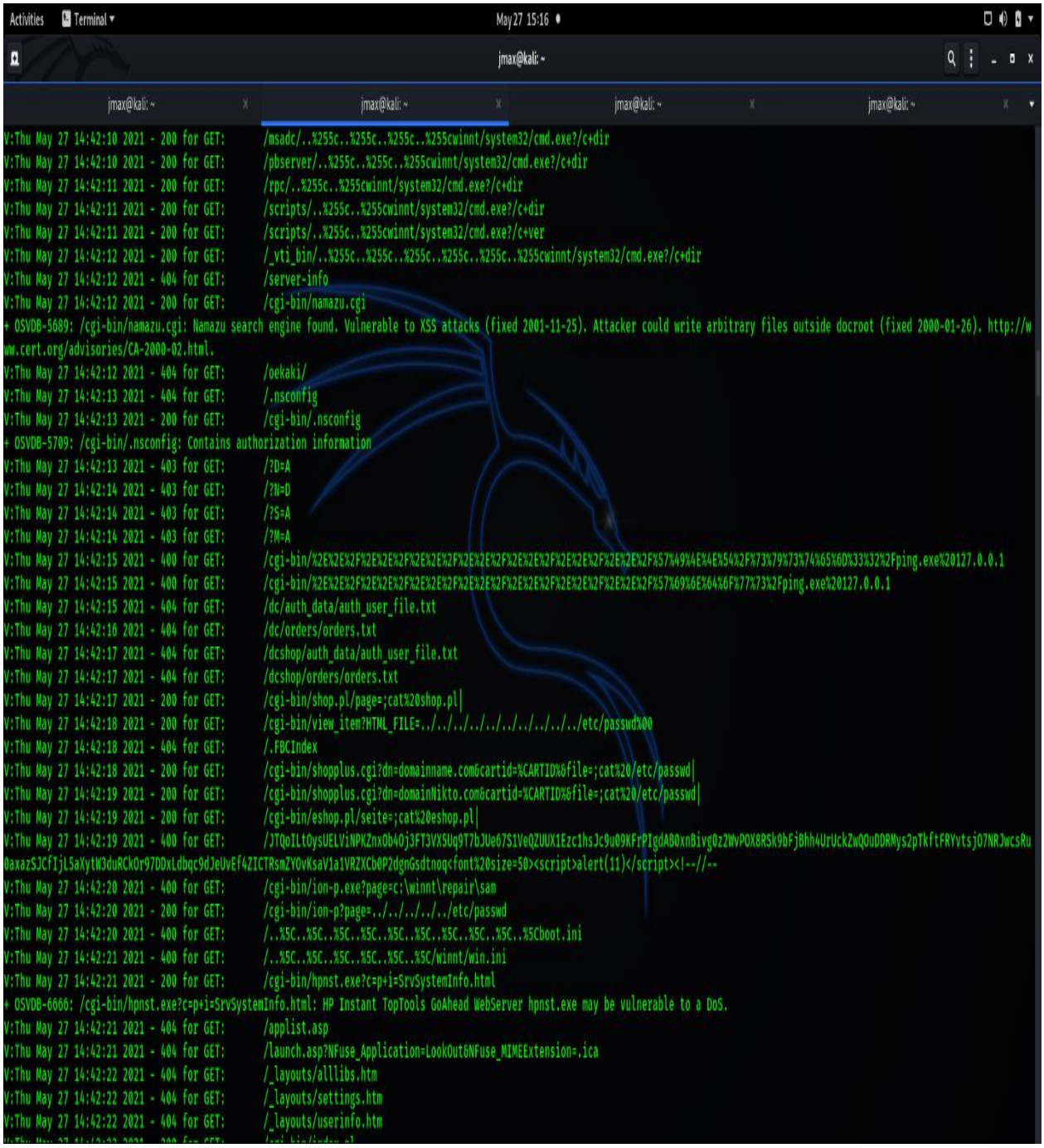


3. ajax.aliexpress.com

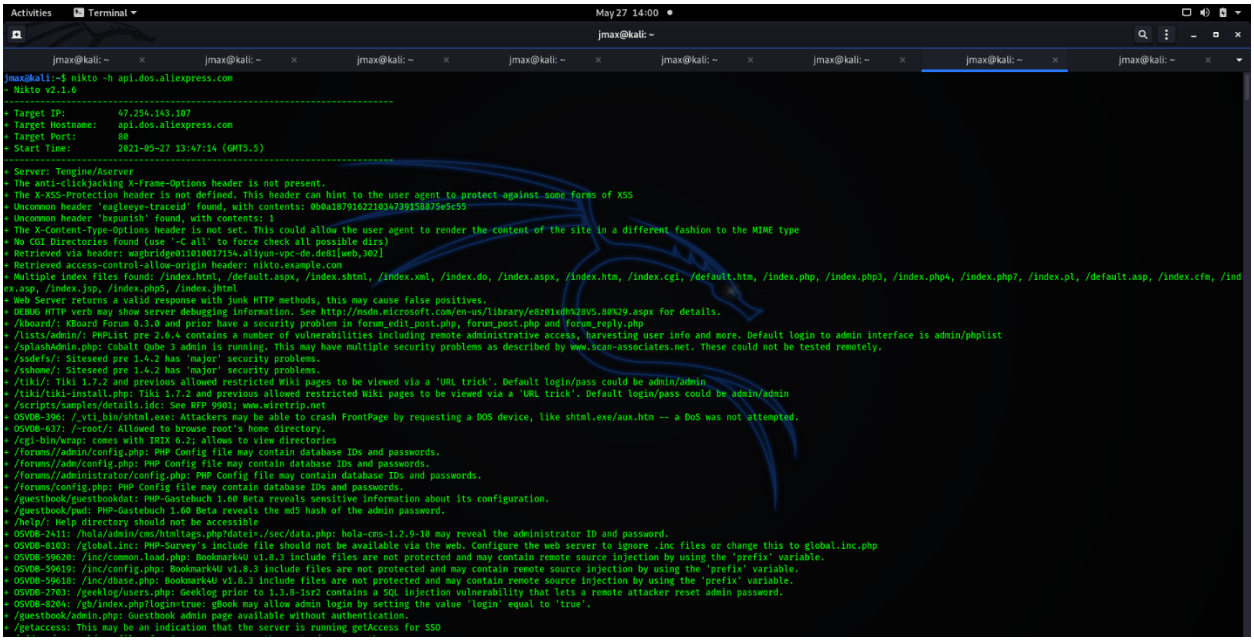


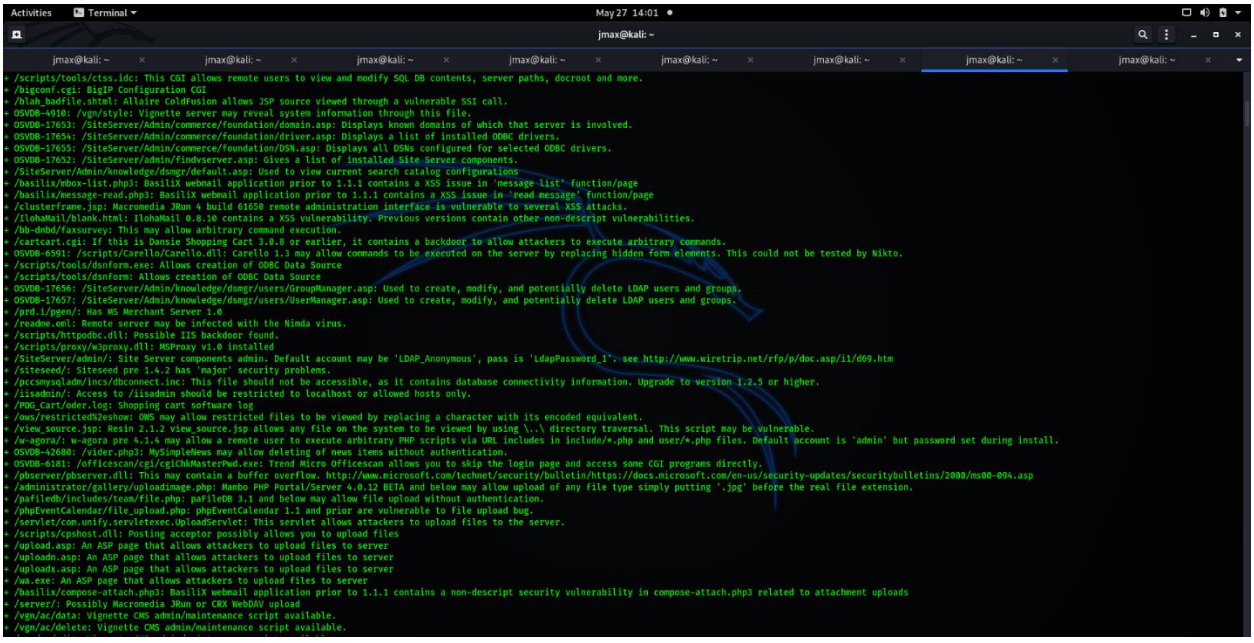
4. amacc.aliexpress.com




Activities
Terminal
May 27 15:16
jmax@kali: ~
jmax@kali: ~
jmax@kali: ~
jmax@kali: ~
jmax@kali: ~
V:Thu May 27 14:42:10 2021 - 200 for GET: /msadc/..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir
V:Thu May 27 14:42:10 2021 - 200 for GET: /pbserver/..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir
V:Thu May 27 14:42:11 2021 - 200 for GET: /rpc/..%255c..%255cwinnt/system32/cmd.exe?/c+dir
V:Thu May 27 14:42:11 2021 - 200 for GET: /scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir
V:Thu May 27 14:42:11 2021 - 200 for GET: /scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+ver
V:Thu May 27 14:42:12 2021 - 200 for GET: /_vti_bin/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir
V:Thu May 27 14:42:12 2021 - 404 for GET: /server-info
V:Thu May 27 14:42:12 2021 - 200 for GET: /cgi-bin/namazu.cgi
+ OSVDB-5689: /cgi-bin/namazu.cgi: Namazu search engine found. Vulnerable to XSS attacks (fixed 2001-11-25). Attacker could write arbitrary files outside docroot (fixed 2000-01-26). http://www.cert.org/advisories/CA-2000-02.html.
V:Thu May 27 14:42:12 2021 - 404 for GET: /oekaki/
V:Thu May 27 14:42:13 2021 - 404 for GET: /.nsconfig
V:Thu May 27 14:42:13 2021 - 200 for GET: /cgi-bin/.nsconfig
+ OSVDB-5709: /cgi-bin/.nsconfig: Contains authorization information
V:Thu May 27 14:42:13 2021 - 403 for GET: /?D=A
V:Thu May 27 14:42:14 2021 - 403 for GET: /?N=D
V:Thu May 27 14:42:14 2021 - 403 for GET: /?S=A
V:Thu May 27 14:42:14 2021 - 403 for GET: /?M=A
V:Thu May 27 14:42:15 2021 - 400 for GET: /cgi-bin/%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%57%49%4E%4E%54%2F%73%79%73%74%65%6D%33%32%2Fping.exe%20127.0.0.1
V:Thu May 27 14:42:15 2021 - 400 for GET: /cgi-bin/%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%2E%2E%2F%57%69%6E%64%6F%77%73%2Fping.exe%20127.0.0.1
V:Thu May 27 14:42:15 2021 - 404 for GET: /dc/auth_data/auth_user_file.txt
V:Thu May 27 14:42:16 2021 - 404 for GET: /dc/orders/orders.txt
V:Thu May 27 14:42:17 2021 - 404 for GET: /dcshop/auth_data/auth_user_file.txt
V:Thu May 27 14:42:17 2021 - 404 for GET: /dcshop/orders/orders.txt
V:Thu May 27 14:42:17 2021 - 200 for GET: /cgi-bin/shop.pl/page=;cat%20shop.pl|
V:Thu May 27 14:42:18 2021 - 200 for GET: /cgi-bin/view_item?HTML_FILE=../../../../../../../../../../etc/passwd%00
V:Thu May 27 14:42:18 2021 - 404 for GET: /.FBCIndex
V:Thu May 27 14:42:18 2021 - 200 for GET: /cgi-bin/shopplus.cgi?dn=domainname.com&cartid=%CARTID%&file=;cat%20/etc/passwd|
V:Thu May 27 14:42:19 2021 - 200 for GET: /cgi-bin/shopplus.cgi?dn=domainNikto.com&cartid=%CARTID%&file=;cat%20/etc/passwd|
V:Thu May 27 14:42:19 2021 - 200 for GET: /cgi-bin/eshop.pl/seite=;cat%20eshop.pl|
V:Thu May 27 14:42:19 2021 - 400 for GET: /JTQoILtOysUELViNPKZnxOb4Oj3FT3VX5Uq9T7bJUe67S1VeQZUUX1Ezc1hsJc9u09KFrPIgdAB0xnBivgOz2WvPOX8RSk9bFjBhh4UrUckZwQOuDDRMys2pTkftFRYvtsjO7NRJwcsRu0axazSJCfIjL5aXytW3duRCkOr97DDxLdbqc9dJeUvEf4ZICTRsmZYOvKsaV1a1VRZXCb0P2dgnGsdtnoq<font%20size=50><script>alert(11)</script><!--//--
V:Thu May 27 14:42:20 2021 - 400 for GET: /cgi-bin/ion-p.exe?page=c:\winnt\repair\sam
V:Thu May 27 14:42:20 2021 - 200 for GET: /cgi-bin/ion-p?page=../../../../../etc/passwd
V:Thu May 27 14:42:20 2021 - 400 for GET: /..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5Cboot.ini
V:Thu May 27 14:42:21 2021 - 400 for GET: /..%5C..%5C..%5C..%5C..%5C..%5C/winnt/win.ini
V:Thu May 27 14:42:21 2021 - 200 for GET: /cgi-bin/hpnst.exe?c=p+i=SrvSystemInfo.html
+ OSVDB-6666: /cgi-bin/hpnst.exe?c=p+i=SrvSystemInfo.html: HP Instant TopTools GoAhead WebServer hpnst.exe may be vulnerable to a DoS.
V:Thu May 27 14:42:21 2021 - 404 for GET: /applist.asp
V:Thu May 27 14:42:21 2021 - 404 for GET: /launch.asp?NFuse_Application=LookOut&NFuse_MIMEExtension=.ica
V:Thu May 27 14:42:22 2021 - 404 for GET: /_layouts/alllibs.htm
V:Thu May 27 14:42:22 2021 - 404 for GET: /_layouts/settings.htm
V:Thu May 27 14:42:22 2021 - 404 for GET: /_layouts/userinfo.htm

5. api.dos.aliexpress.com

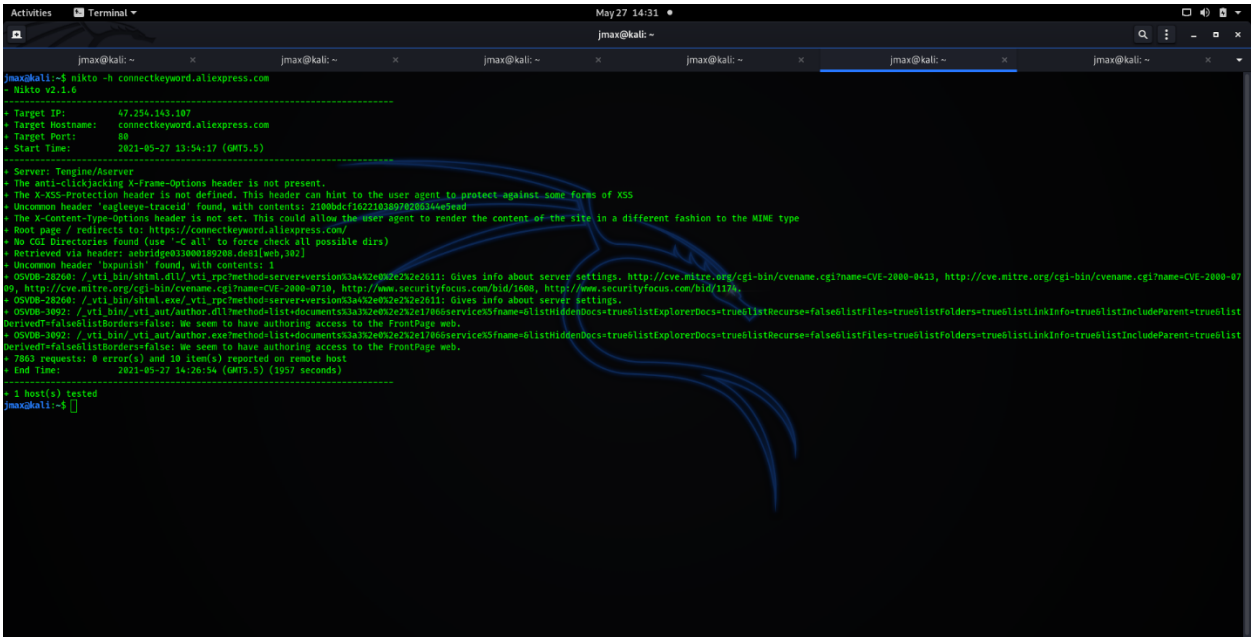




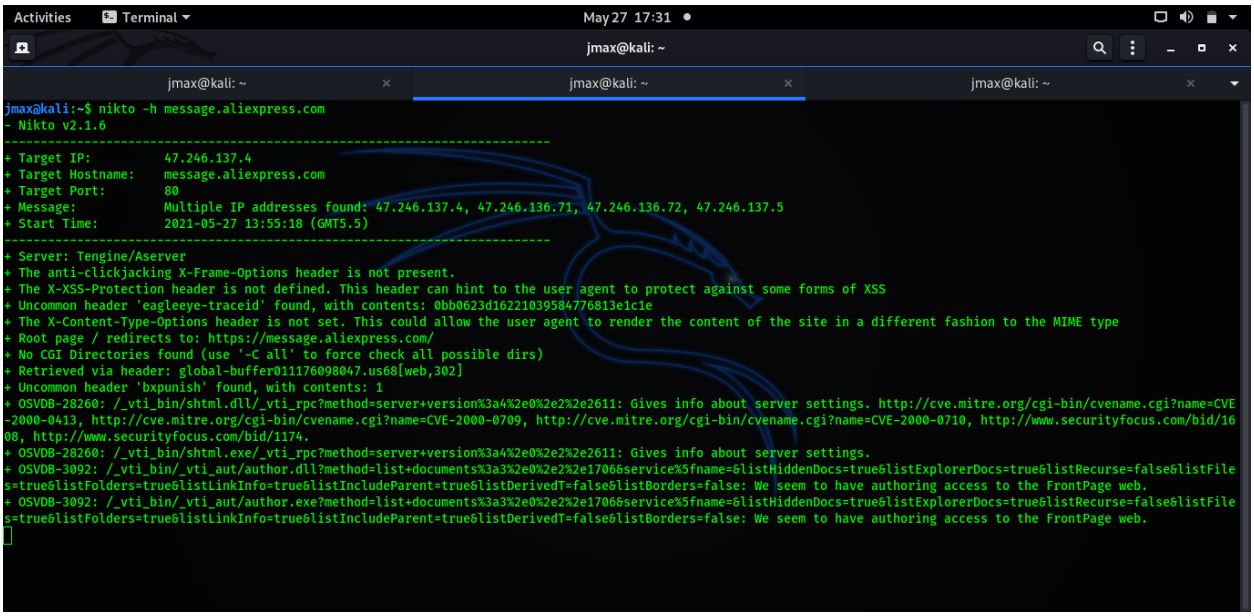
6. best.aliexpress.com

7. brands.aliexpress.com

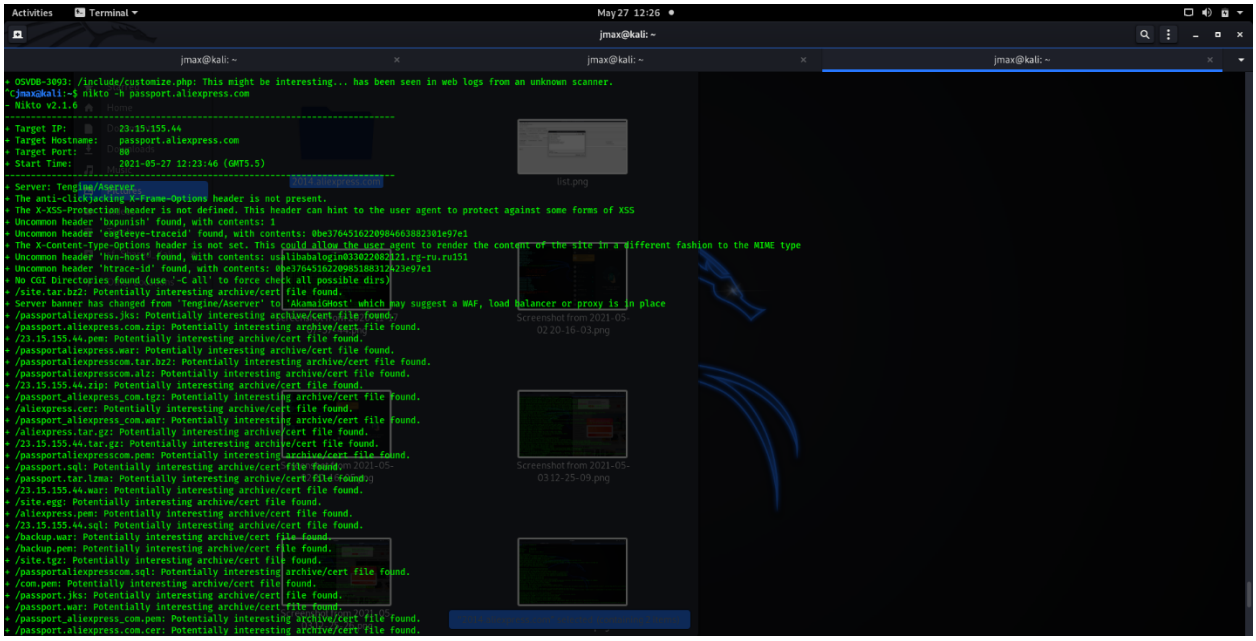
8. connectkeyword.aliexpress.com

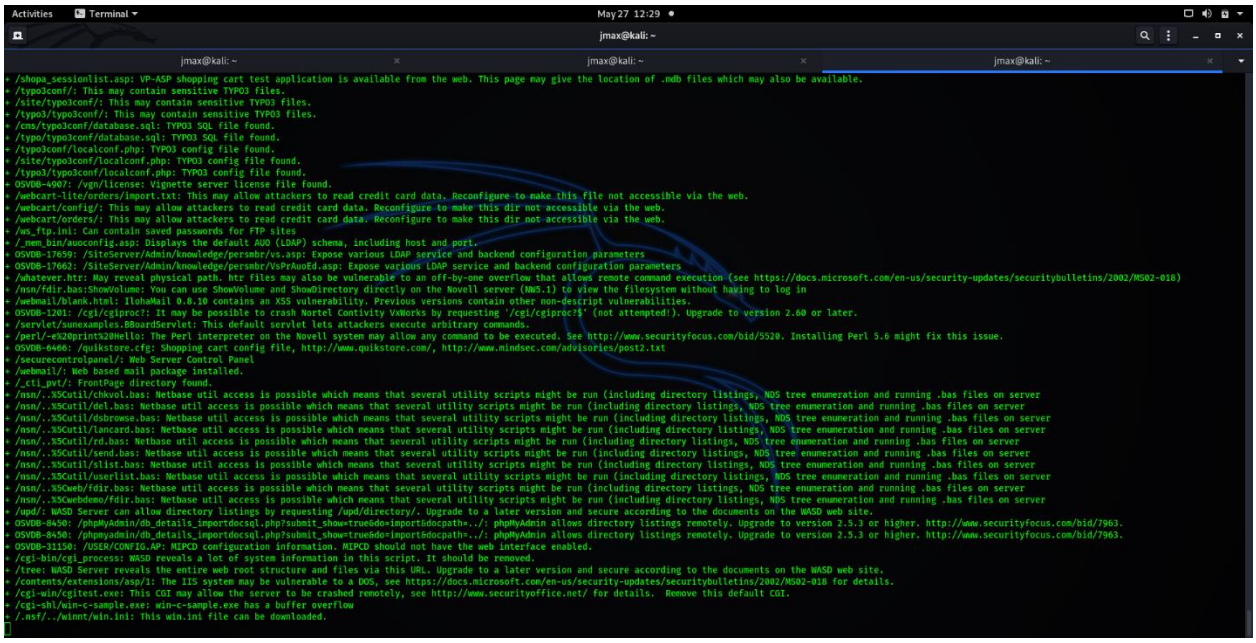


9. message.aliexpress.com

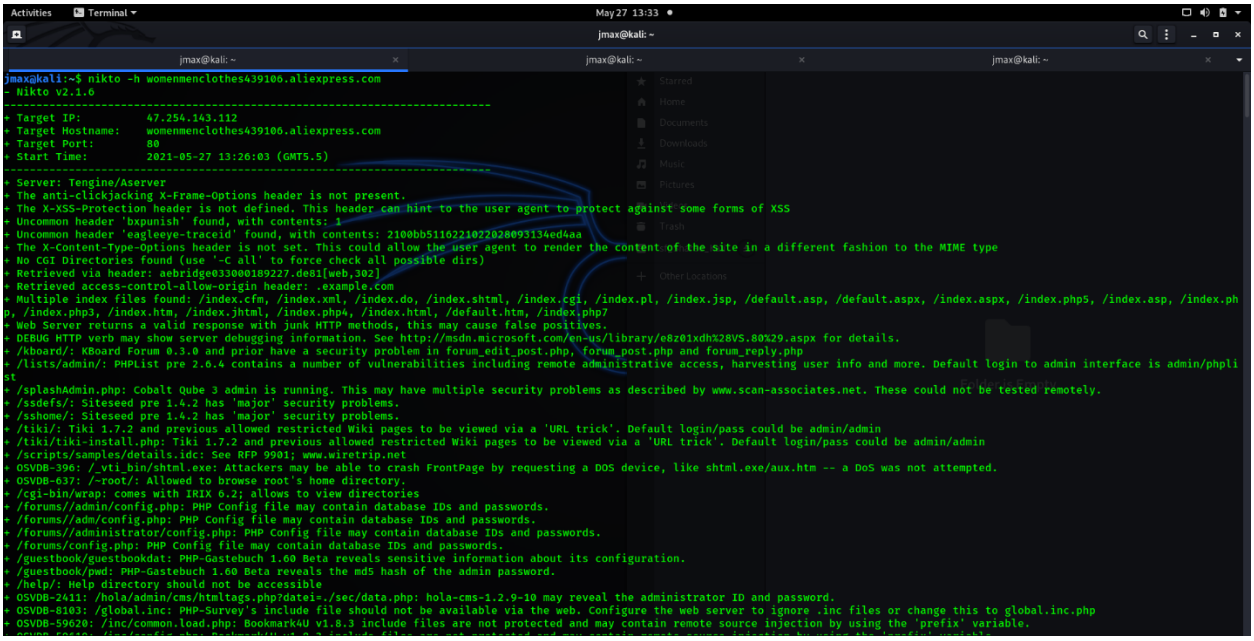


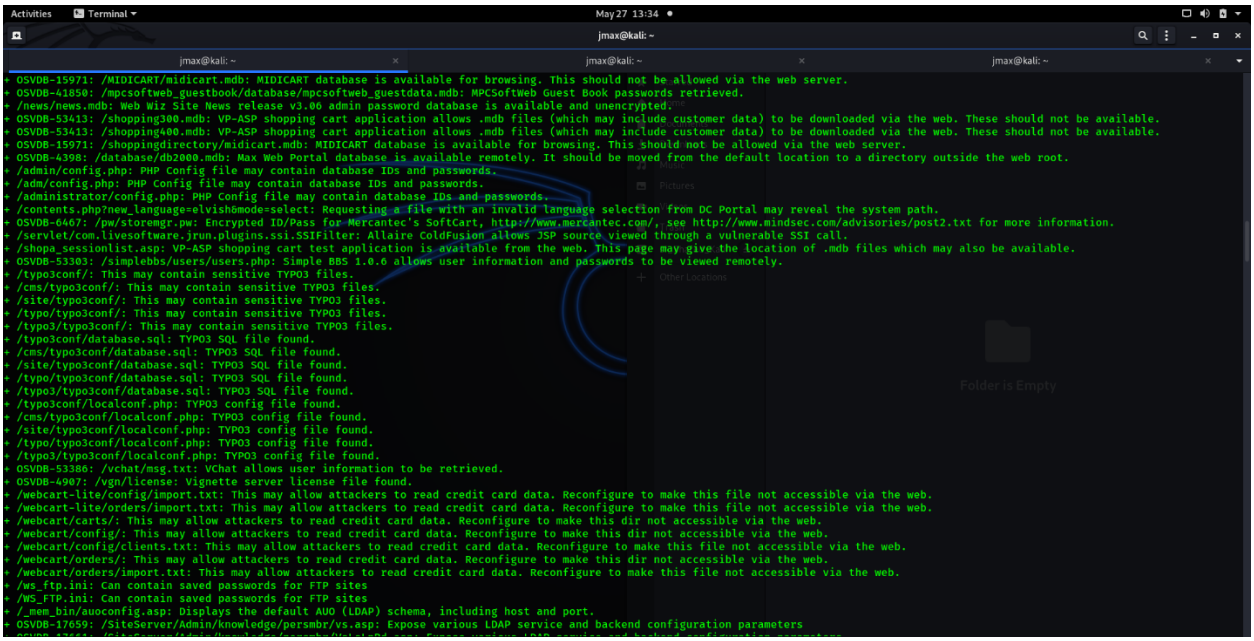
10. passport.aliexpress.com

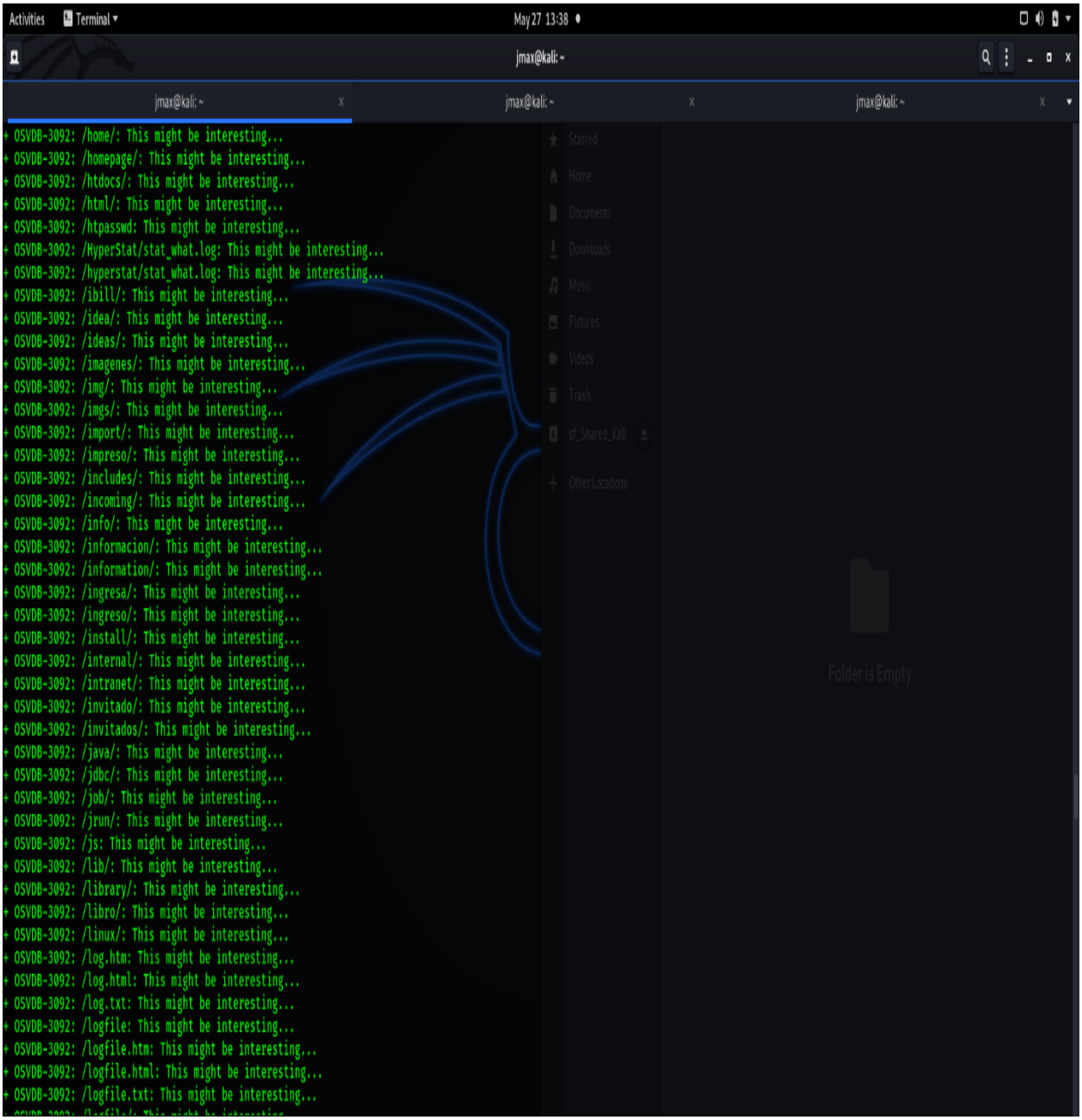




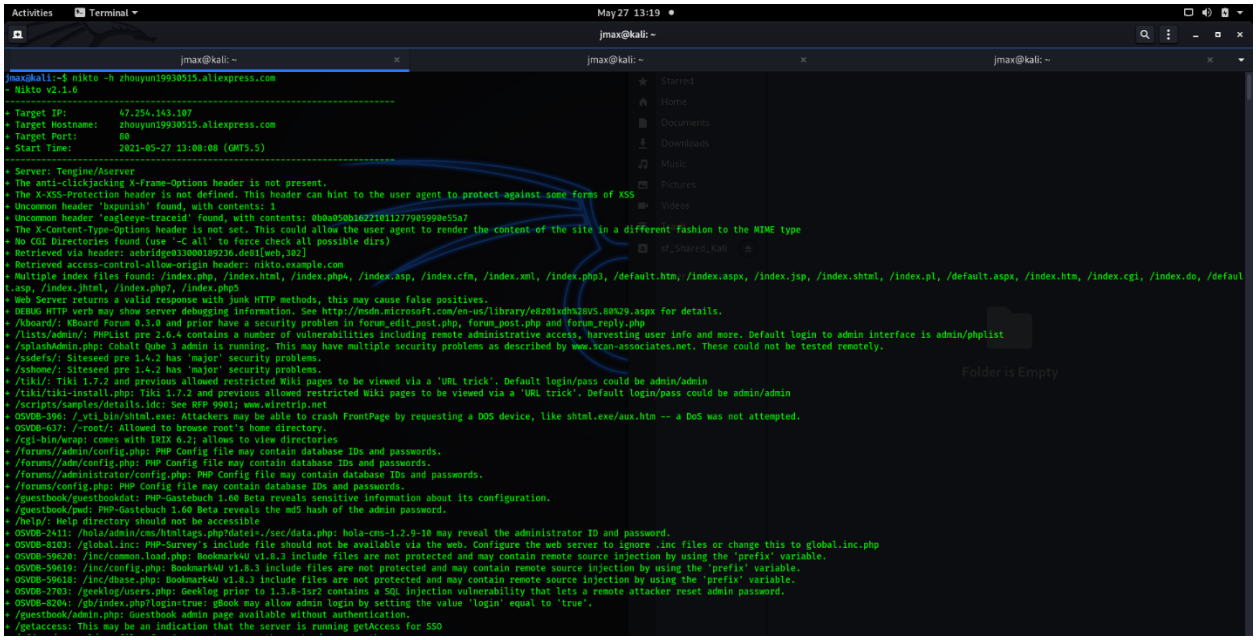
11. womenmenclothes439106.aliexpress.com

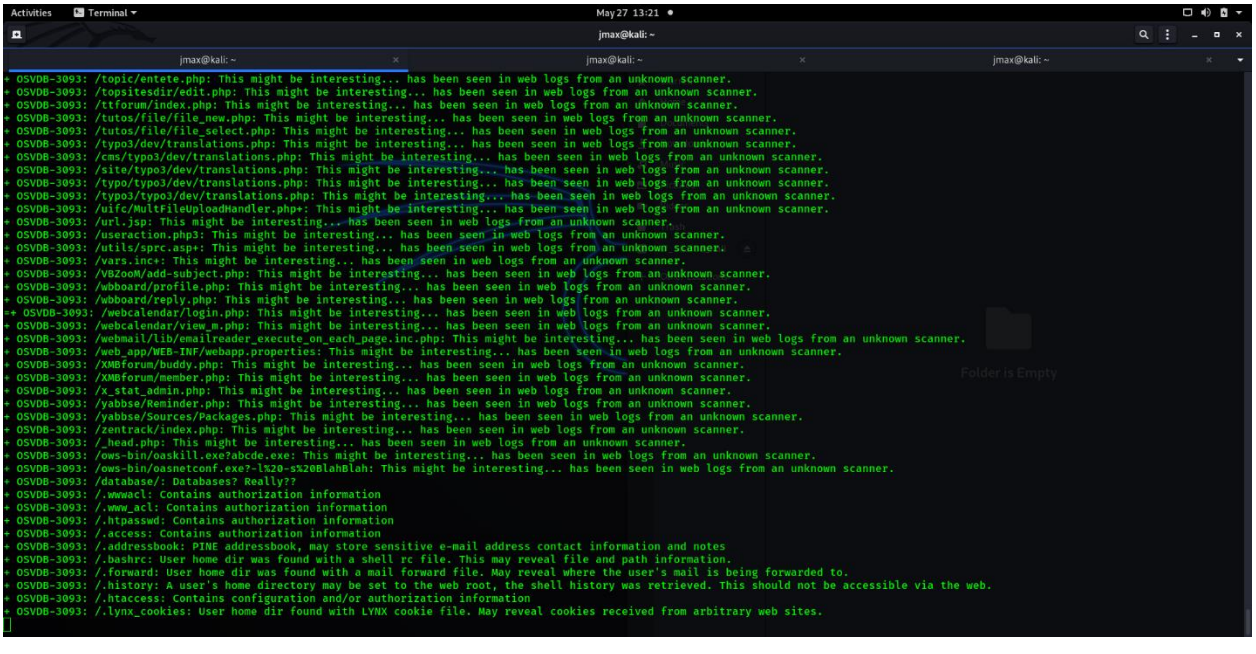





Activities
Terminal
May 27 13:38
jmax@kali: ~
jmax@kali: ~
jmax@kali: ~
jmax@kali: ~
+ OSVDB-3092: /home/: This might be interesting...
+ OSVDB-3092: /homepage/: This might be interesting...
+ OSVDB-3092: /htdocs/: This might be interesting...
+ OSVDB-3092: /html/: This might be interesting...
+ OSVDB-3092: /htpasswd: This might be interesting...
+ OSVDB-3092: /HyperStat/stat_what.log: This might be interesting...
+ OSVDB-3092: /hyperstat/stat_what.log: This might be interesting...
+ OSVDB-3092: /ibill/: This might be interesting...
+ OSVDB-3092: /idea/: This might be interesting...
+ OSVDB-3092: /ideas/: This might be interesting...
+ OSVDB-3092: /imagenes/: This might be interesting...
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3092: /imgs/: This might be interesting...
+ OSVDB-3092: /import/: This might be interesting...
+ OSVDB-3092: /impreso/: This might be interesting...
+ OSVDB-3092: /includes/: This might be interesting...
+ OSVDB-3092: /incoming/: This might be interesting...
+ OSVDB-3092: /info/: This might be interesting...
+ OSVDB-3092: /informacion/: This might be interesting...
+ OSVDB-3092: /information/: This might be interesting...
+ OSVDB-3092: /ingresa/: This might be interesting...
+ OSVDB-3092: /ingreso/: This might be interesting...
+ OSVDB-3092: /install/: This might be interesting...
+ OSVDB-3092: /internal/: This might be interesting...
+ OSVDB-3092: /intranet/: This might be interesting...
+ OSVDB-3092: /invitado/: This might be interesting...
+ OSVDB-3092: /invitados/: This might be interesting...
+ OSVDB-3092: /java/: This might be interesting...
+ OSVDB-3092: /jdbc/: This might be interesting...
+ OSVDB-3092: /job/: This might be interesting...
+ OSVDB-3092: /jrun/: This might be interesting...
+ OSVDB-3092: /js: This might be interesting...
+ OSVDB-3092: /lib/: This might be interesting...
+ OSVDB-3092: /library/: This might be interesting...
+ OSVDB-3092: /libro/: This might be interesting...
+ OSVDB-3092: /linux/: This might be interesting...
+ OSVDB-3092: /log.htm: This might be interesting...
+ OSVDB-3092: /log.html: This might be interesting...
+ OSVDB-3092: /log.txt: This might be interesting...
+ OSVDB-3092: /logfile: This might be interesting...
+ OSVDB-3092: /logfile.htm: This might be interesting...
+ OSVDB-3092: /logfile.html: This might be interesting...
+ OSVDB-3092: /logfile.txt: This might be interesting...
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
sf_Shared_Kali
Other Locations
Folder is Empty

12.zhouyun19930515.aliexpress.com



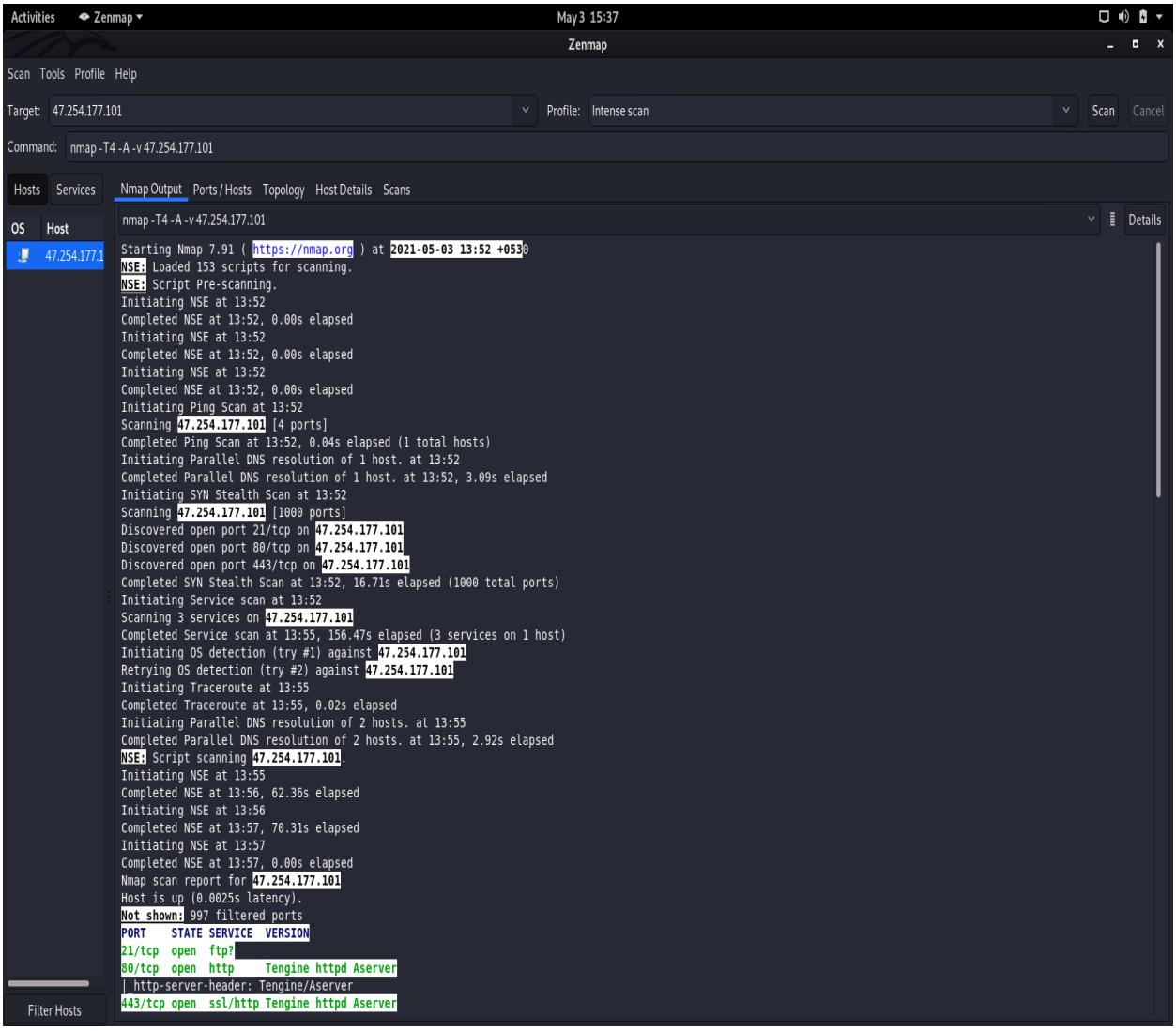


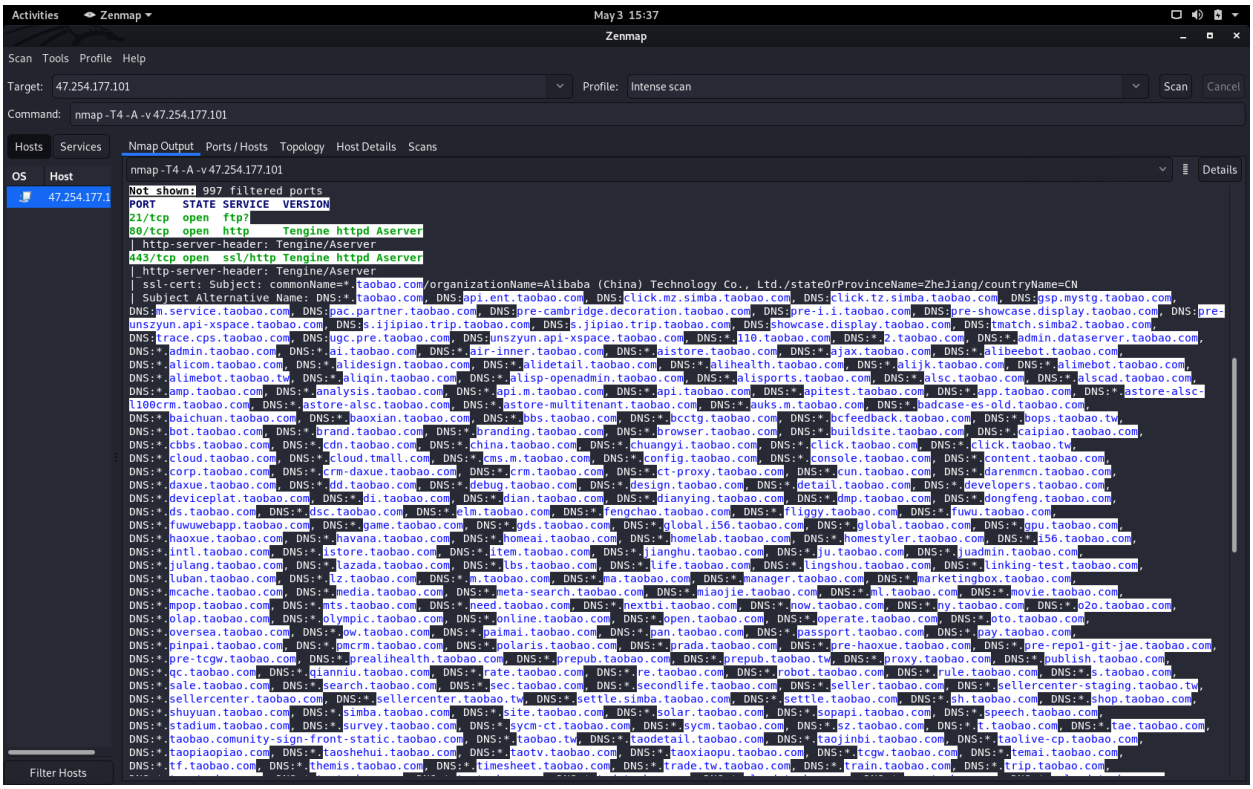
Find open ports and running services

1. Zenmap

Zenmap is the graphical user interface for the Nmap security scanner, and it has hundreds of settings. This scanner can also view Nmap commands. It allows users to save and compare scans, view network topology maps, examine displays of ports running on a host or all hosts on a network, and save scans in a searchable database, among other things.

Following results, I found after scanning the selected domain using Zenmap security scanner.

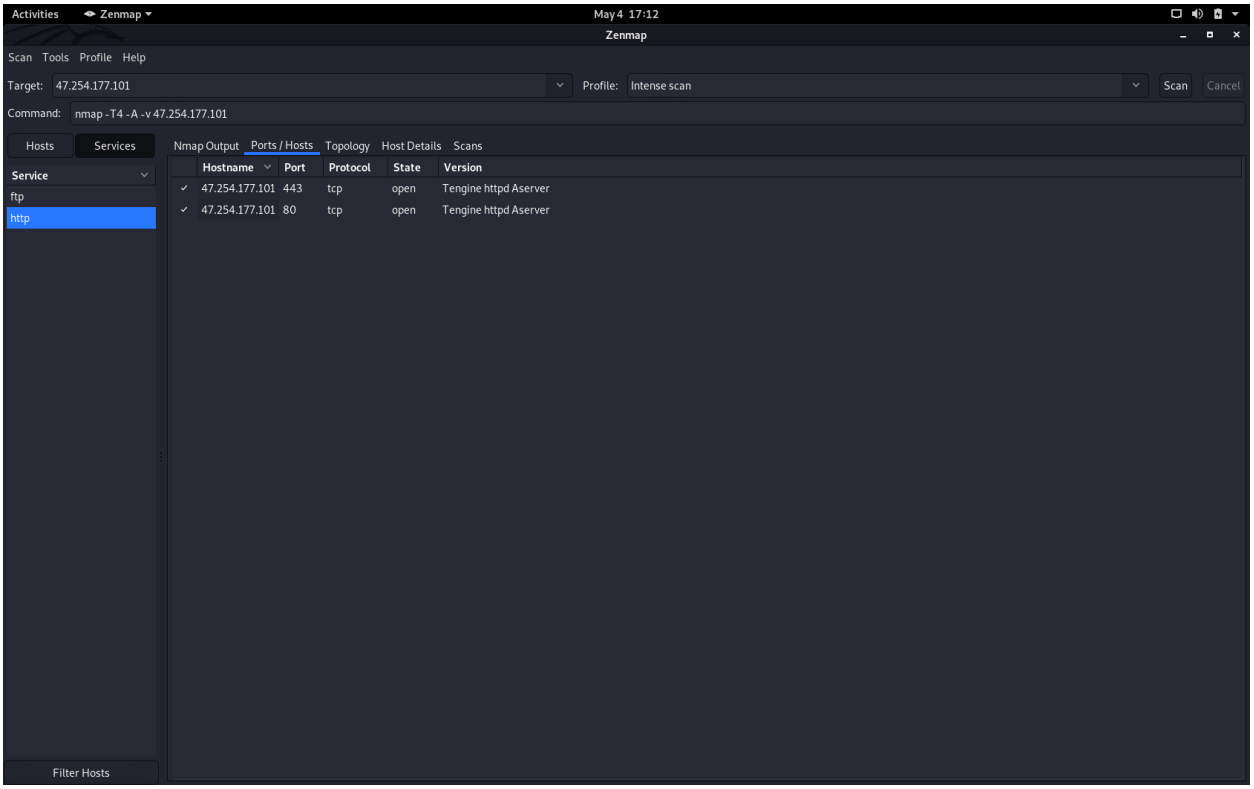


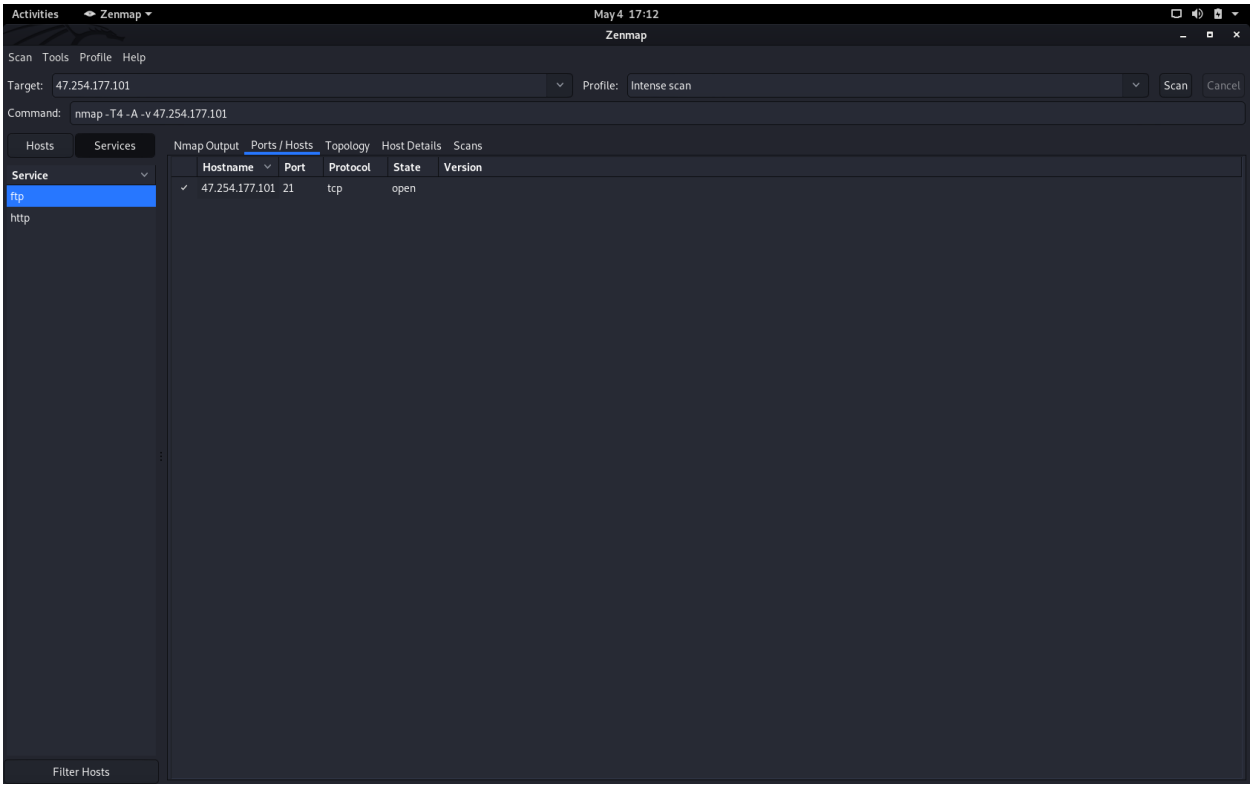

Activities
Zenmap
May 3 15:37
Zenmap
Scan Tools Profile Help
Target: 47.254.177.101
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 47.254.177.101
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
47.254.177.1
nmap -T4 -A -v 47.254.177.101
Details
Not shown: 997 filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp?
80/tcp open http Tengine httpd Aserver
| http-server-header: Tengine/Aserver
443/tcp open ssl/http Tengine httpd Aserver
| http-server-header: Tengine/Aserver
| ssl-cert: Subject: commonName=*.taobao.com/organizationName=Alibaba (China) Technology Co., Ltd./stateOrProvinceName=ZheJiang/countryName=CN
| Subject Alternative Name: DNS:*.taobao.com, DNS:api.ent.taobao.com, DNS:click.mz.simba.taobao.com, DNS:click.tz.simba.taobao.com, DNS:gsp.mystg.taobao.com,
DNS:m.service.taobao.com, DNS:bac.partner.taobao.com, DNS:pre-cambridge.decoration.taobao.com, DNS:pre-i.i.taobao.com, DNS:pre-showcase.display.taobao.com, DNS:pre-
unszyun.api-xspace.taobao.com, DNS:s.ijipiao.trip.taobao.com, DNS:s.jipiao.trip.taobao.com, DNS:showcase.display.taobao.com, DNS:tmatch.simba2.taobao.com,
DNS:trace.cps.taobao.com, DNS:ugc.pre.taobao.com, DNS:unszyun.api-xspace.taobao.com, DNS:*.l10.taobao.com, DNS:*.2.taobao.com, DNS:*.admin.dataserver.taobao.com,
DNS:*.admin.taobao.com, DNS:*.ai.taobao.com, DNS:*.air-inner.taobao.com, DNS:*.aistore.taobao.com, DNS:*.ajax.taobao.com, DNS:*.alibeebot.taobao.com,
DNS:*.alicom.taobao.com, DNS:*.alidesign.taobao.com, DNS:*.alidetail.taobao.com, DNS:*.alihealth.taobao.com, DNS:*.alijk.taobao.com, DNS:*.alimebot.taobao.com,
DNS:*.alimebot.taobao.tw, DNS:*.aliqin.taobao.com, DNS:*.alisp-openadmin.taobao.com, DNS:*.alisports.taobao.com, DNS:*.alsc.taobao.com, DNS:*.alscad.taobao.com,
DNS:*.amp.taobao.com, DNS:*.analysis.taobao.com, DNS:*.api.m.taobao.com, DNS:*.api.taobao.com, DNS:*.apitest.taobao.com, DNS:*.app.taobao.com, DNS:*.astore-alsc-
l100crm.taobao.com, DNS:*.astore-alsc.taobao.com, DNS:*.astore-multitenant.taobao.com, DNS:*.auks.m.taobao.com, DNS:*.badcase-es-old.taobao.com,
DNS:*.baichuan.taobao.com, DNS:*.baoxian.taobao.com, DNS:*.bbs.taobao.com, DNS:*.bcctg.taobao.com, DNS:*.bcfeedback.taobao.com, DNS:*.bops.taobao.tw,
DNS:*.bot.taobao.com, DNS:*.brand.taobao.com, DNS:*.branding.taobao.com, DNS:*.browser.taobao.com, DNS:*.buildsite.taobao.com, DNS:*.caipiao.taobao.com,
DNS:*.cbbs.taobao.com, DNS:*.cdn.taobao.com, DNS:*.china.taobao.com, DNS:*.chuangyi.taobao.com, DNS:*.click.taobao.com, DNS:*.click.taobao.tw,
DNS:*.cloud.taobao.com, DNS:*.cloud.tmall.com, DNS:*.cms.m.taobao.com, DNS:*.config.taobao.com, DNS:*.console.taobao.com, DNS:*.content.taobao.com,
DNS:*.corp.taobao.com, DNS:*.crm-daxue.taobao.com, DNS:*.crm.taobao.com, DNS:*.ct-proxy.taobao.com, DNS:*.cun.taobao.com, DNS:*.darenmcn.taobao.com,
DNS:*.daxue.taobao.com, DNS:*.dd.taobao.com, DNS:*.debug.taobao.com, DNS:*.design.taobao.com, DNS:*.detail.taobao.com, DNS:*.developers.taobao.com,
DNS:*.deviceplat.taobao.com, DNS:*.di.taobao.com, DNS:*.dian.taobao.com, DNS:*.dianying.taobao.com, DNS:*.dmp.taobao.com, DNS:*.dongfeng.taobao.com,
DNS:*.ds.taobao.com, DNS:*.dsc.taobao.com, DNS:*.elm.taobao.com, DNS:*.fengchao.taobao.com, DNS:*.fliggy.taobao.com, DNS:*.fuwu.taobao.com,
DNS:*.fuwuwebapp.taobao.com, DNS:*.game.taobao.com, DNS:*.gds.taobao.com, DNS:*.global.i56.taobao.com, DNS:*.global.taobao.com, DNS:*.gpu.taobao.com,
DNS:*.haoxue.taobao.com, DNS:*.havana.taobao.com, DNS:*.homeai.taobao.com, DNS:*.homelab.taobao.com, DNS:*.homestyler.taobao.com, DNS:*.i56.taobao.com,
DNS:*.intl.taobao.com, DNS:*.istore.taobao.com, DNS:*.item.taobao.com, DNS:*.jianghu.taobao.com, DNS:*.ju.taobao.com, DNS:*.juadmin.taobao.com,
DNS:*.julang.taobao.com, DNS:*.lazada.taobao.com, DNS:*.lbs.taobao.com, DNS:*.life.taobao.com, DNS:*.lingshou.taobao.com, DNS:*.linking-test.taobao.com,
DNS:*.luban.taobao.com, DNS:*.lz.taobao.com, DNS:*.m.taobao.com, DNS:*.ma.taobao.com, DNS:*.manager.taobao.com, DNS:*.marketingbox.taobao.com,
DNS:*.mcache.taobao.com, DNS:*.media.taobao.com, DNS:*.meta-search.taobao.com, DNS:*.miaojie.taobao.com, DNS:*.ml.taobao.com, DNS:*.movie.taobao.com,
DNS:*.mpop.taobao.com, DNS:*.mts.taobao.com, DNS:*.need.taobao.com, DNS:*.nextbi.taobao.com, DNS:*.now.taobao.com, DNS:*.ny.taobao.com, DNS:*.o2o.taobao.com,
DNS:*.olap.taobao.com, DNS:*.olympic.taobao.com, DNS:*.online.taobao.com, DNS:*.open.taobao.com, DNS:*.operate.taobao.com, DNS:*.oto.taobao.com,
DNS:*.oversea.taobao.com, DNS:*.ow.taobao.com, DNS:*.paimai.taobao.com, DNS:*.pan.taobao.com, DNS:*.passport.taobao.com, DNS:*.pay.taobao.com,
DNS:*.pinpai.taobao.com, DNS:*.pmcrm.taobao.com, DNS:*.polaris.taobao.com, DNS:*.prada.taobao.com, DNS:*.pre-haoxue.taobao.com, DNS:*.pre-repo1-git-jae.taobao.com,
DNS:*.pre-tcgw.taobao.com, DNS:*.prealihealth.taobao.com, DNS:*.prepub.taobao.com, DNS:*.prepub.taobao.tw, DNS:*.proxy.taobao.com, DNS:*.publish.taobao.com,
DNS:*.qc.taobao.com, DNS:*.qianniu.taobao.com, DNS:*.rate.taobao.com, DNS:*.re.taobao.com, DNS:*.robot.taobao.com, DNS:*.rule.taobao.com, DNS:*.s.taobao.com,
DNS:*.sale.taobao.com, DNS:*.search.taobao.com, DNS:*.sec.taobao.com, DNS:*.secondlife.taobao.com, DNS:*.seller.taobao.com, DNS:*.sellercenter-staging.taobao.tw,
DNS:*.sellercenter.taobao.com, DNS:*.sellercenter.taobao.tw, DNS:*.settle.simba.taobao.com, DNS:*.settle.taobao.com, DNS:*.sh.taobao.com, DNS:*.shop.taobao.com,
DNS:*.shuyuan.taobao.com, DNS:*.simba.taobao.com, DNS:*.site.taobao.com, DNS:*.solar.taobao.com, DNS:*.sopapi.taobao.com, DNS:*.speech.taobao.com,
DNS:*.stadium.taobao.com, DNS:*.survey.taobao.com, DNS:*.sycm-ct.taobao.com, DNS:*.sycm.taobao.com, DNS:*.sz.taobao.com, DNS:*.t.taobao.com, DNS:*.tae.taobao.com,
DNS:*.taobao.community-sign-front-static.taobao.com, DNS:*.taobao.tw, DNS:*.taodetail.taobao.com, DNS:*.taojinbi.taobao.com, DNS:*.taolive-cp.taobao.com,
DNS:*.taopiaopiao.com, DNS:*.taoshehui.taobao.com, DNS:*.taotv.taobao.com, DNS:*.taoxiaopu.taobao.com, DNS:*.tcgw.taobao.com, DNS:*.temai.taobao.com,
DNS:*.tf.taobao.com, DNS:*.themis.taobao.com, DNS:*.timesheet.taobao.com, DNS:*.trade.tw.taobao.com, DNS:*.train.taobao.com, DNS:*.trip.taobao.com,
Filter Hosts


Activities
Zenmap
May 4 17:11
Zenmap
Scan Tools Profile Help
Target: 47.254.177.101
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 47.254.177.101
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
47.254.177.1
nmap -T4 -A -v 47.254.177.101
Details
DNS:*.taopiaopiao.com, DNS:*.taoshehui.taobao.com, DNS:*.taotv.taobao.com, DNS:*.taoxiaopu.taobao.com, DNS:*.tcgw.taobao.com, DNS:*.temai.taobao.com,
DNS:*.tf.taobao.com, DNS:*.themis.taobao.com, DNS:*.timesheet.taobao.com, DNS:*.trade.tw.taobao.com, DNS:*.train.taobao.com, DNS:*.trip.taobao.com,
DNS:*.try.taobao.com, DNS:*.tv.taobao.com, DNS:*.tw.taobao.com, DNS:*.txd.taobao.com, DNS:*.uland.taobao.com, DNS:*.ump.taobao.com, DNS:*.upload.taobao.com,
DNS:*.ut.taobao.com, DNS:*.uz.taobao.com, DNS:*.video.taobao.com, DNS:*.vip.taobao.com, DNS:*.virtualbuy.taobao.com, DNS:*.wangpu.taobao.com,
DNS:*.wangwang.taobao.com, DNS:*.wangxin.taobao.com, DNS:*.wapa.taobao.com, DNS:*.wapa.taobao.tw, DNS:*.waptest.taobao.com, DNS:*.we.taobao.com,
DNS:*.webappp.taobao.com, DNS:*.work.taobao.com, DNS:*.world.taobao.com, DNS:*.wow-share.taobao.com, DNS:*.ws-nextbi.taobao.com, DNS:*.wuliu.taobao.com,
DNS:*.ww.taobao.com, DNS:*.x-space.taobao.com, DNS:*.xconsultant-gateway.taobao.com, DNS:*.xiami.com, DNS:*.xiangqing.taobao.com, DNS:*.xue.taobao.com,
DNS:*.yingxiao.taobao.com, DNS:*.youku.taobao.com, DNS:*.yueke.taobao.com, DNS:*.yulebao.taobao.com, DNS:*.yun.taobao.com, DNS:*.yunos-tv.taobao.com,
DNS:*.zb.taobao.com, DNS:*.zuanshi.taobao.com, DNS:taopiaopiao.com, DNS:xiami.com, DNS:taobao.com
| Issuer: commonName=GlobalSign Organization Validation CA - SHA256 - G2/organizationName=GlobalSign nv-sa/countryName=BE
| Public Key type: ec
| Public Key bits: 256
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-07-06T06:52:02
| Not valid after: 2021-07-05T07:46:19
| MD5: 2404 f4ae b464 f843 850c 9ee1 f1da e4e0
| SHA-1: 53ea 3472 a057 59d9 dc0f a5d4 4d37 99ff 89c4 68bf
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=17 (Good luck!)
IP ID Sequence Generation: Incremental

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 2.99 ms 10.0.2.2
2 3.04 ms 47.254.177.101

NSE: Script Post-scanning.
Initiating NSE at 14:37
Completed NSE at 14:37, 0.00s elapsed
Initiating NSE at 14:37
Completed NSE at 14:37, 0.00s elapsed
Initiating NSE at 14:37
Completed NSE at 14:37, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 377.65 seconds
Raw packets sent: 3076 (139.896KB) | Rcvd: 178 (20.048KB)
Filter Hosts

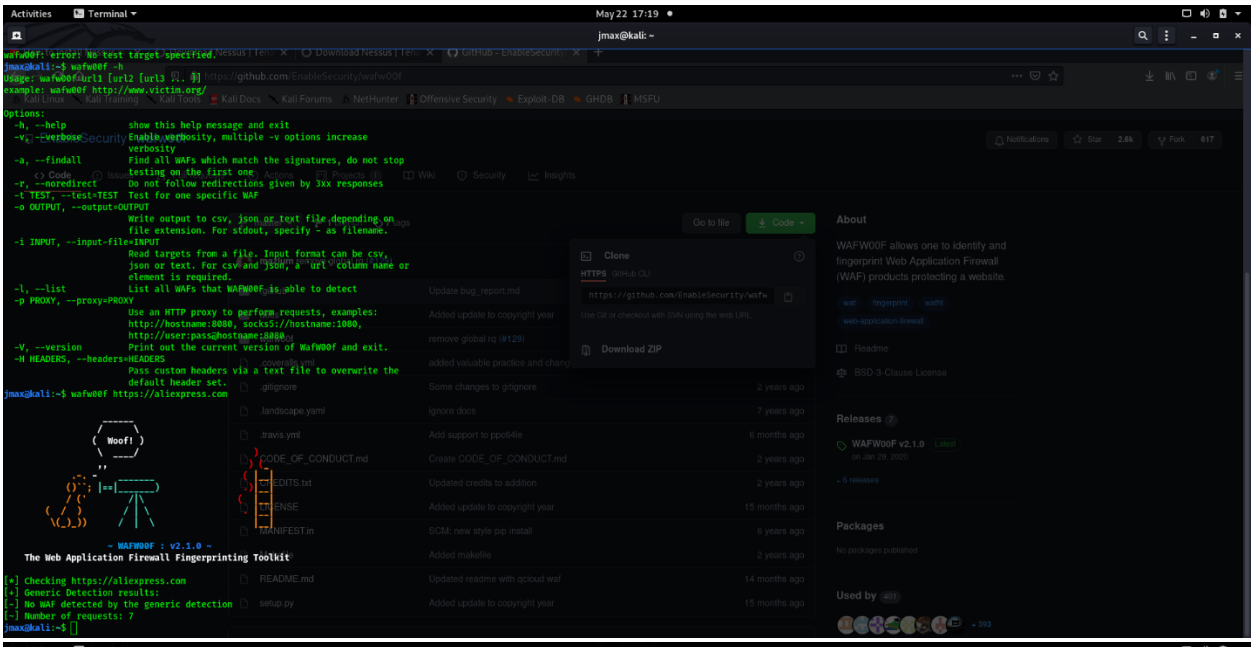

Activities
Zenmap
May 4 17:12
Zenmap
Scan Tools Profile Help
Target: 47.254.177.101
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 47.254.177.101
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Service
ftp
http
Hostname
Port
Protocol
State
Version
47.254.177.101 443 tcp open Tengine httpd Aserver
47.254.177.101 80 tcp open Tengine httpd Aserver
Filter Hosts

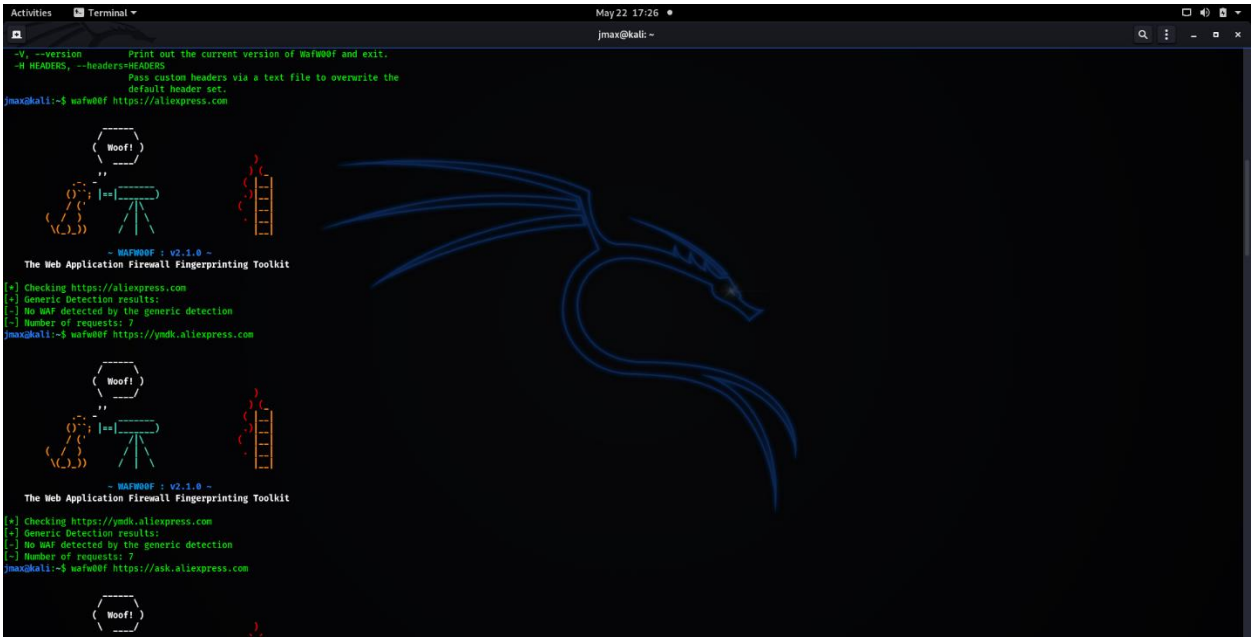

Activities
Zenmap
May 4 17:12
Zenmap
Scan Tools Profile Help
Target: 47.254.177.101
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 47.254.177.101
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Service
ftp
http
Hostname
Port
Protocol
State
Version
47.254.177.101 21 tcp open
Filter Hosts

Discovering target domain firewall protection

1. Wafw00f

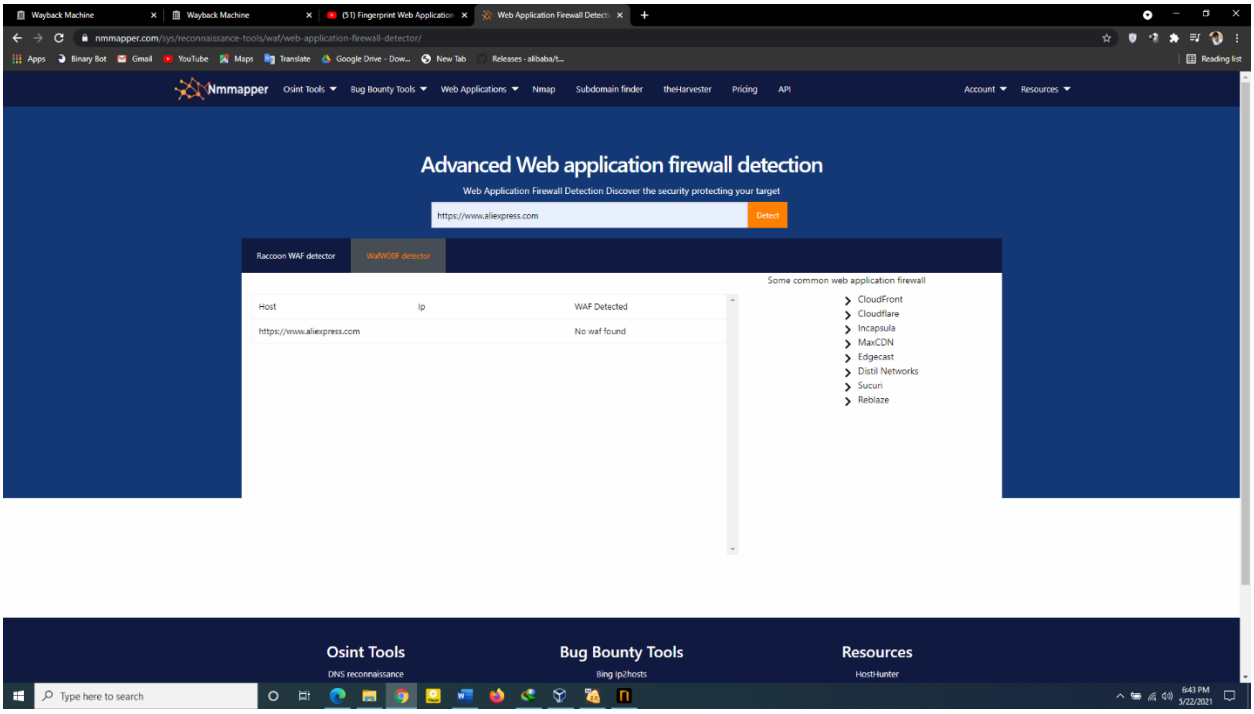
WAFW00F is a Python utility that aids in the fingerprinting and identification of Web Application Firewall (WAF) solutions. It is an active reconnaissance tool in the sense that it connects to the web server, but it begins with a standard HTTP response and escalates as needed.

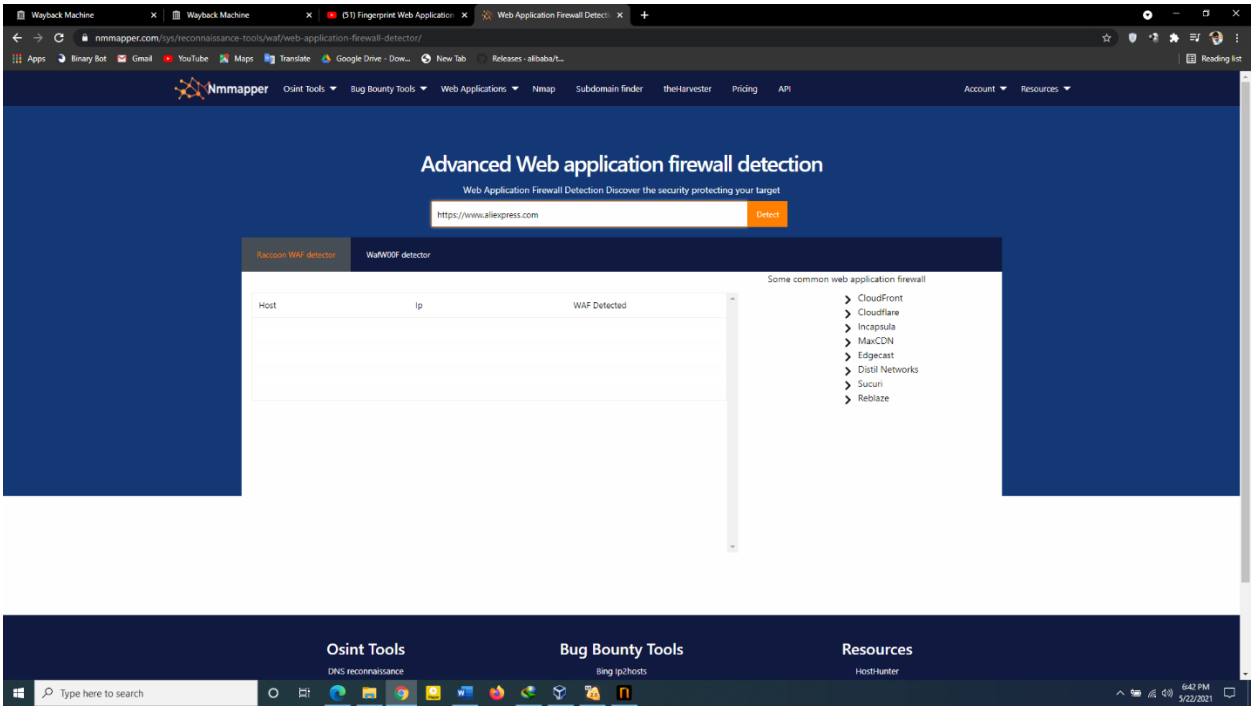




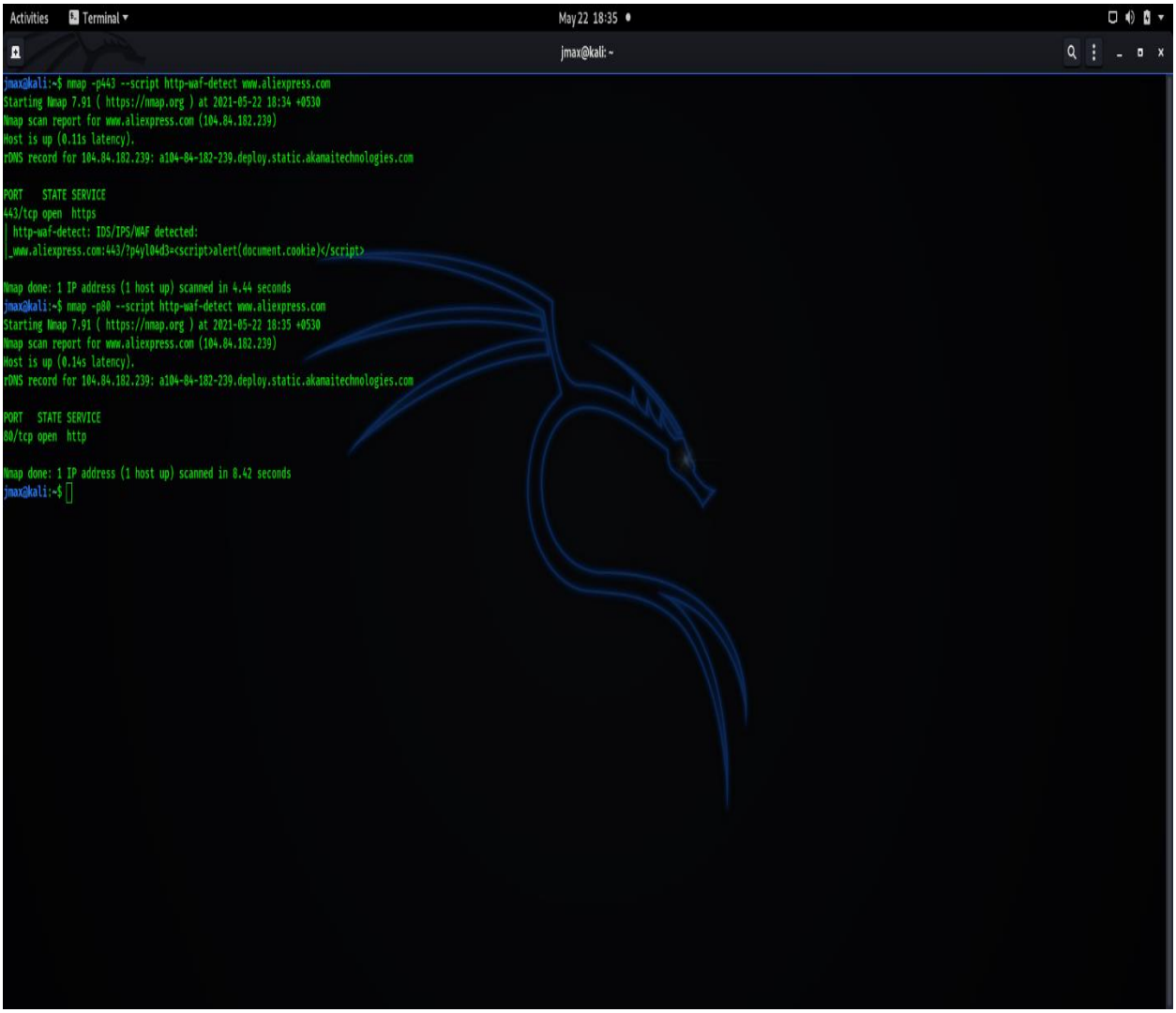
2. Nmap

After scanning using wafw00f tool, I need to confirm whether firewall protection there or not. Then I use Nmap tool and Nmmapper Website for detect the firewall protection that selected targeted domain.





Finally, I could see detected firewall protection details in Nmap tool.

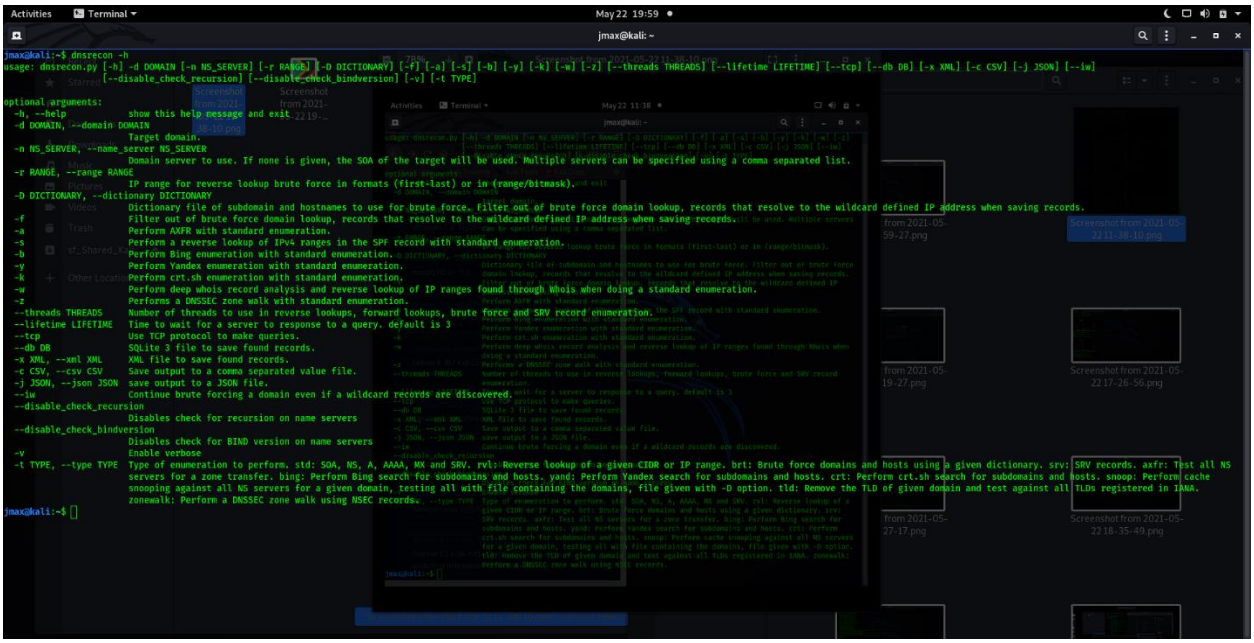


DNS enumeration

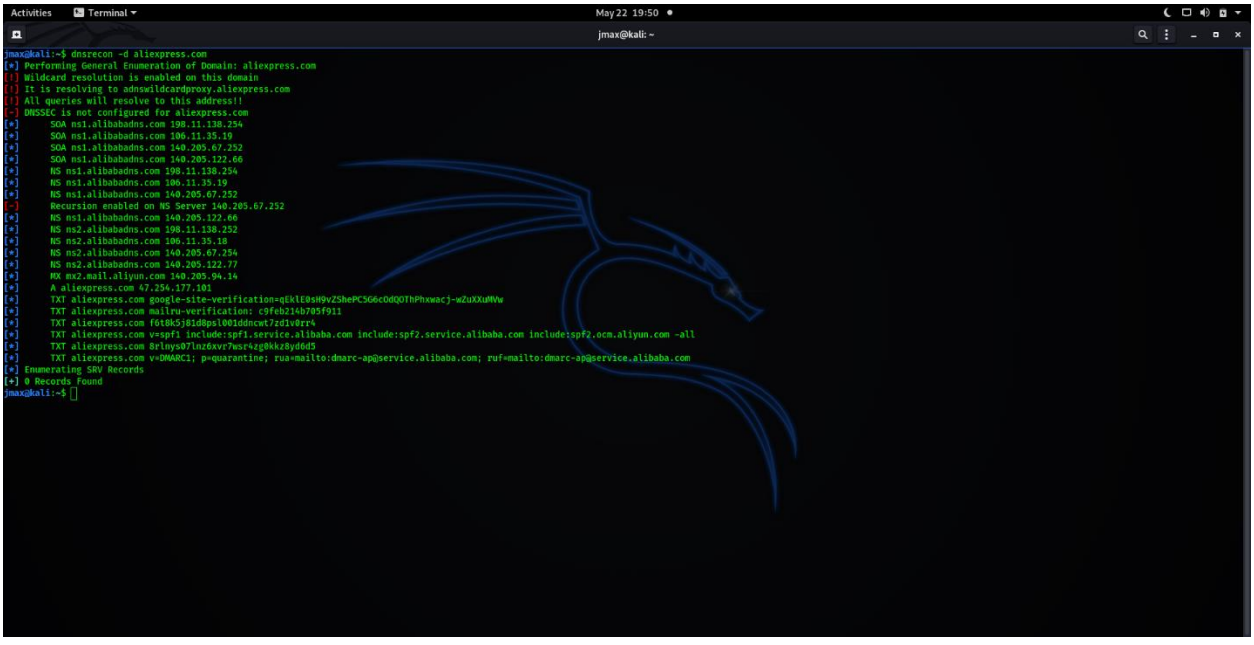
1. Dnsrecon

DNSRecon is a python tool that gathers DNS information. DNSRecon is a DNS reconnaissance tool that can execute a wide range of enumerations, including conventional record enumeration, Zone transfer, Reverse lookup, Google lookup, Zone wandering, cache snooping, and Domain Brute-Forcing.

This is it's behavior using help command.



After scanning I could enumerate following Domain name services.



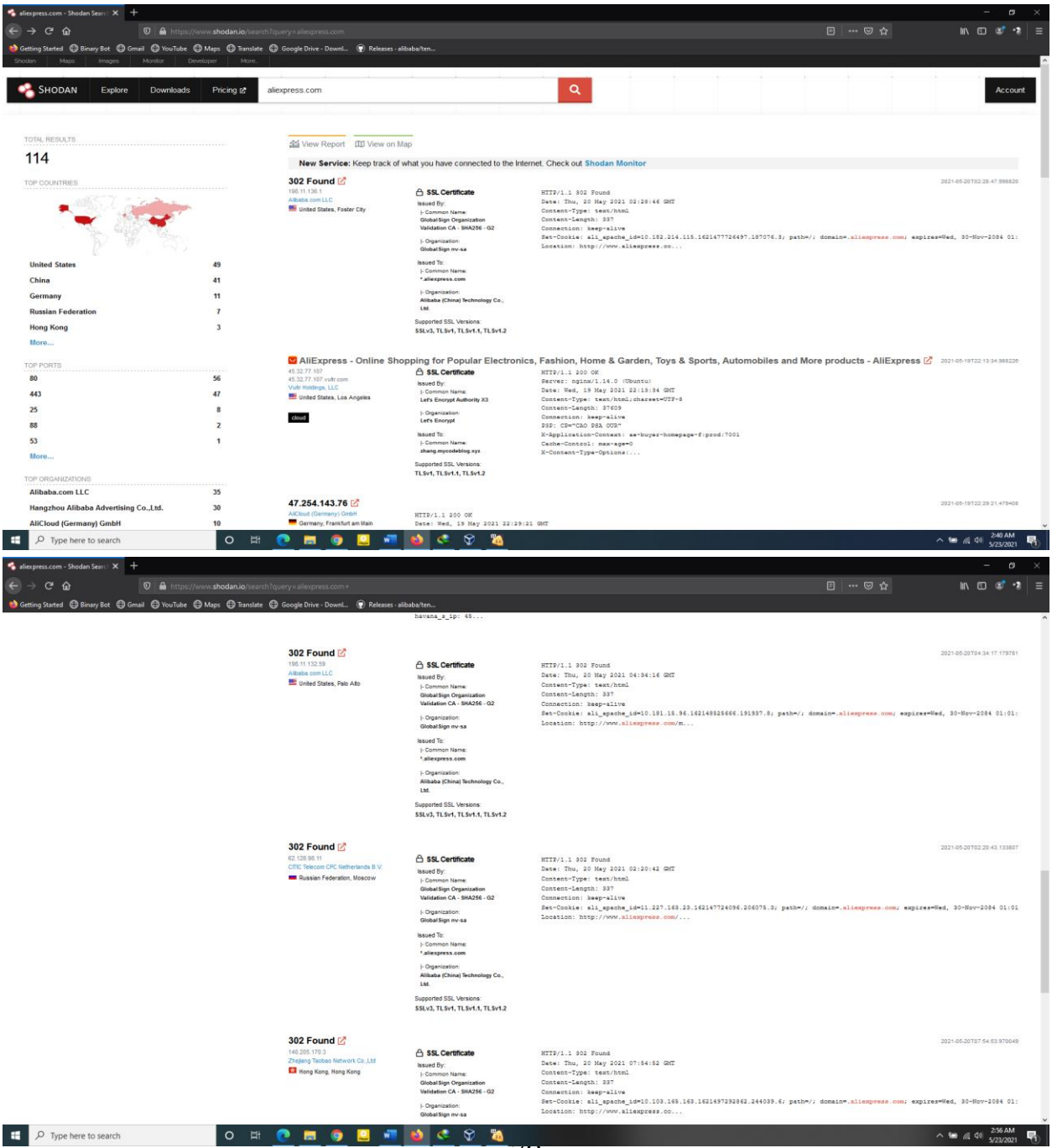
Public Device Enumeration

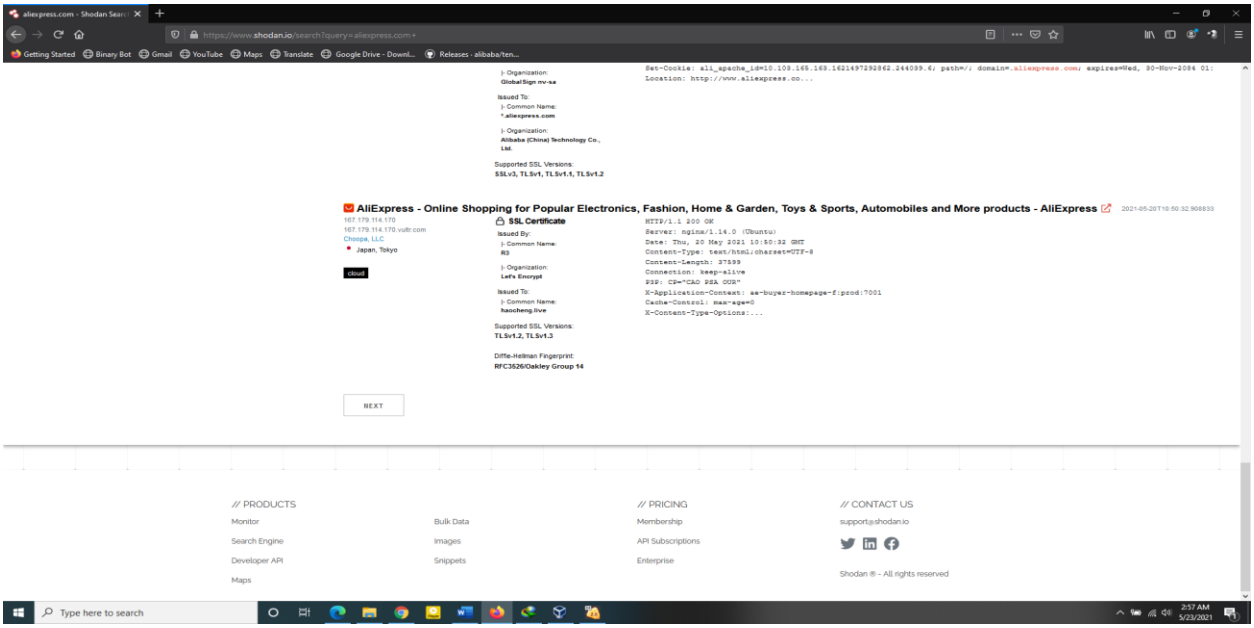
1. **Shodan**

Shodan is a search engine that uses a number of filters to help users identify various sorts of computers (webcams, routers, servers, and so on) connected to the internet. Some have referred to it as a search engine for service banners, which are metadata sent back to the client by the server.

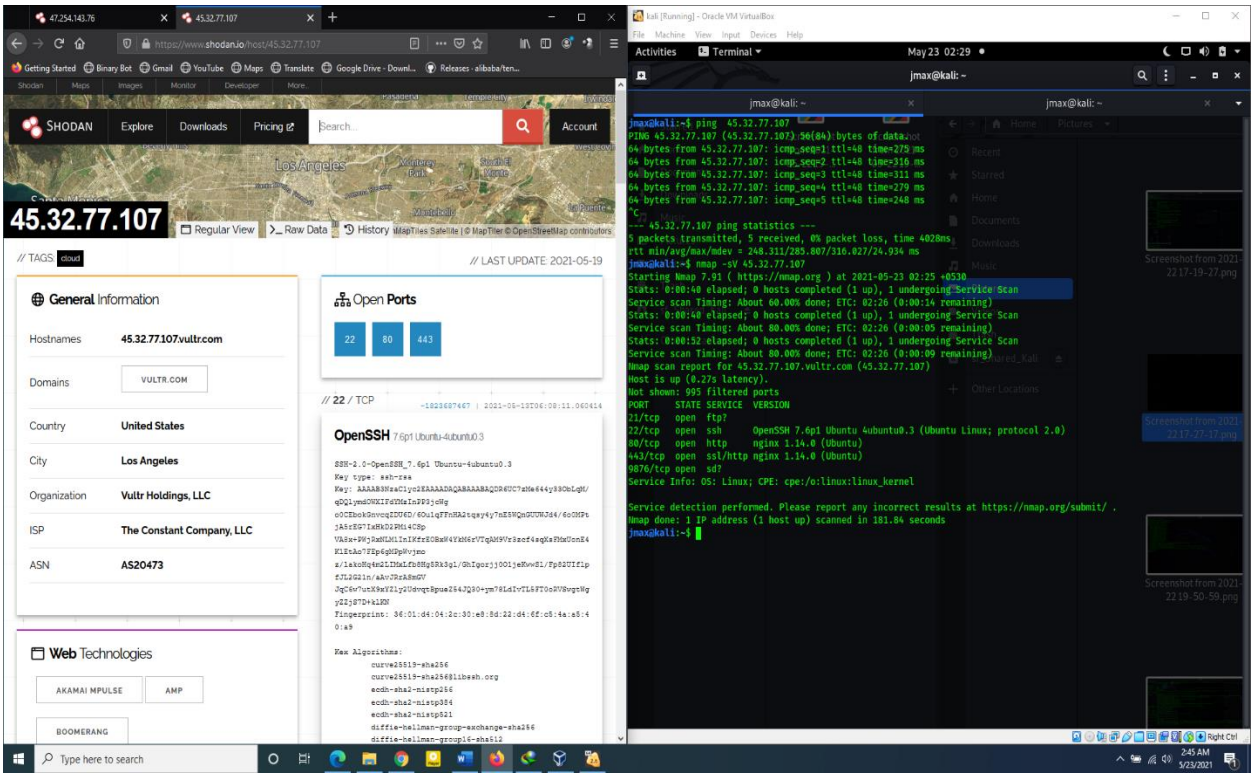
Link: https://www.shodan.io/

Following Details could be extracted from the shodan.io

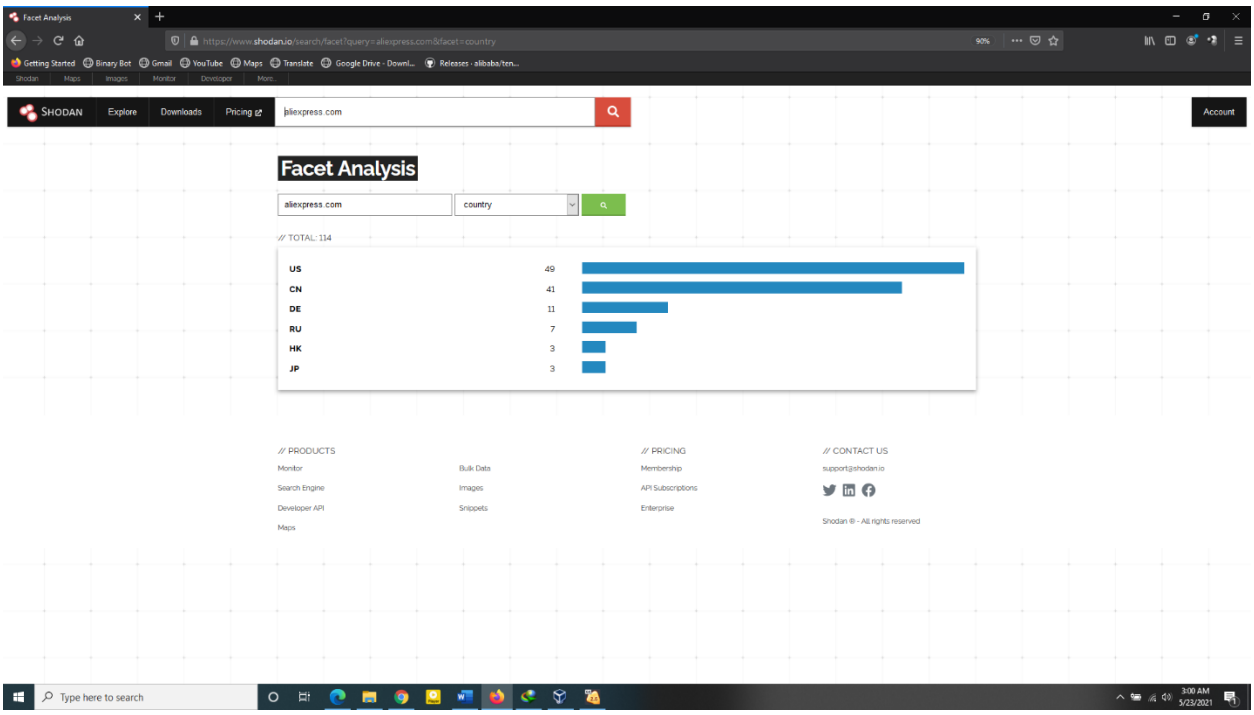


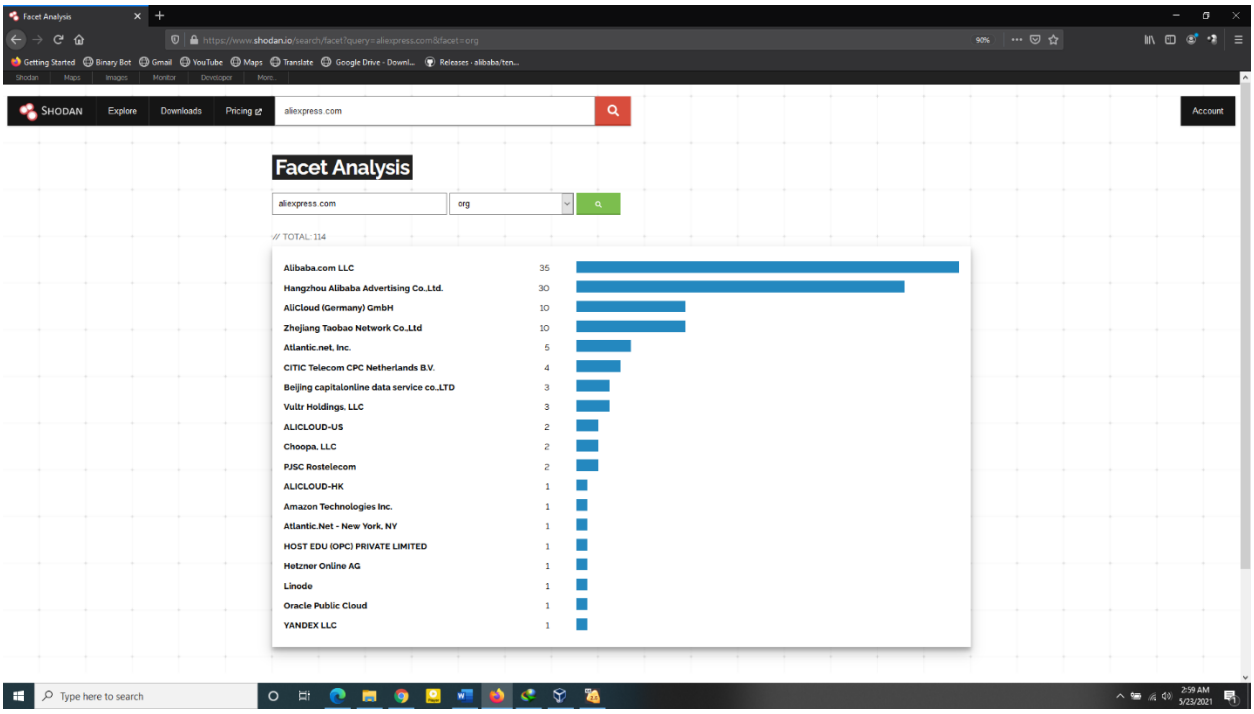


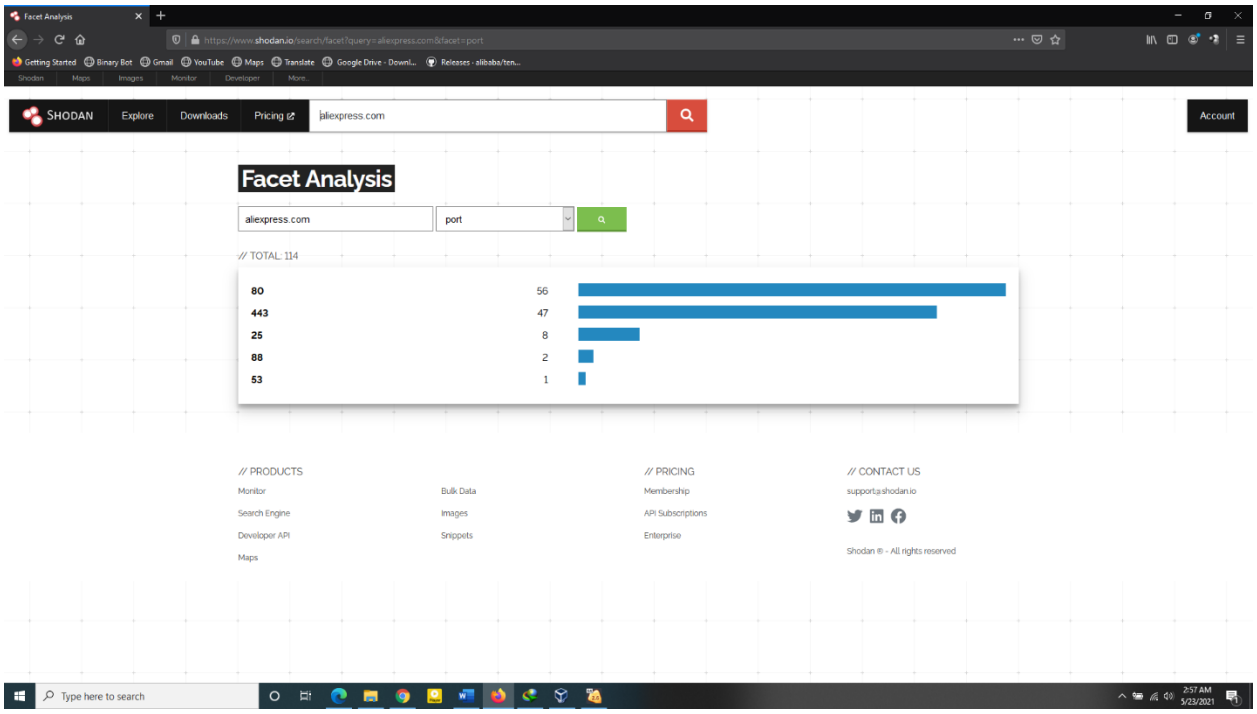
Then I just try the one of the IP address of above results. Then I tried to extract more details related IP address.

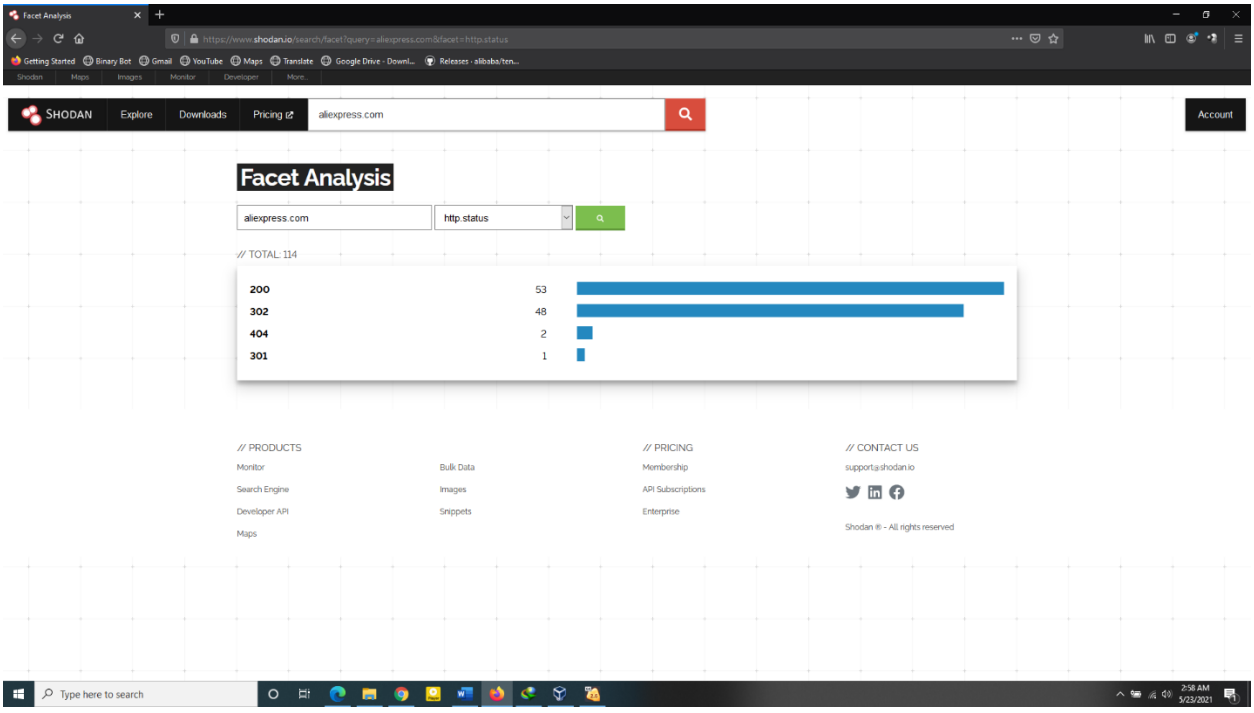


Following Screenshots are contain the summery of the domain specifications including organization, port, HTTP status and country.





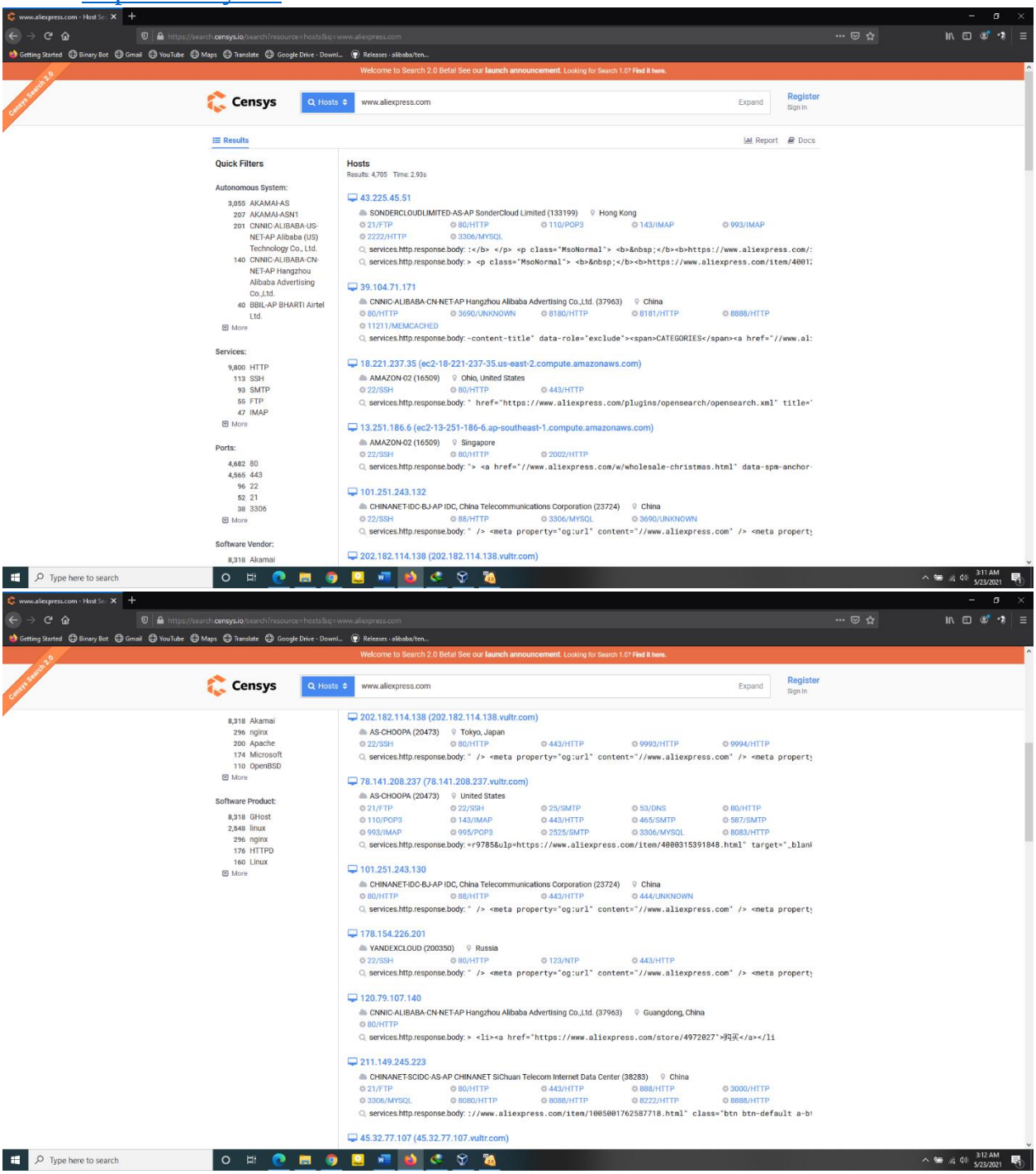

Facet Analysis
SHODAN
Explore
Downloads
Pricing
aliexpress.com
Account
Facet Analysis
aliexpress.com
port
// TOTAL: 114
80 56
443 47
25 8
88 2
53 1
// PRODUCTS
Monitor
Search Engine
Developer API
Maps
Bulk Data
Images
Snippets
// PRICING
Membership
API Subscriptions
Enterprise
// CONTACT US
support@shodan.io
Shodan ® - All rights reserved

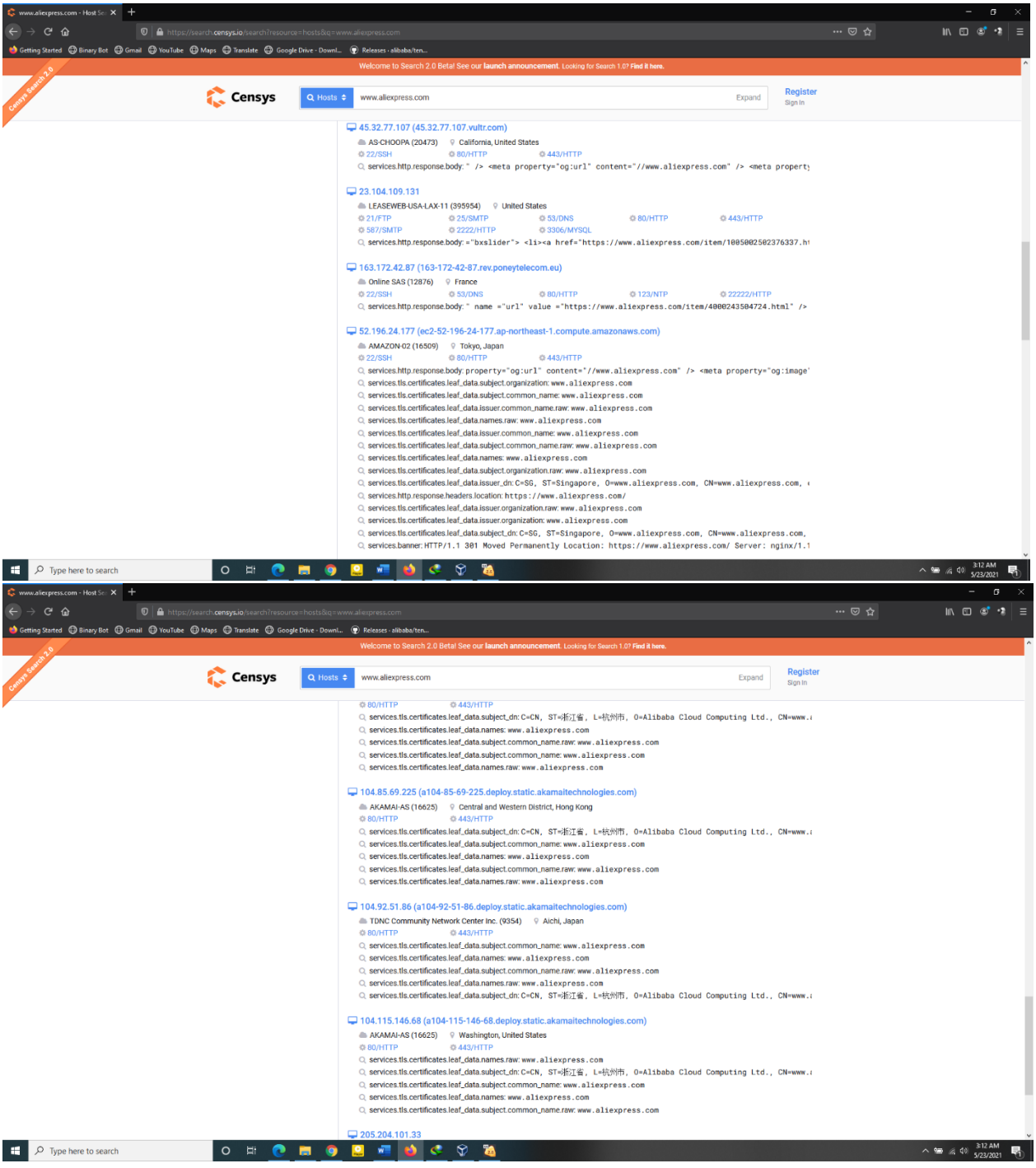

Facet Analysis
SHODAN
Explore
Downloads
Pricing
aliexpress.com
Account
Facet Analysis
aliexpress.com
http.status
// TOTAL: 114
200 53
302 48
404 2
301 1
// PRODUCTS
Monitor
Search Engine
Developer API
Maps
Bulk Data
Images
Snippets
// PRICING
Membership
API Subscriptions
Enterprise
// CONTACT US
support@shodan.io
Shodan ® - All rights reserved

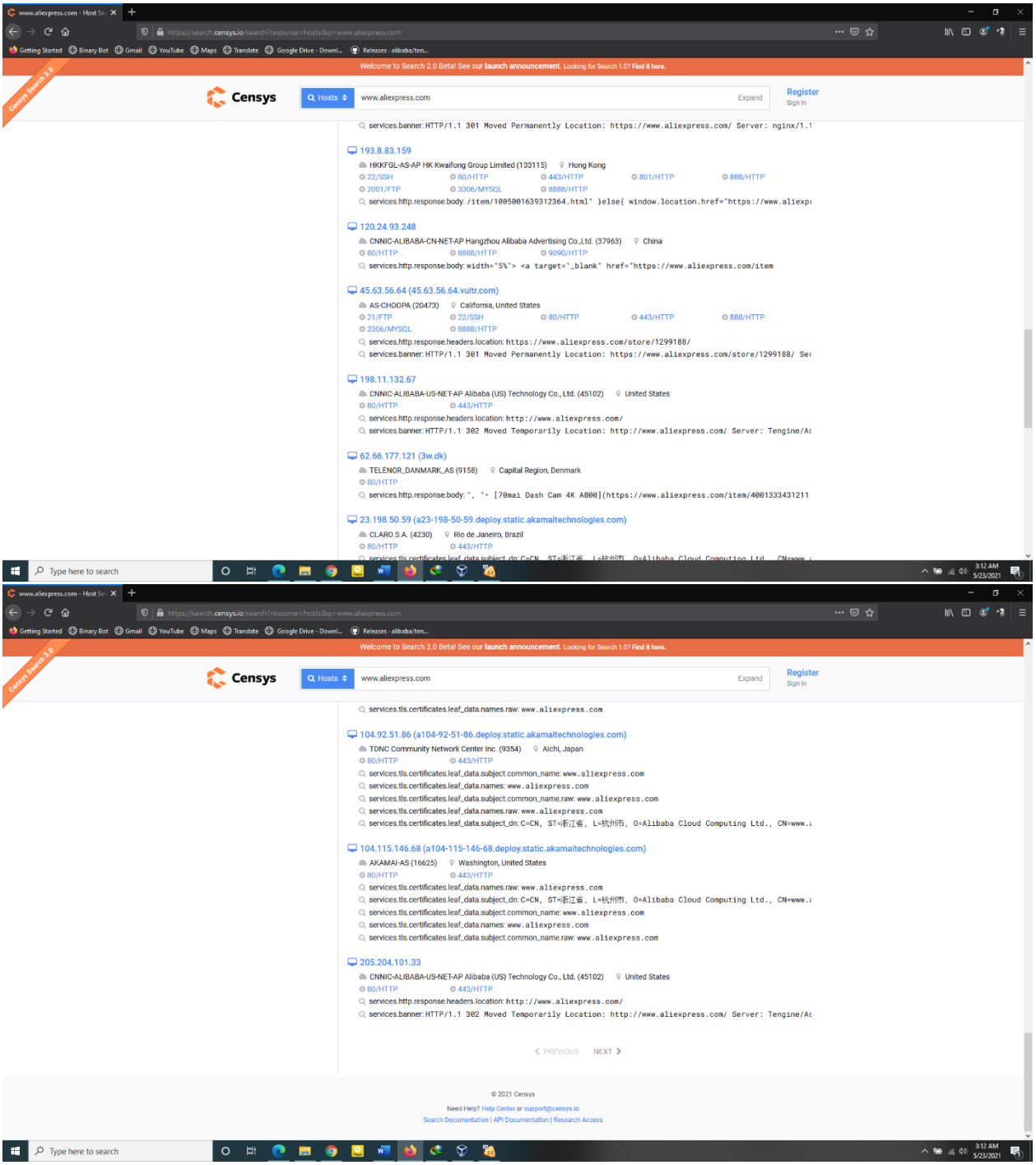
2. Censys

Censys, like Shodan, is a public search engine that allows researchers to ask queries about the hosts and networks that make up the Internet.

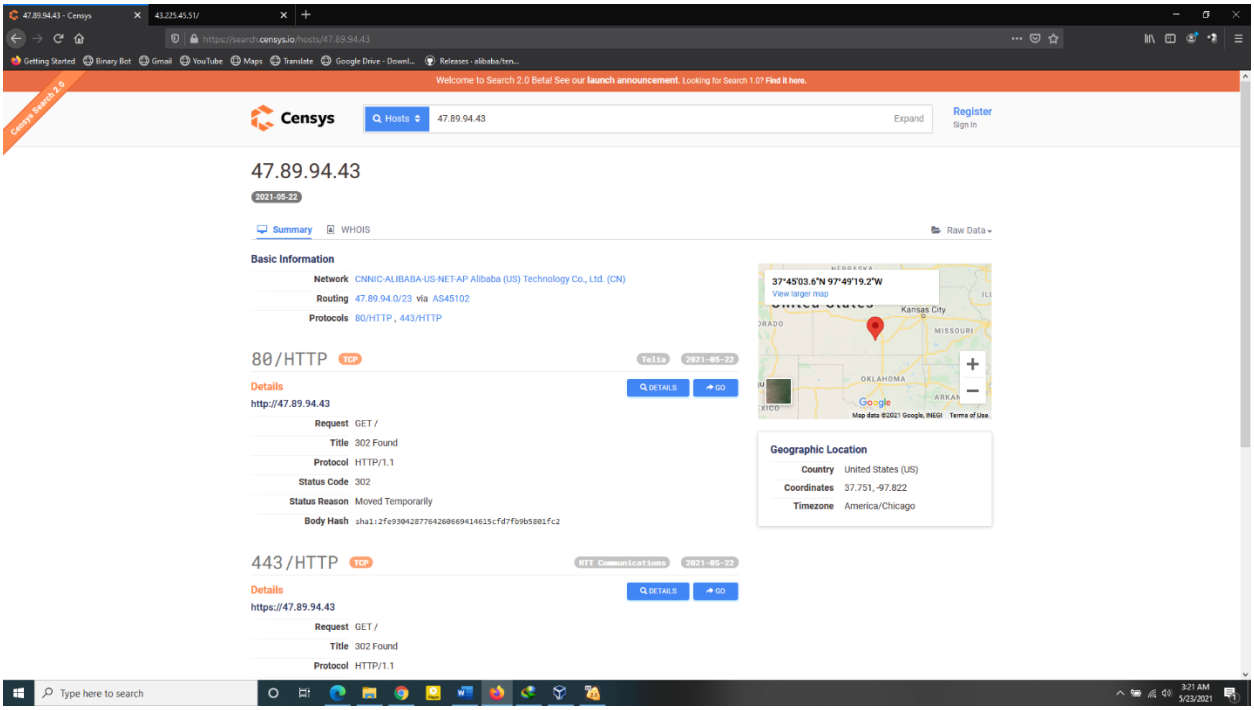
Link: https://censys.io



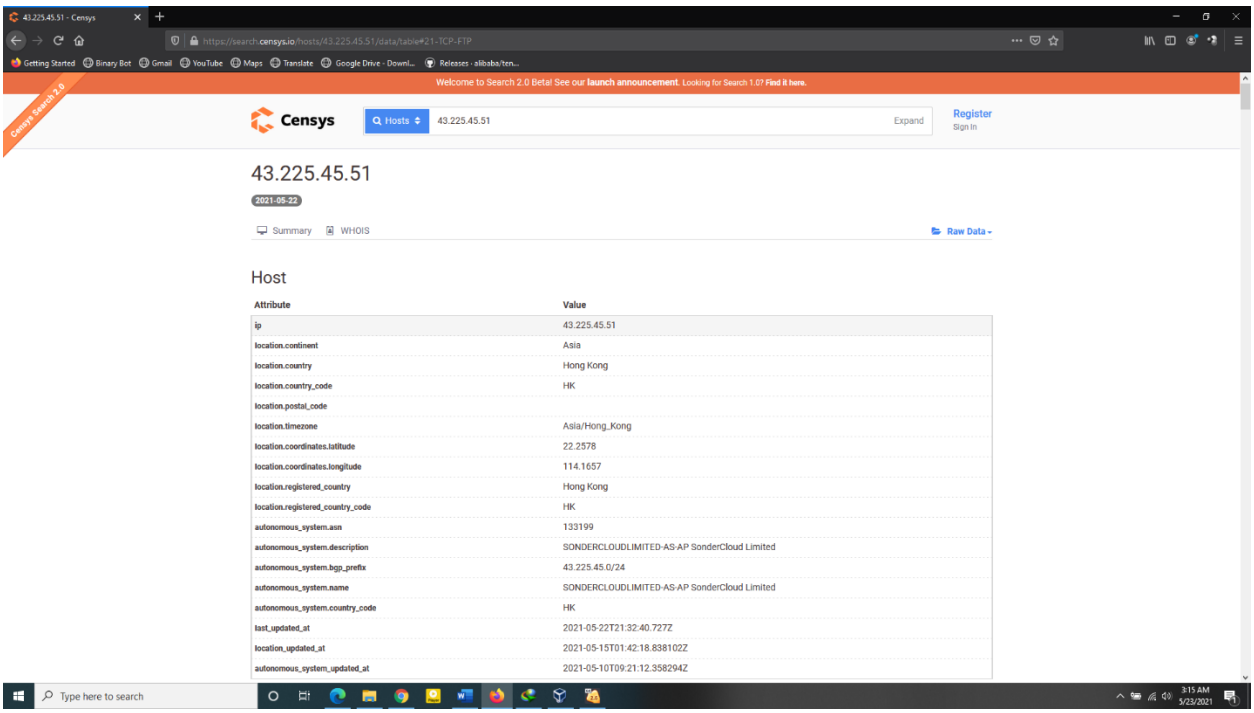

Censys
Hosts
www.aliexpress.com
Expand
Register
Sign In
45.32.77.107 (45.32.77.107.vultr.com)
AS-CHOOPA (20473)
California, United States
22/SSH
80/HTTP
443/HTTP
23.104.109.131
LEASEWEB-USA-LAX-11 (395954)
United States
21/FTP
25/SMTP
53/DNS
80/HTTP
443/HTTP
587/SMTP
2222/HTTP
3306/MYSQL
163.172.42.87 (163-172-42-87.rev.poneytelecom.eu)
Online SAS (12876)
France
22/SSH
53/DNS
80/HTTP
123/NTP
22222/HTTP
52.196.24.177 (ec2-52-196-24-177.ap-northeast-1.compute.amazonaws.com)
AMAZON-02 (16509)
Tokyo, Japan
22/SSH
80/HTTP
443/HTTP
104.85.69.225 (a104-85-69-225.deploy.static.akamaitechnologies.com)
AKAMAI-AS (16625)
Central and Western District, Hong Kong
104.92.51.86 (a104-92-51-86.deploy.static.akamaitechnologies.com)
TDNC Community Network Center Inc. (9354)
Aichi, Japan
104.115.146.68 (a104-115-146-68.deploy.static.akamaitechnologies.com)
AKAMAI-AS (16625)
Washington, United States
205.204.101.33
Type here to search

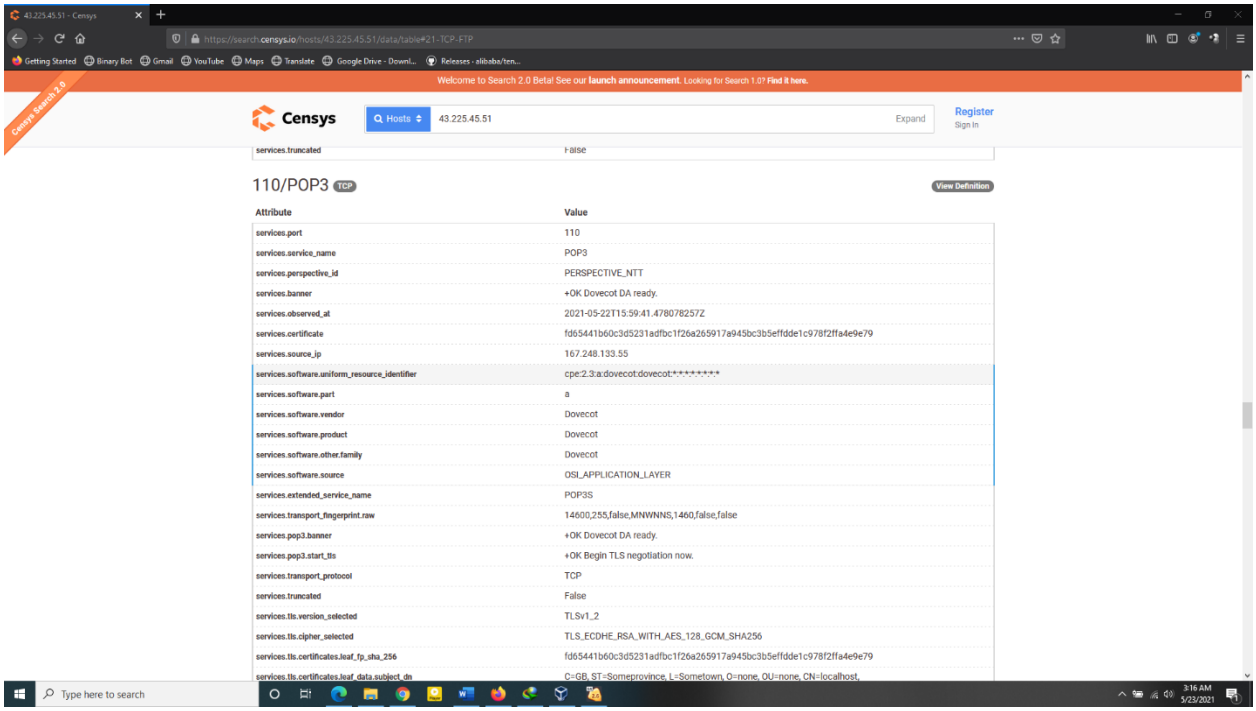

www.aliexpress.com - Host Se
https://search.censys.io/search?resource=hosts&q=www.aliexpress.com
Getting Started
Binary Bot
Gmail
YouTube
Maps
Translate
Google Drive - Downl...
Releases · alibaba/ten...
Welcome to Search 2.0 Beta! See our launch announcement. Looking for Search 1.0? Find it here.
Censys Search 2.0
Censys
Hosts
www.aliexpress.com
Expand
Register
Sign In
services.banner: HTTP/1.1 301 Moved Permanently Location: https://www.aliexpress.com/ Server: nginx/1.1
193.8.83.159
HKKFGL-AS-AP HK Kwaifong Group Limited (133115)
Hong Kong
22/SSH
80/HTTP
443/HTTP
801/HTTP
888/HTTP
2001/FTP
3306/MYSQL
8888/HTTP
services.http.response.body: /item/1005001639312364.html" }else{ window.location.href="https://www.aliexpr
120.24.93.248
CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd. (37963)
China
80/HTTP
8888/HTTP
9090/HTTP
services.http.response.body: width="5%"> <a target="_blank" href="https://www.aliexpress.com/item
45.63.56.64 (45.63.56.64.vultr.com)
AS-CHOOPA (20473)
California, United States
21/FTP
22/SSH
80/HTTP
443/HTTP
888/HTTP
3306/MYSQL
8888/HTTP
services.http.response.headers.location: https://www.aliexpress.com/store/1299188/
services.banner: HTTP/1.1 301 Moved Permanently Location: https://www.aliexpress.com/store/1299188/ Ser
198.11.132.67
CNNIC-ALIBABA-US-NET-AP Alibaba (US) Technology Co., Ltd. (45102)
United States
80/HTTP
443/HTTP
services.http.response.headers.location: http://www.aliexpress.com/
services.banner: HTTP/1.1 302 Moved Temporarily Location: http://www.aliexpress.com/ Server: Tengine/A
62.66.177.121 (3w.dk)
TELENOR_DANMARK_AS (9158)
Capital Region, Denmark
80/HTTP
services.http.response.body: ", "• [70mai Dash Cam 4K A800](https://www.aliexpress.com/item/4001333431211
23.198.50.59 (a23-198-50-59.deploy.static.akamaitechnologies.com)
CLARO S.A. (4230)
Rio de Janeiro, Brazil
80/HTTP
443/HTTP
Type here to search
3:12 AM
5/23/2021
services.tls.certificates.leaf_data.names.raw: www.aliexpress.com
104.92.51.86 (a104-92-51-86.deploy.static.akamaitechnologies.com)
TDNC Community Network Center Inc. (9354)
Aichi, Japan
80/HTTP
443/HTTP
services.tls.certificates.leaf_data.subject.common_name: www.aliexpress.com
services.tls.certificates.leaf_data.names: www.aliexpress.com
services.tls.certificates.leaf_data.subject.common_name.raw: www.aliexpress.com
services.tls.certificates.leaf_data.names.raw: www.aliexpress.com
services.tls.certificates.leaf_data.subject_dn: C=CN, ST=浙江省, L=杭州市, O=Alibaba Cloud Computing Ltd., CN=www.
104.115.146.68 (a104-115-146-68.deploy.static.akamaitechnologies.com)
AKAMAI-AS (16625)
Washington, United States
80/HTTP
443/HTTP
services.tls.certificates.leaf_data.names.raw: www.aliexpress.com
services.tls.certificates.leaf_data.subject_dn: C=CN, ST=浙江省, L=杭州市, O=Alibaba Cloud Computing Ltd., CN=www.
services.tls.certificates.leaf_data.subject.common_name: www.aliexpress.com
services.tls.certificates.leaf_data.names: www.aliexpress.com
services.tls.certificates.leaf_data.subject.common_name.raw: www.aliexpress.com
205.204.101.33
CNNIC-ALIBABA-US-NET-AP Alibaba (US) Technology Co., Ltd. (45102)
United States
80/HTTP
443/HTTP
services.http.response.headers.location: http://www.aliexpress.com/
services.banner: HTTP/1.1 302 Moved Temporarily Location: http://www.aliexpress.com/ Server: Tengine/A
PREVIOUS
NEXT
© 2021 Censys
Need Help? Help Center or support@censys.io
Search Documentation | API Documentation | Research Access

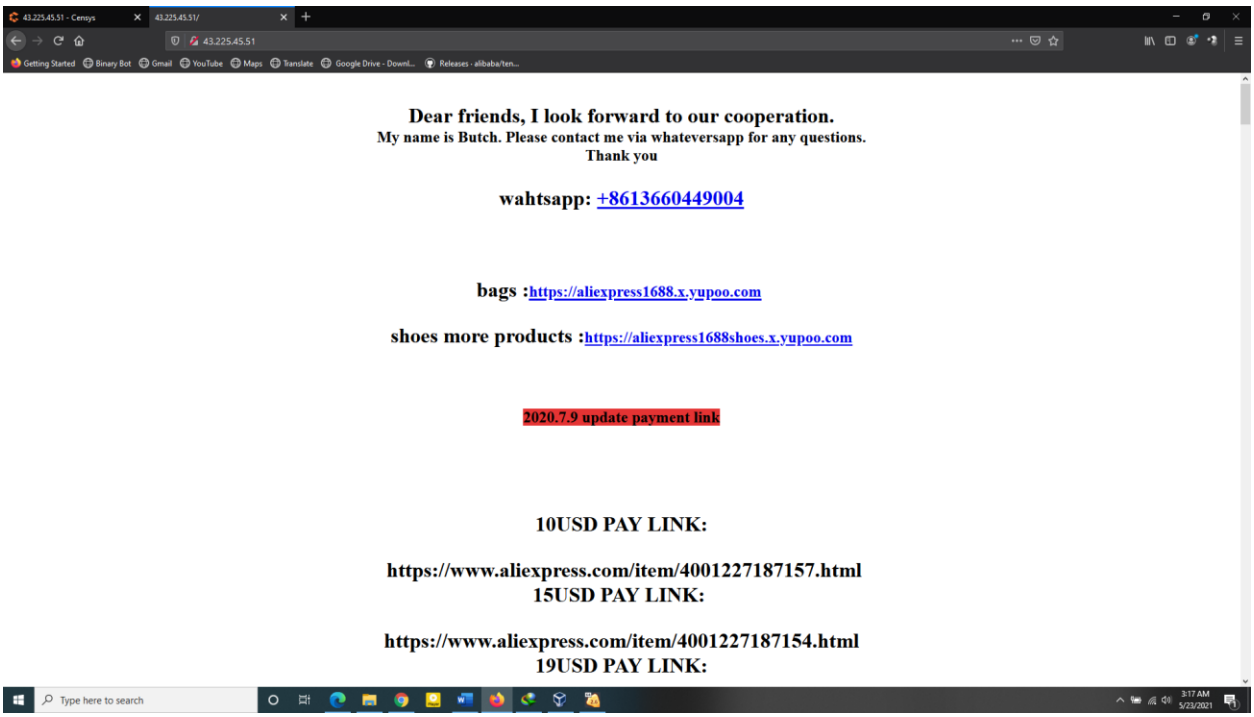
According to Following Screenshot We can get the details of the domain's related IP address.



Following Screenshots show selected IP address specific information from the results.




Censys
Hosts
43.225.45.51
Expand
Register
Sign In
services.truncated
False
110/POP3
TCP
View Definition
Attribute
Value
services.port
110
services.service_name
POP3
services.perspective_id
PERSPECTIVE_NTT
services.banner
+OK Dovecot DA ready.
services.observed_at
2021-05-22T15:59:41.478078257Z
services.certificate
fd65441b60c3d5231adfbc1f26a265917a945bc3b5effdde1c978f2ffa4e9e79
services.source_ip
167.248.133.55
services.software.uniform_resource_identifier
cpe:2.3:a:dovecot:dovecot:*:*:*:*:*:*:*:*
services.software.part
a
services.software.vendor
Dovecot
services.software.product
Dovecot
services.software.other.family
Dovecot
services.software.source
OSI_APPLICATION_LAYER
services.extended_service_name
POP3S
services.transport_fingerprint.raw
14600,255,false,MNWNNS,1460,false,false
services.pop3.banner
+OK Dovecot DA ready.
services.pop3.start_tls
+OK Begin TLS negotiation now.
services.transport_protocol
TCP
services.truncated
False
services.tls.version_selected
TLSv1_2
services.tls.cipher_selected
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
services.tls.certificates.leaf_fp_sha_256
fd65441b60c3d5231adfbc1f26a265917a945bc3b5effdde1c978f2ffa4e9e79
services.tls.certificates.leaf_data.subject_dn
C=GB, ST=Someprovince, L=Sometown, O=none, OU=none, CN=localhost,
Type here to search
3:16 AM
5/23/2021


43.225.45.51
Dear friends, I look forward to our cooperation.
My name is Butch. Please contact me via whateversapp for any questions.
Thank you
wahtsapp: +8613660449004
bags :https://aliexpress1688.x.yupoo.com
shoes more products :https://aliexpress1688shoes.x.yupoo.com
2020.7.9 update payment link
10USD PAY LINK:
https://www.aliexpress.com/item/4001227187157.html
15USD PAY LINK:
https://www.aliexpress.com/item/4001227187154.html
19USD PAY LINK:
Type here to search
3:17 AM
5/23/2021

Find Structure of File System

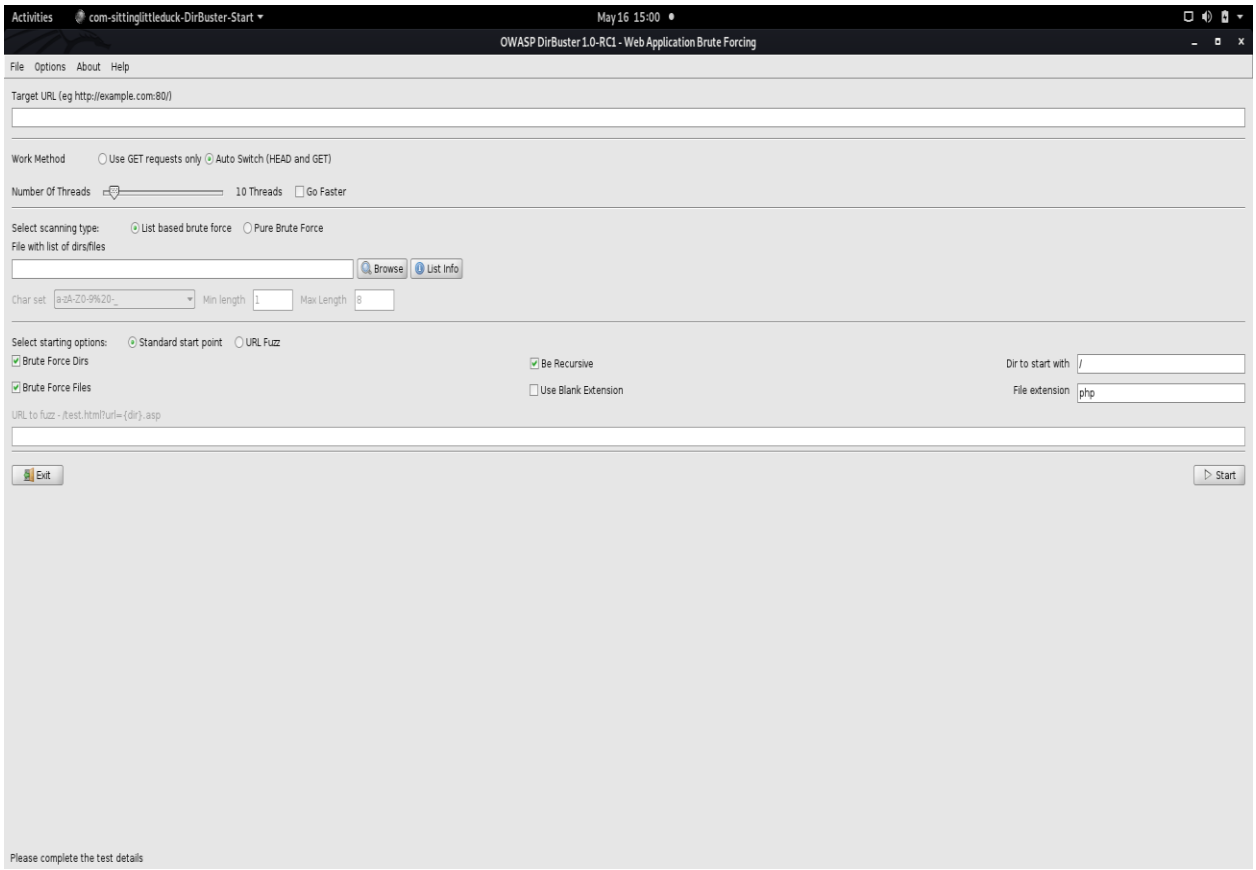
1. OWASP DirBuster

DirBuster is a multi-threaded Java application that brute-forces the names of directories and files on web/application servers. The list was created from the ground up by searching the Internet and gathering the directories and files that developers really use.

When I using DirBuster tool, my inputs get from the test results of the Nikto ,Zenmap,Sublist3r.

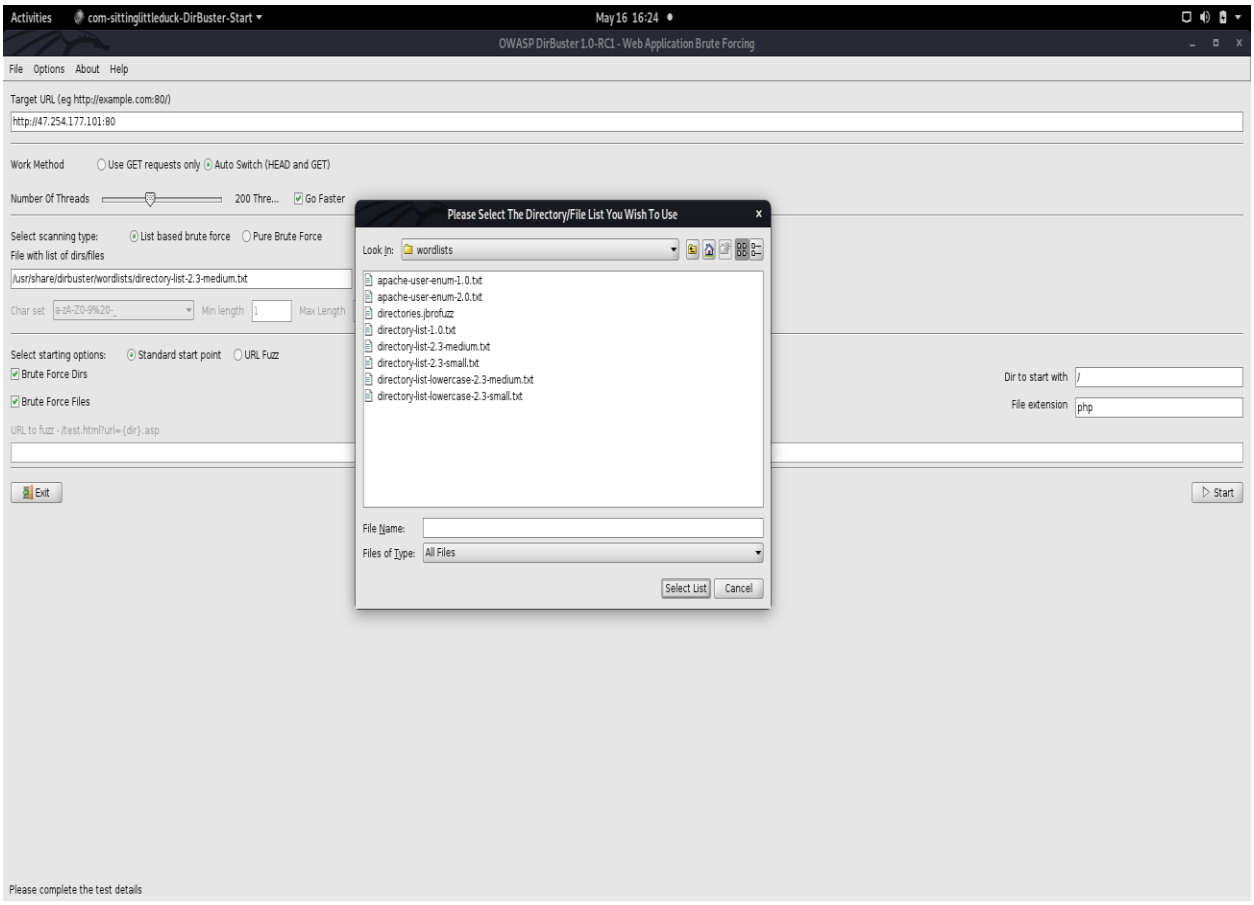
I tried few times using above test results. Following screenshots are express the DirBuster Test Results. This test takes about 10-20 minutes to complete. That time varies depending on the number of filters.

The following is the typical interface of DirBuster Tool.



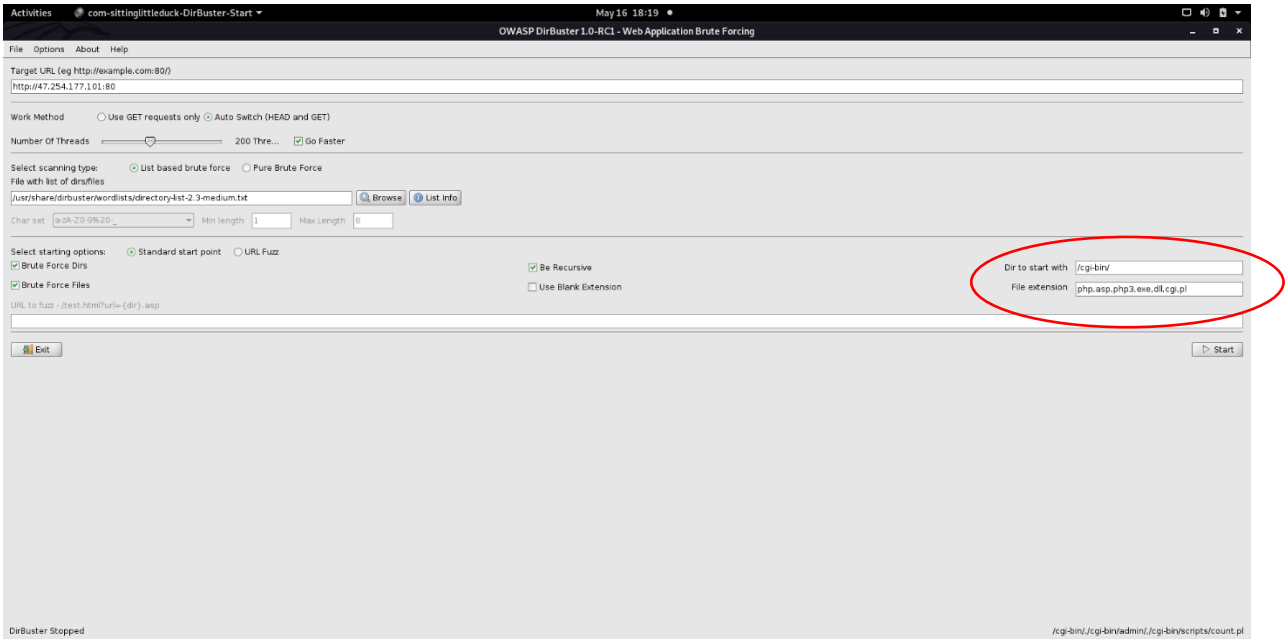
According to the screenshot above, first the URL should be entered along with the required domain and the port number according to the sample given there. Then select the scan type. List based brute force should be selected and it was not successful in selecting Pure Brute Force. When selecting a thread size, the default size is 200.

Next you need to select a list from the list provided by DirBuster. It is shown in the screenshot below.



Then you need to enter the paths or directories after the domain related to Brute Force. Next you need to enter the possible file extensions as well.

I researched and used the information obtained in the section for the below mentioned input fields. According to the Zenmap result mentioned above, 3 port numbers have been identified as open and 2 of them are HTTP and the other is FTP. Although all three ports were used for the scan, the most successful was port number 443, an HTTP service.



There are hundreds of directories found from the reconnaissance. Few directories are shown below.

/cgi-bin/

/cgi-bin/admin/

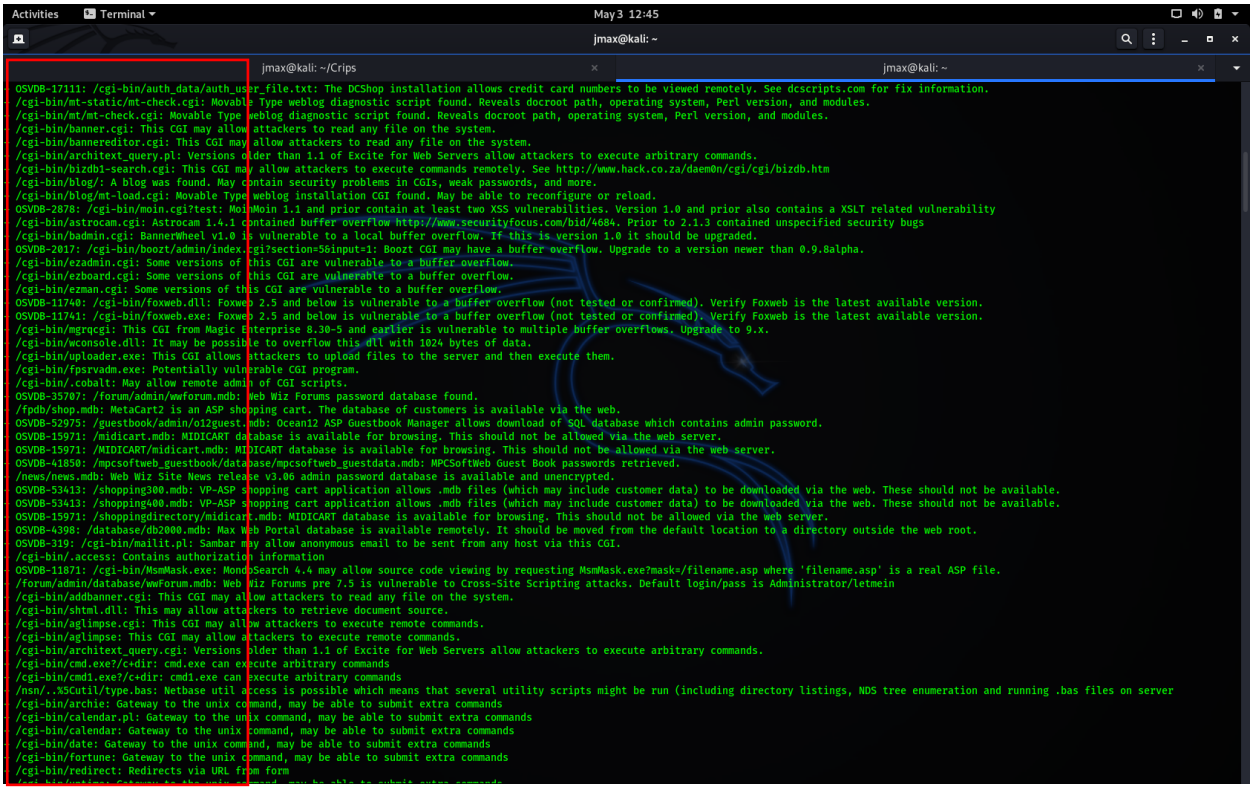
/cgi-bin/scripts/

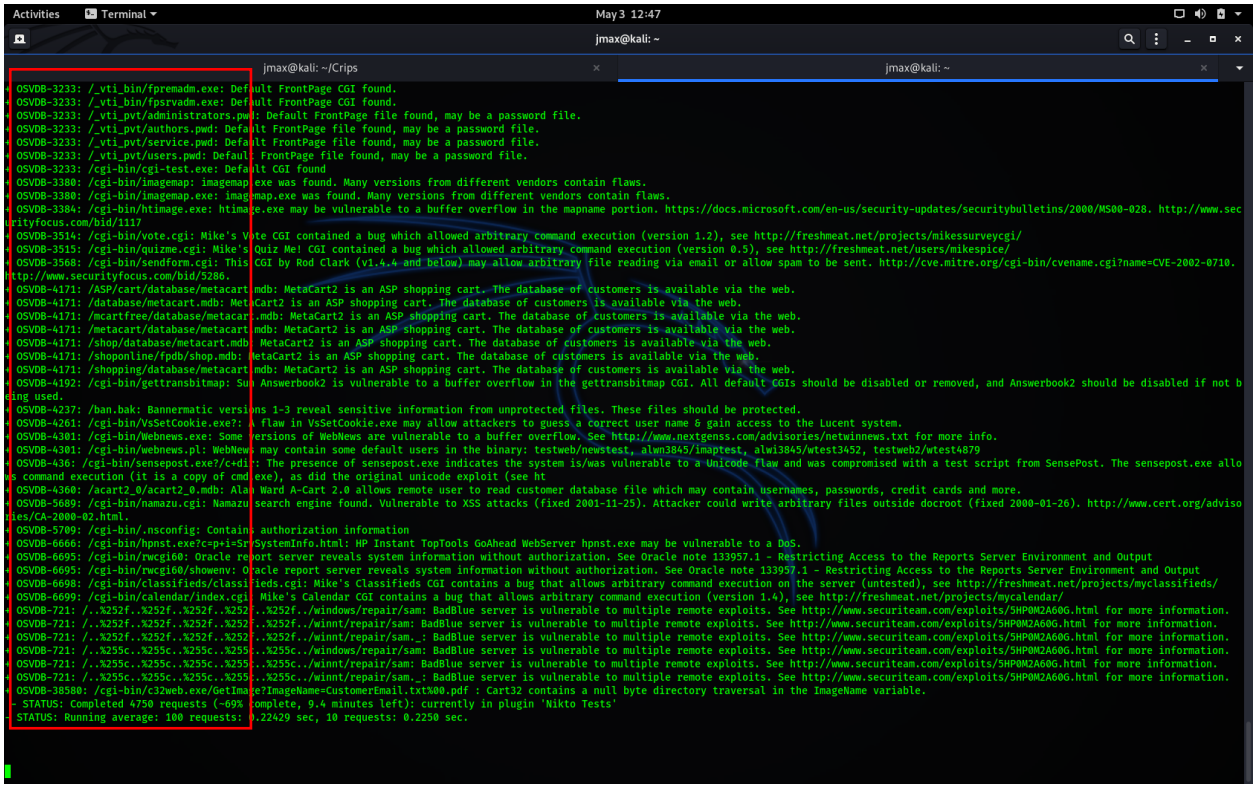
/_vti_bin/

/metacart/database/

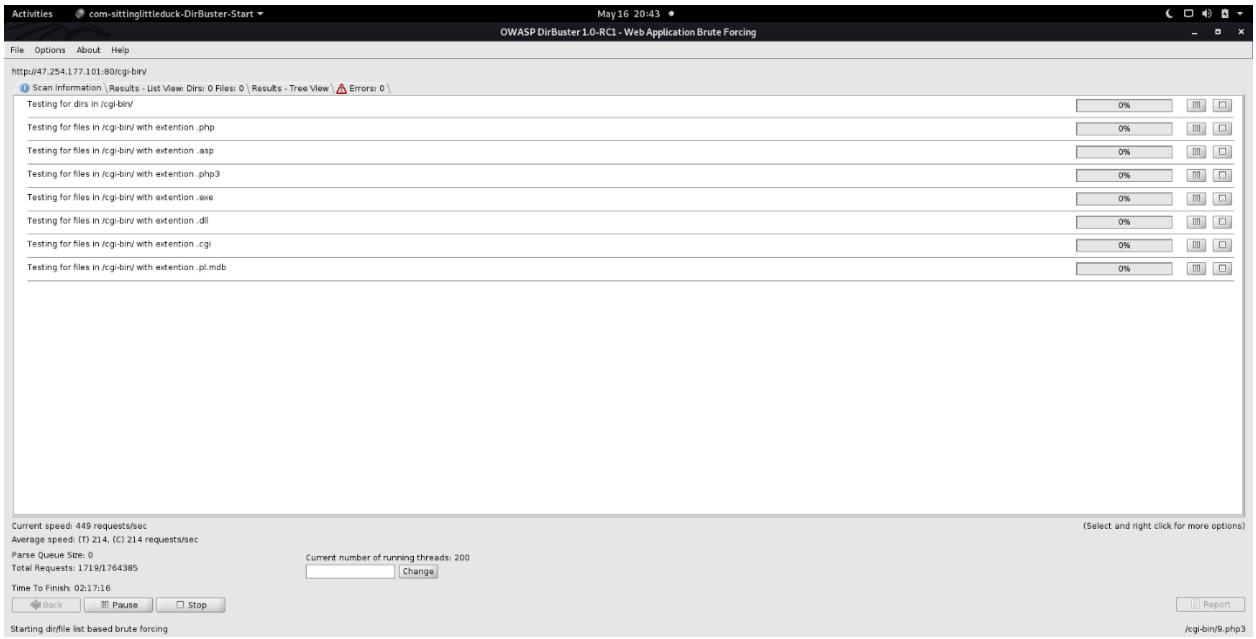
/ASP/cart/database/

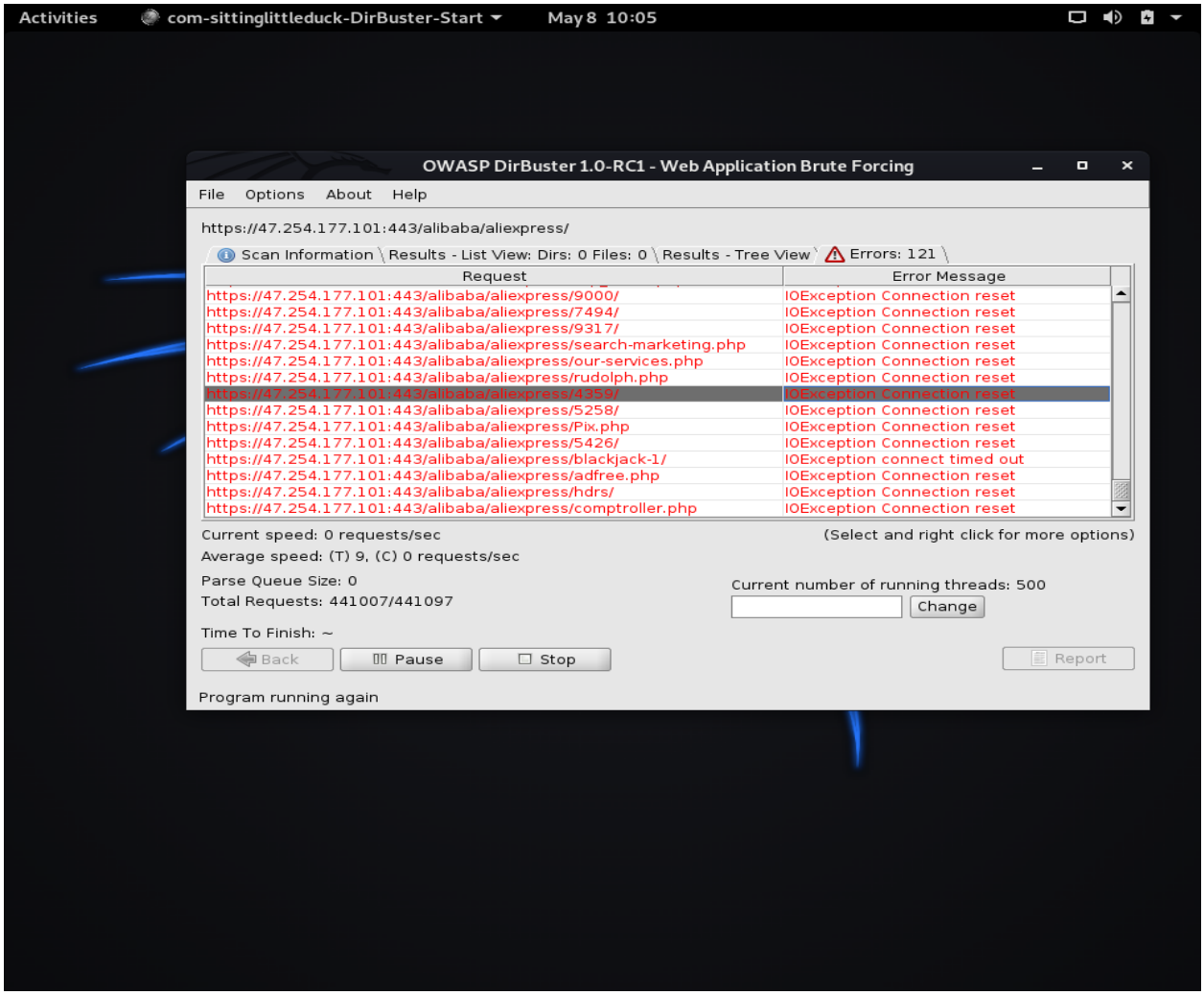
Below are some of the few results explored and extracted in the reconnaissance section.

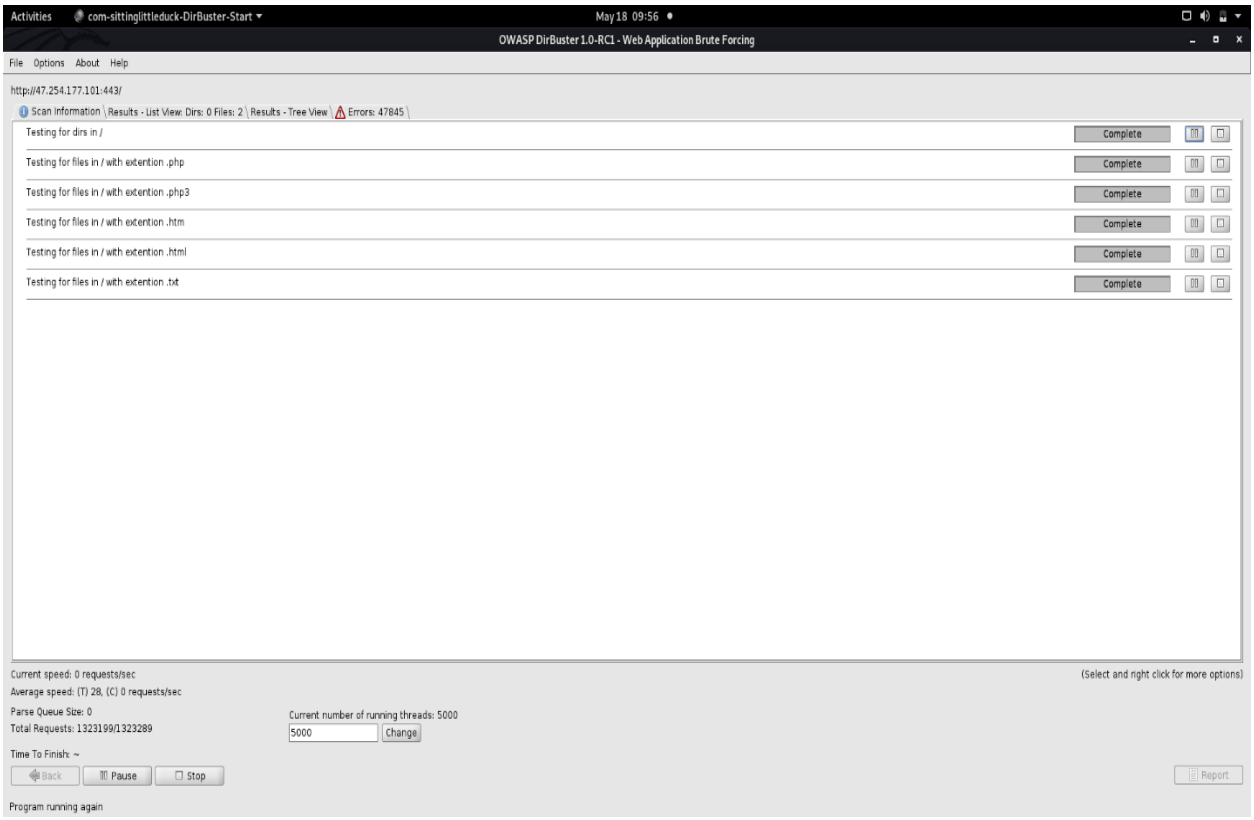


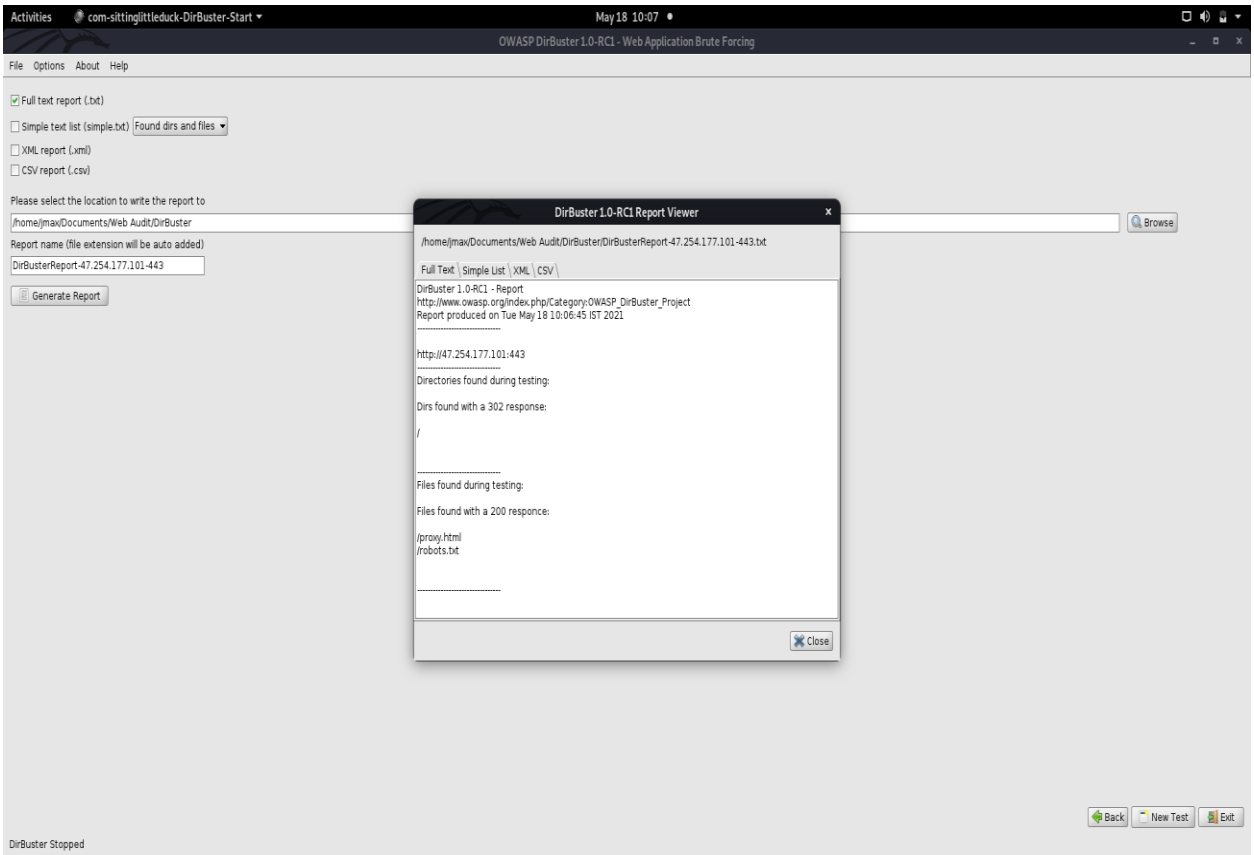


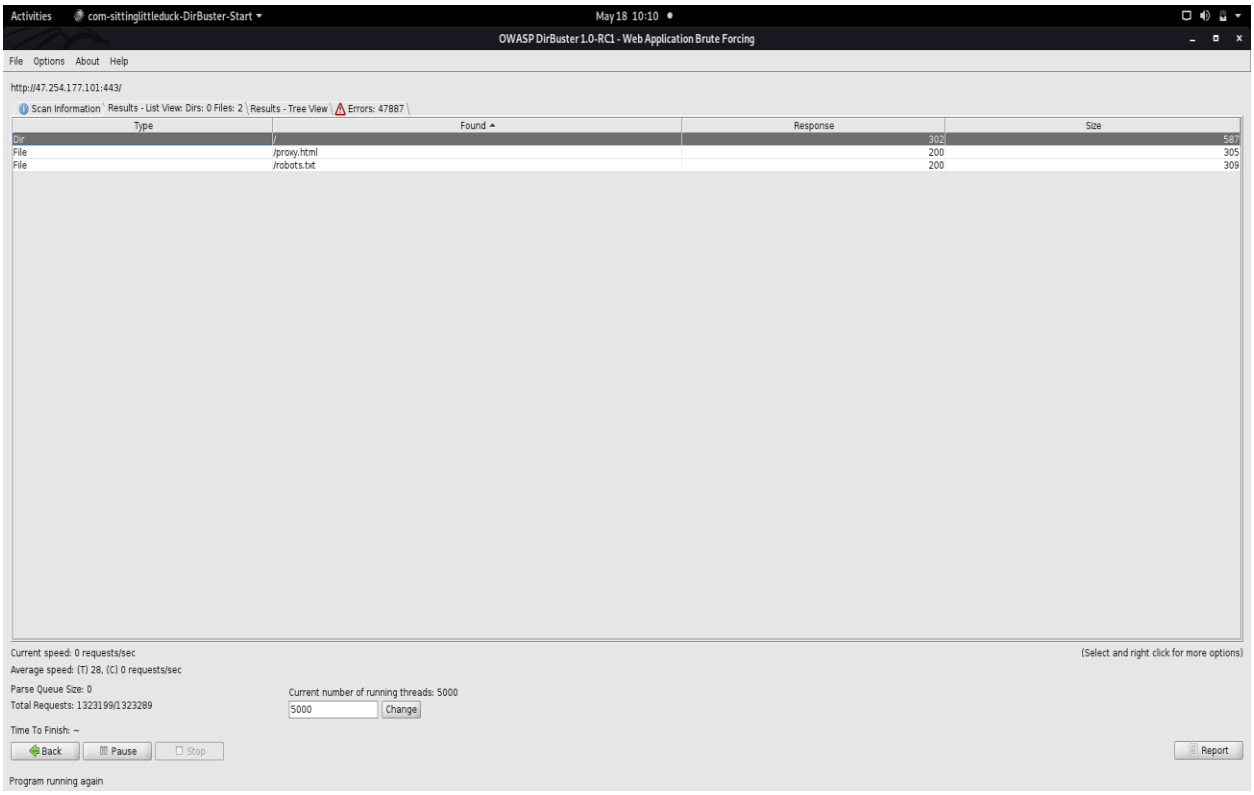
Below are some screenshots of sample attempts at scanning …

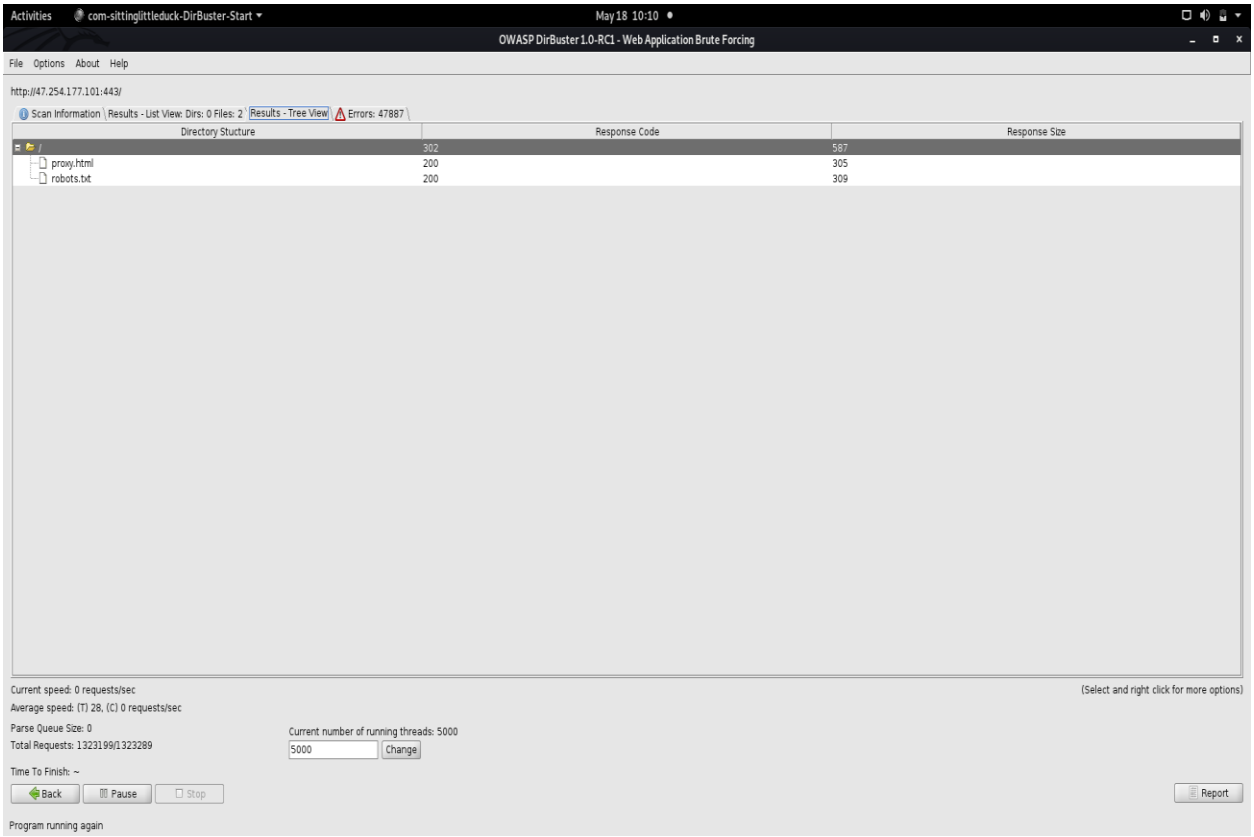




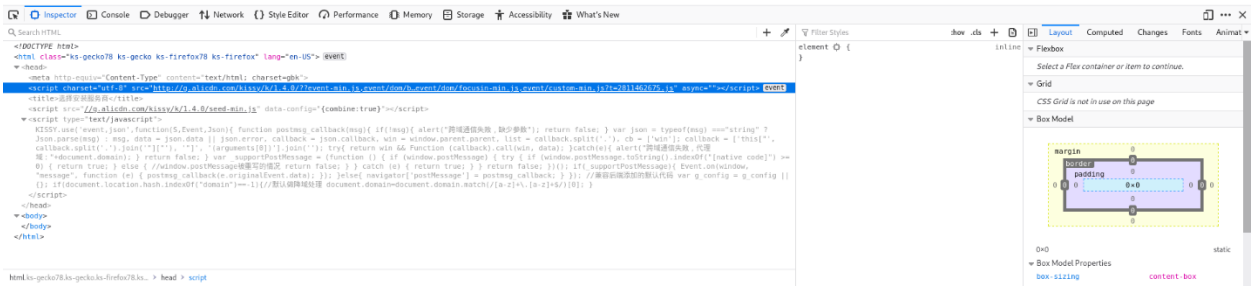

Activities
com-sittinglittleduck-DirBuster-Start
May 18 09:56
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://47.254.177.101:443/
Scan Information \ Results - List View: Dirs: 0 Files: 2 \ Results - Tree View \ Errors: 47845 \
Testing for dirs in /
Testing for files in / with extention .php
Testing for files in / with extention .php3
Testing for files in / with extention .htm
Testing for files in / with extention .html
Testing for files in / with extention .txt
Complete
Current speed: 0 requests/sec
Average speed: (T) 28, (C) 0 requests/sec
Parse Queue Size: 0
Total Requests: 1323199/1323289
Time To Finish: ~
Current number of running threads: 5000
5000
Change
Back
Pause
Stop
(Select and right click for more options)
Report
Program running again


Activities
com-sittinglittleduck-DirBuster-Start
May 18 10:07
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
Full text report (.txt)
Simple text list (simple.txt)
Found dirs and files
XML report (.xml)
CSV report (.csv)
Please select the location to write the report to
/home/jmax/Documents/Web Audit/DirBuster
Browse
Report name (file extension will be auto added)
DirBusterReport-47.254.177.101-443
Generate Report
DirBuster 1.0-RC1 Report Viewer
/home/jmax/Documents/Web Audit/DirBuster/DirBusterReport-47.254.177.101-443.txt
Full Text
Simple List
XML
CSV
DirBuster 1.0-RC1 - Report
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Tue May 18 10:06:45 IST 2021
http://47.254.177.101:443
Directories found during testing:
Dirs found with a 302 response:
/
Files found during testing:
Files found with a 200 responce:
/proxy.html
/robots.txt
Close
Back
New Test
Exit
DirBuster Stopped

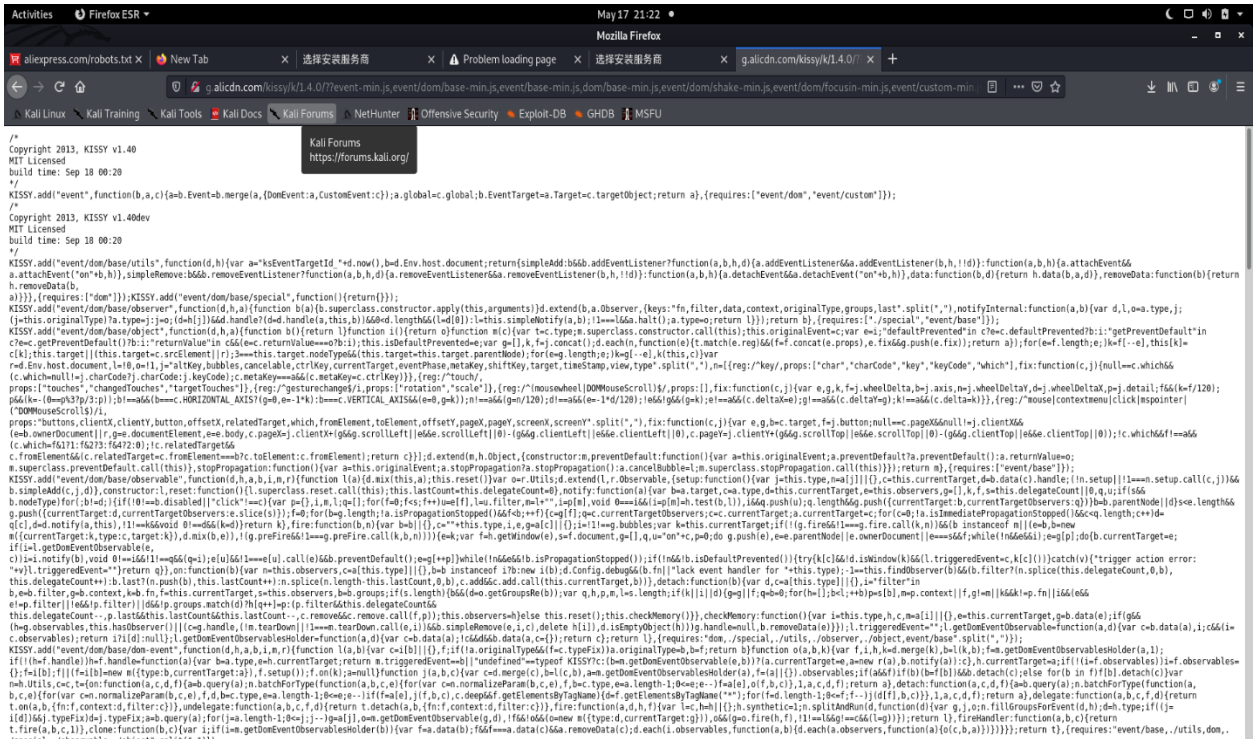

Activities
com-sittinglittleduck-DirBuster-Start
May 18 10:10
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://47.254.177.101:443/
Scan Information Results - List View: Dirs: 0 Files: 2 Results - Tree View Errors: 47887
Type Found Response Size
Dir / 302 587
File /proxy.html 200 305
File /robots.txt 200 309
Current speed: 0 requests/sec
(Select and right click for more options)
Average speed: (T) 28, (C) 0 requests/sec
Parse Queue Size: 0
Total Requests: 1323199/1323289
Current number of running threads: 5000
5000
Change
Time To Finish: ~
Back
Pause
Stop
Report
Program running again

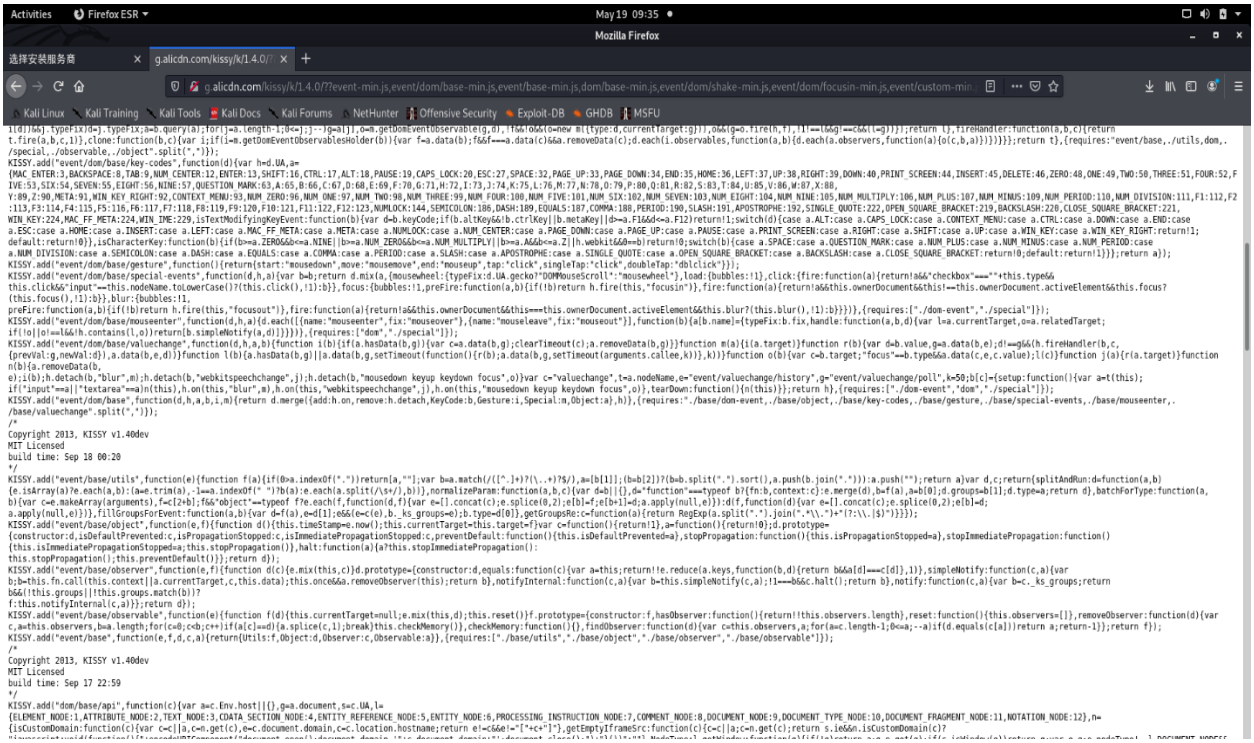

Activities
com-sittinglittleduck-DirBuster-Start
May 18 10:10
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://47.254.177.101:443/
Scan Information Results - List View: Dirs: 0 Files: 2 Results - Tree View Errors: 47887
Directory Stucture Response Code Response Size
/ 302 587
proxy.html 200 305
robots.txt 200 309
Current speed: 0 requests/sec
(Select and right click for more options)
Average speed: (T) 28, (C) 0 requests/sec
Parse Queue Size: 0
Total Requests: 1323199/1323289
Current number of running threads: 5000
5000
Change
Time To Finish: ~
Back
Pause
Stop
Report
Program running again

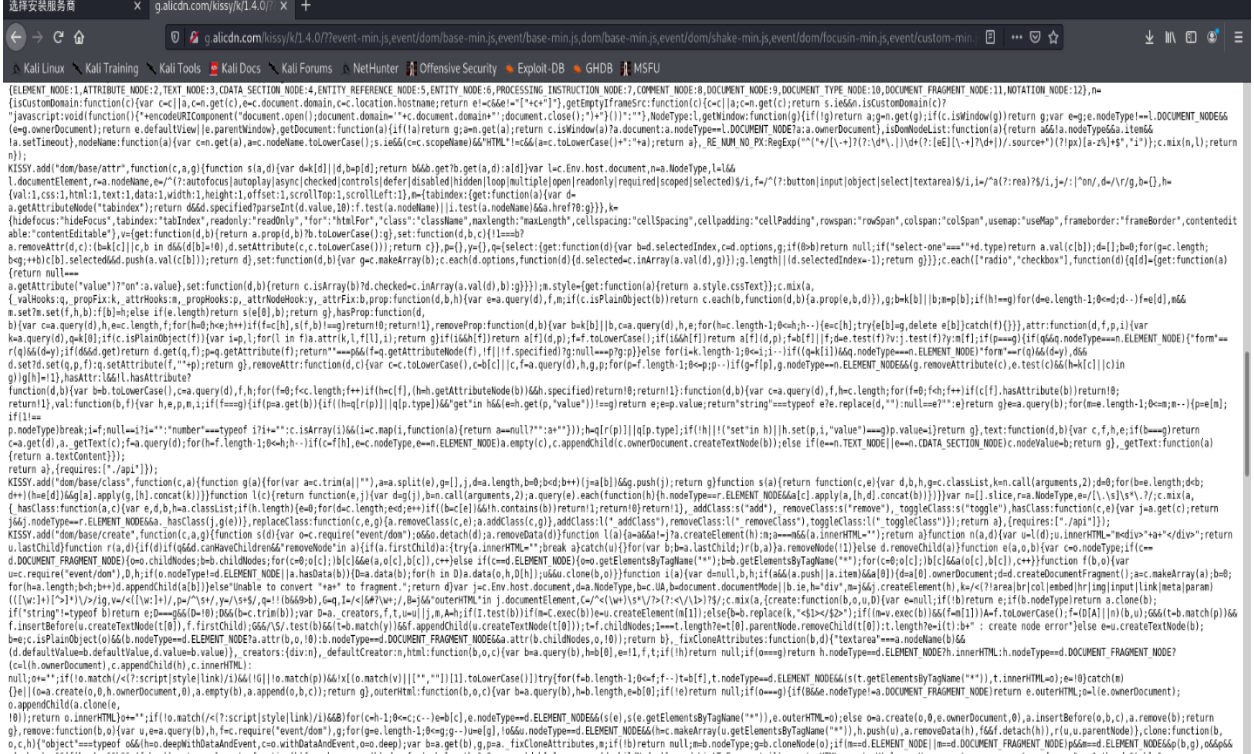
First open the proxy.html file

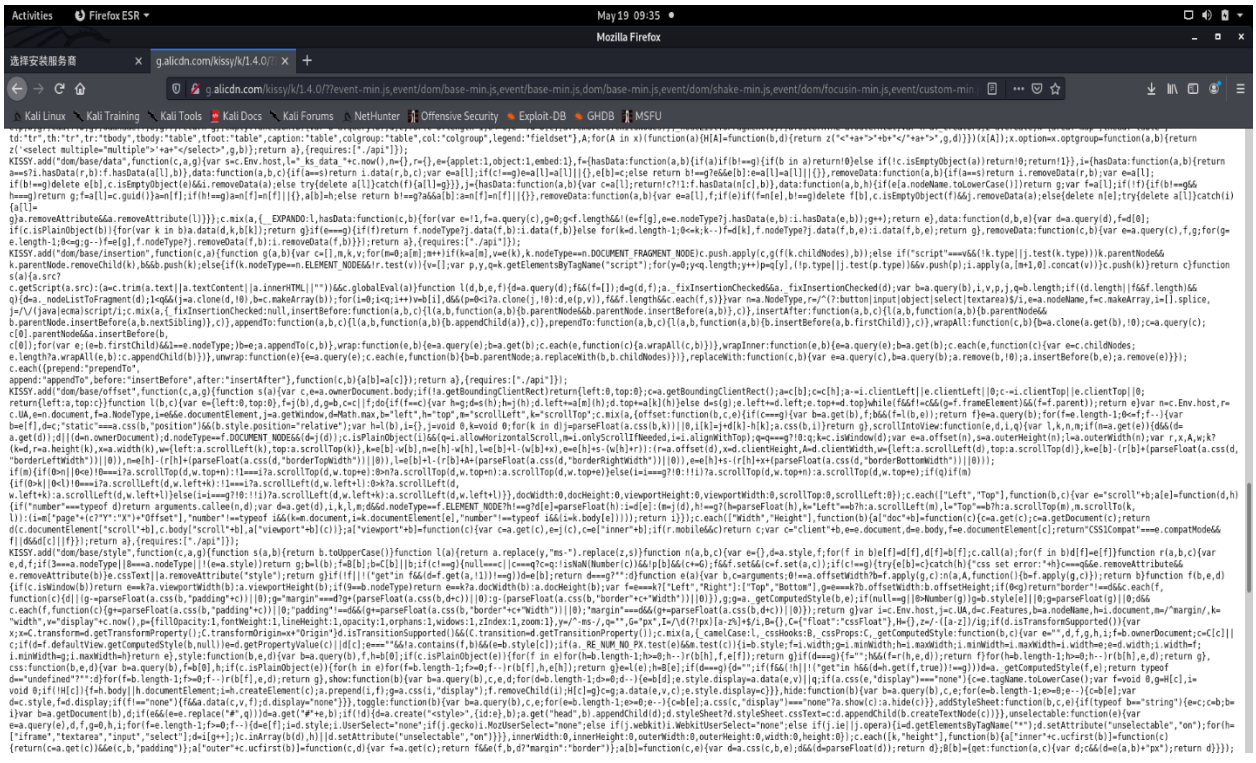


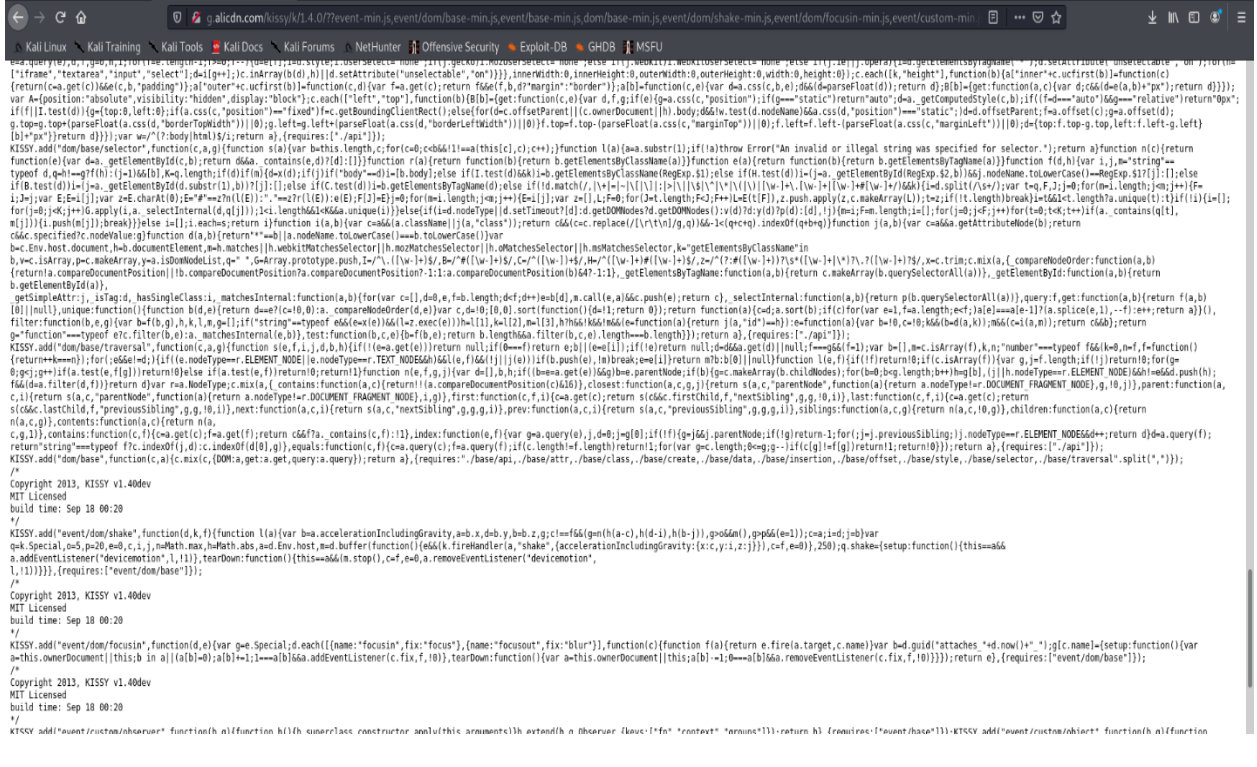
I then went to Inspect Elements and found some JavaScript files through that src link. These files are from a subdomain of the aliexpress.com domain.

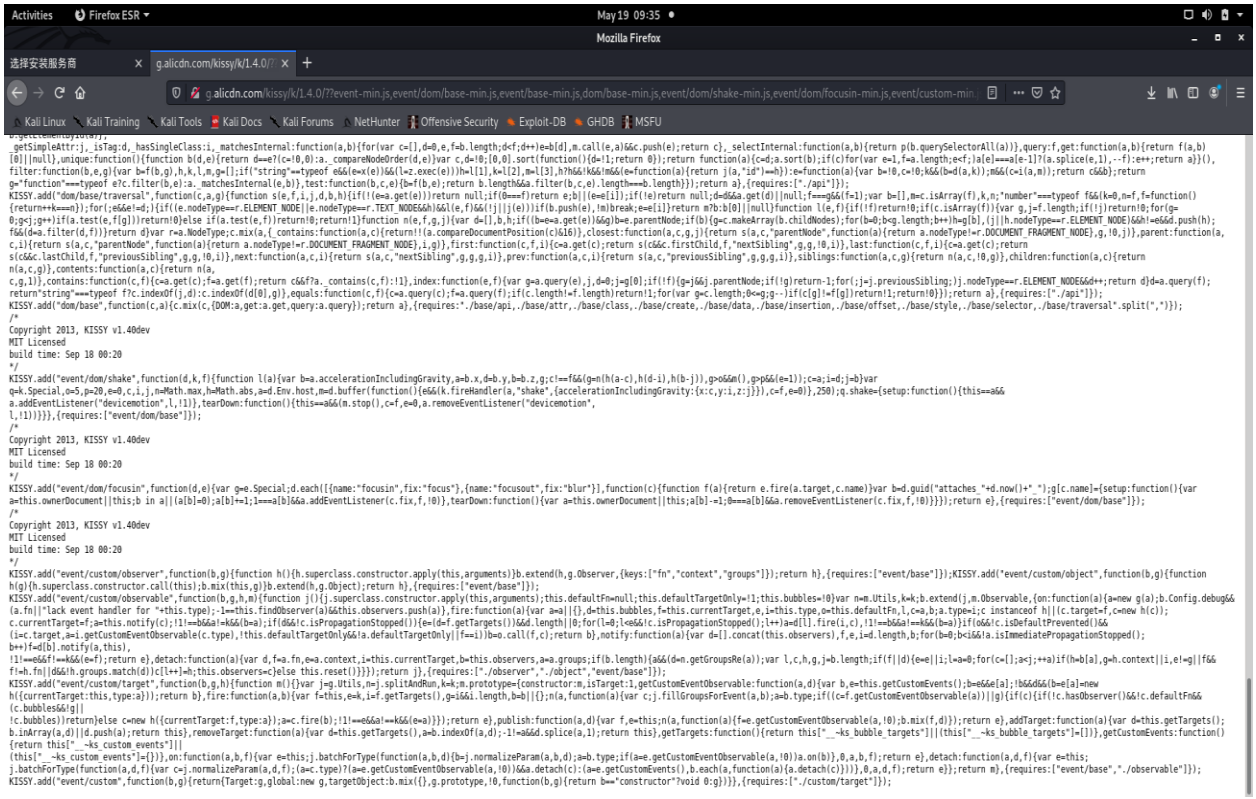



Activities
Firefox ESR
May 19 09:35
Mozilla Firefox
选择安装服务商
g.alicdn.com/kissy/k/1.4.0/??event-min.js,event/dom/base-min.js,event/base-min.js,dom/base-min.js,event/dom/shake-min.js,event/dom/focusin-min.js,event/custom-min
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU

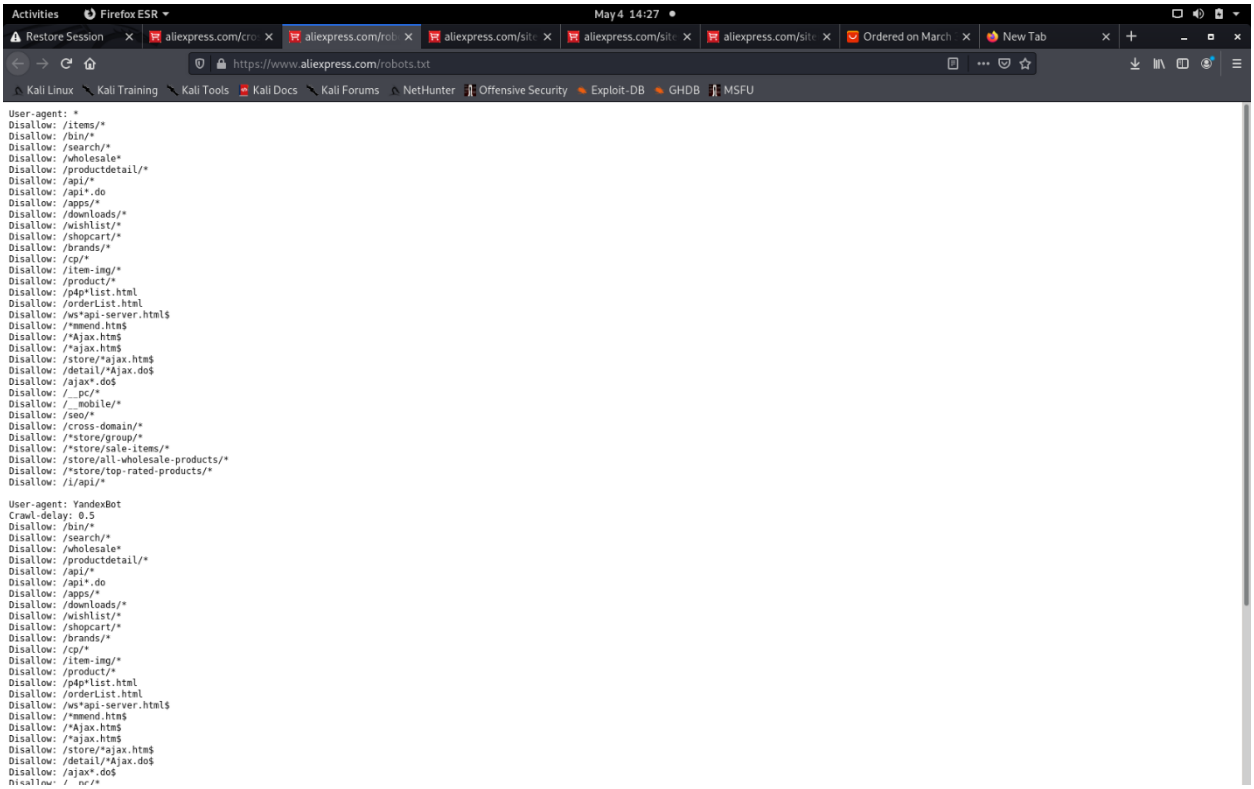

Activities
Firefox ESR
May 19 09:35
Mozilla Firefox
选择安装服务商
g.alicdn.com/kissy/k/1.4.0/??event-min.js,event/dom/base-min.js,event/base-min.js,dom/base-min.js,event/dom/shake-min.js,event/dom/focusin-min.js,event/custom-min
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU


Activities
Firefox ESR
May 19 09:35
Mozilla Firefox
选择安装服务商
g.alicdn.com/kissy/k/1.4.0/??event-min.js,event/dom/base-min.js,event/base-min.js,dom/base-min.js,event/dom/shake-min.js,event/dom/focusin-min.js,event/custom-min
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU


Activities
Firefox ESR
May 19 09:35
Mozilla Firefox
选择安装服务商
g.alicdn.com/kissy/k/1.4.0/??event-min.js,event/dom/base-min.js,event/base-min.js,dom/base-min.js,event/dom/shake-min.js,event/dom/focusin-min.js,event/custom-min
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU

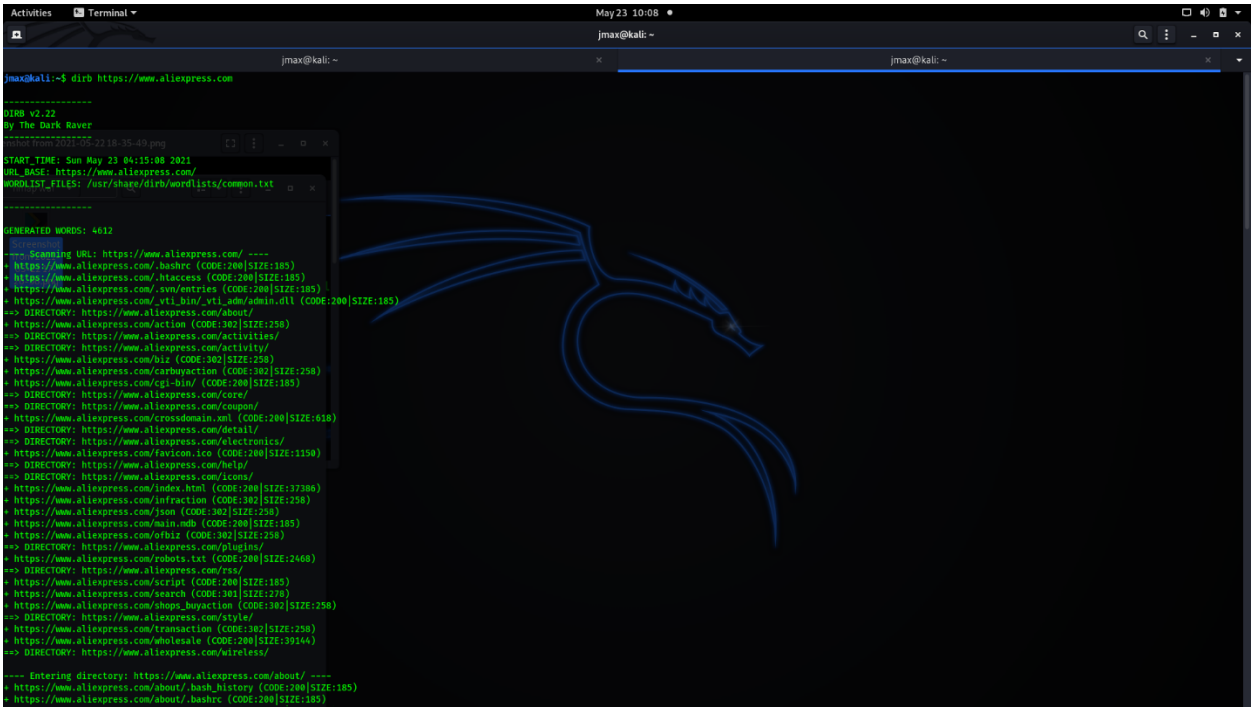


Then I opened the robots.txt file, which contains AliExpress's user-agents and several sub-directories that are unique to them.



2. Dirb Tool

DIRB is a content scanner for the web. It searches for Web Objects that are already present (and/or hidden). It operates by executing a dictionary-based attack on a web server and then evaluating the response. For ease of use, DIRB comes with a collection of preconfigured attack wordlists, but you can also use your own.



Vulnerability Analyzing Phrase & Recommendation

Netsparker

According to this web audit, to scan the OWASP Top 10 vulnerabilities of our selected domain and sub domains. I used Netsparker Professional to scan the OWASP Top 10 vulnerabilities.

Netsparker is an automated online application security scanner that allows you to scan websites, web applications, and web services for security issues while remaining fully customisable. Netsparker can scan any web application, independent of the platform or programming language used to create it.

SQL injection, Cross-site Scripting (XSS), and other web application problems are also automatically detected. We may create a Details report, a Summary report, and an OWASP Top 10 Security Risk report for our scope. Netsparker analyzed the domains below, and the vulnerabilities were categorised as OWASP Top 10.

https://www.aliexpress.com

Vulnerabilities By OWASP 2017

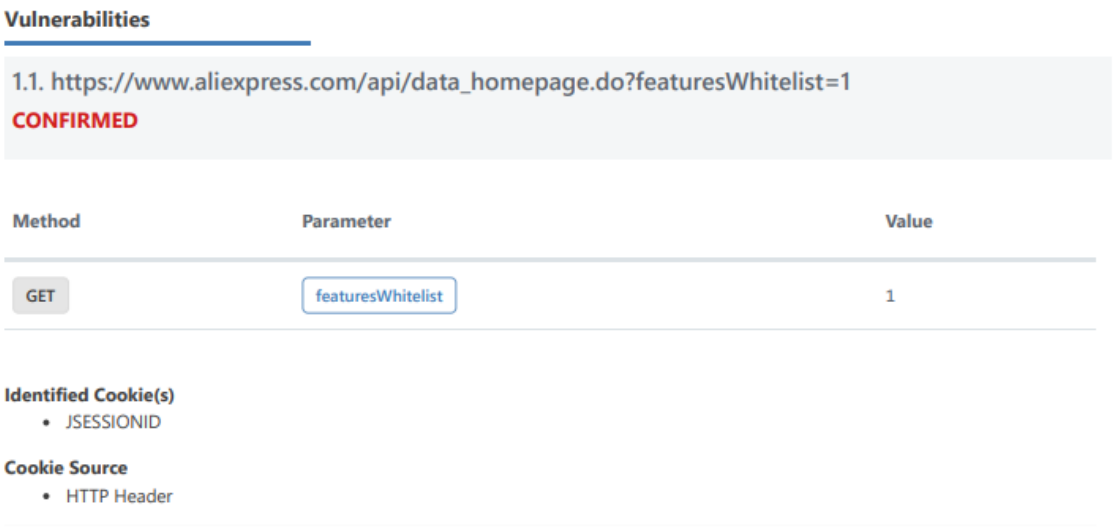
CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A3 - SENSITIVE DATA EXPOSURE				
	Session Cookie Not Marked as Secure	GET	https://www.aliexpress.com/api/data_homepage.do?featuresWhitelist=1	HIGH
	Weak Ciphers Enabled	GET	https://www.aliexpress.com/	MEDIUM
	Cookie Not Marked as Secure	GET	https://www.aliexpress.com/api/load_ams_path.htm?path=aliexpress.com%2Fcommon%2F@langField%2Fae-footer.htm	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://www.aliexpress.com/	LOW
	Passive Mixed Content over HTTPS	GET	https://www.aliexpress.com/category/100005823/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://www.aliexpress.com/	BEST PRACTICE
	Referrer-Policy Not Implemented	GET	https://www.aliexpress.com/	BEST PRACTICE

SENSITIVE DATA EXPOSURE

- **Session Cookie Not Marked as Secure**
- Method : GET
- Severity : HIGH

Netsparker discovered an HTTPS session cookie that was not tagged as secure.

This means that an attacker who successfully intercepts communications after a successful man-in-the-middle assault could potentially steal the cookie. It's worth noting that Netsparker deduced that the cookie in question is session-related based on its name.



Impact

This cookie will be transmitted over a HTTP connection, therefore an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to your website

Request

```
GET /api/data_homepage.do?featuresWhitelist=1 HTTP/1.1
Host: www.aliexpress.com
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5,en-US,en;q=0.9
Cache-Control: no-cache
Cookie: ali_apache_id=11.176.96.1.1622108561499.192327.6; xman_us_f=x_locale=en_US&x_l=0&x_c_chg=1&x_as
_i=%7B%22aeuCID%22%3A%22%22%2C%22cookieCacheEffectTime%22%3A1622108861517%2C%22isCookieCache%22%3A%22Y%
22%2C%22ms%22%3A%220%22%7D&acs_rt=2c8c5a0aa91644e88951b7ca4fa13571; AKA_A2=A; JSESSIONID=917BE72D4BAD21
9A494AC9CFA292E7EA; acs_usuc_t=x_csrf=3g6_0ha_32sd&acs_rt=2c8c5a0aa91644e88951b7ca4fa13571; aep_usuc_f=
site=glo_n&c_tp=USD&region=NL&b_locale=en_US; intl_common_forever=oSYJitXde7oguPgpCi1D7ecq5BPUuQ7bIuVCz
GIX7gfbl7Utun+pPQ==; intl_locale=en_US; xman_f=GjpqAmnoj6VaT/arM8AbM31YV7S11uFEv53hFSJR/sbmH/QgxZHU+6dR
Grwhfafw2vYih2VhakvlF9eprBNd19F75wlT7Td0F4m1HTJ2gpSnL3Bhn4jp+w==; xman_t=D3HVjjZG5uKe253JVPv6goHmuTWt+7
VsAV10u3kKX2vPCexh+CnqXEn/oDyGHGzk
Referer: https://www.aliexpress.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 521.4061 Total Bytes Received : 59244 Body Length : 57698 Is Compressed : No

```
HTTP/1.1 200 OK
X-Application-Context: ae-buyer-homepage-f:prod:7001
EagleEye-TraceId: 0b0a5568162210857131455 13e4959
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Access-Control-Allow-Origin: https://hz.aliexpress.com
Set-Cookie: xman_us_f=x_locale=en_US&x_l=0&x_c_chg=1&x_as_i=%7B%22aeuCID%22%3A%22%22%2C%22cookieCacheEf
fectTime%22%3A1622108861517%2C%22isCookieCache%22%3A%22Y%22%2C%22ms%22%3A%220%22%7D&acs_rt=2c8c5a0aa916
44e88951b7ca4fa13571; Domain=.aliexpress.com; Expires=Tue, 14-Jun-2089 12:56:58 GMT; Path=/; Secure; Sa
meSite=None
Set-Cookie: JSESSIONID=A05BAC93567DAD2906D3745F87604565; Path=/; HttpOnly
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Strict-Transport-Security: max-age=31536000
Transfer-Encoding: chunked
P3P: CP="CAO PSA OUR"
X-Akamai-Fwd-Auth-SHA: BF2AE0D9BB1BD77A56F48EB42B1788E0398CAAB83E0E37F2582466C9018E018B
Server: Tengine/Aserver
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
Connection: Transfer-Encoding
Expires: 0
X-Frame-Options: DENY
Vary: Accept-Encoding
Timing-Allow-Origin: *
X-Akamai-Fwd-Auth-Sign: pJeLZyn5QivxAPhh0DfvVJJcqwzFQrdxlza7IvL4cN5XObnU3wJDFHZXI4roXSGNGZ0tBpYwlVB/H18
8S0BM9R25WsGelk1+IblCtX8PPBk=
Server-Timing: edge; dur=1
Server-Timing: origin; dur=360
Server-Timing: cdn-cache; desc=MISS
X-Akamai-Fwd-Auth-Data: 265233562, 23.43.48.222, 1622108571, 212.104.236.90
Content-Type: appl
…
08861517%2C%22isCookieCache%22%3A%22Y%22%2C%22ms%22%3A%220%22%7D&acs_rt=2c8c5a0aa91644e88951b7ca4fa1357
1; Domain=.aliexpress.com; Expires=Tue, 14-Jun-2089 12:56:58 GMT; Path=/; Secure; SameSite=None
Set-Cookie: JSESSIONID=A05BAC93567DAD2906D3745F87604565; Path=/; HttpOnly

Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Strict-Transport-Security: max-age=31536000
Transfer-Encoding: chunked
P3P: CP="CAO PSA OUR"
X-Akamai-Fwd-Auth-SHA: BF2AE0D9BB1BD77
…
```

Actions to Take

1. See the recommendation for solution.

2. Mark all cookies used within the application as secure. (If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure.)

Recommendations

Mark all cookies used within the application as secure.

Required Skills for Successful Exploitation

To exploit this issue, the attacker needs to be able to intercept traffic. This generally requires local access to the web server or to the victim's network. Attackers need to understand layer 2 and have gained access to a system between the victim and the web server.

SECURITY MISCONFIGURATION

- **HTTP Strict Transport Security (HSTS) Errors and Warnings**
- Method : GET
- Severity : Medium

Impact

The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

Recommendations

Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Browser vendors declared:

- ✓ Serve a valid certificate

- ✓ If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:
  - In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists
  -
- ✓ Serve an HSTS header on the base domain for HTTPS requests:
  - The max-agemust be at least 31536000 seconds (1 year)
  - The includeSubDomainsdirective must be specified
  - The preloaddirective must be specified
  - If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

USING COMPONENTS WITH KNOWN VULNERABILITIES

- **[Possible] BREACH Attack Detected**
- Method : GET
- Severity : Medium

Netsparker detected that BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) attack is possible on this website.

Due to elements that make BREACH attack possible, SSL/TLS protected traffic remains vulnerable and can be attacked to uncover information from the website.

Regardless of which version of SSL/TLS you use, attacks are still possible. Attacks do not require TLS-layer compression and they can work against any cipher suite.

Impact

Even if you use an SSL/TLS protected connection, an attacker can still view the victim's encrypted traffic and cause the victim to send HTTP requests to the vulnerable web server (by using invisible frames). Following these steps, an attacker could steal information from the website and do the following:

- Inject partial plaintext they have uncovered into a victim's requests.
- Measure the size of encrypted traffic.

Recommendations

Netsparker reported a Possible BREACH Attack issue because the target web page meets the following conditions that facilitate it:

- Served from a server that uses HTTP-level compression (ie. gzip)
- Reflects user-input in the HTTP response bodies
- Contains sensitive information (such as a CSRF token) in HTTP response bodies

To mitigate the issue, we recommend the following solutions:

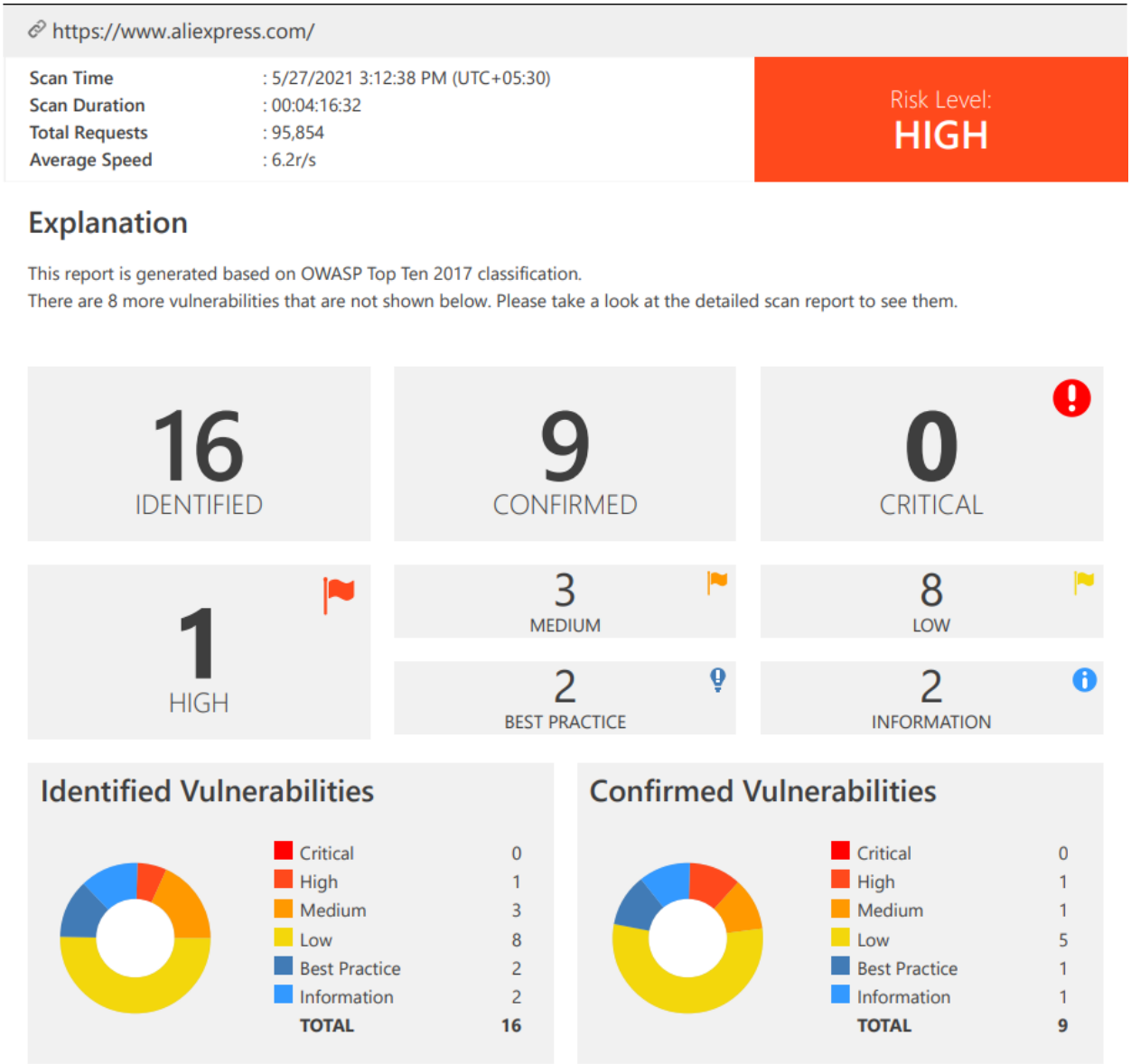
1. If possible, disable HTTP level compression

2. Separate sensitive information from user input

3. Protect vulnerable pages with CSRF token. The SameSite Cookie attribute will mitigate this issue, because to exploit this issue an attacker forces the victim to visit a target website using invisible frames. With the SameSite cookie attribute added, cookies that belong to the target won't be sent with a request that does not include top level navigation.

4. Hide the length of the traffic by adding a random number of bytes to the responses.
5. Add in a rate limit, so that the page maximum is reached five times per minute.

Overview Summary:



https://www.2014.aliexpress.com

Vulnerabilities By OWASP 2017

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A3 - SENSITIVE DATA EXPOSURE				
	Weak Ciphers Enabled	GET	https://2014.aliexpress.com/	MEDIUM
	Insecure HTTP Usage	GET	http://2014.aliexpress.com/	MEDIUM
	Cookie Not Marked as Secure	GET	https://2014.aliexpress.com/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://2014.aliexpress.com/	LOW
	Passive Mixed Content over HTTPS	GET	https://2014.aliexpress.com/wholesale?SearchText=3&catId=3&initiative_id=3&origin=y	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://2014.aliexpress.com/	BEST PRACTICE
	Referrer-Policy Not Implemented	GET	https://2014.aliexpress.com/store/	BEST PRACTICE

SENSITIVE DATA EXPOSURE

- **Weak Ciphers Enabled**
- Method : GET
- Severity : Medium

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Vulnerabilities

2.1. https://2014.aliexpress.com/

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xC009)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xC00A)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xC023)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC024)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

```
[NETSPARKER] SSL Connection
```

Actions to Take

1. For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

a.Click Start, click Run, type `regedt32`or type `regedit`, and then click OK.

b.In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`

c.Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

Recommendations

Configure your web server to disallow using weak ciphers

Overview Summary

https://2014.aliexpress.com/

Scan Time	: 5/26/2021 6:48:58 PM (UTC+05:30)
Scan Duration	: 00:00:40:36
Total Requests	: 41,885
Average Speed	: 17.2r/s

Risk Level: MEDIUM

Explanation

This report is generated based on OWASP Top Ten 2017 classification.
There are 5 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

13 IDENTIFIED	7 CONFIRMED	0 CRITICAL
0 HIGH	3 MEDIUM	8 LOW
	2 BEST PRACTICE	0 INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	3
Low	8
Best Practice	2
Information	0
TOTAL	**13**

Confirmed Vulnerabilities

Critical	0
High	0
Medium	1
Low	5
Best Practice	1
Information	0
TOTAL	**7**

https://www.activities.aliexpress.com

Vulnerabilities By OWASP 2017

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A3 - SENSITIVE DATA EXPOSURE				
	Weak Ciphers Enabled	GET	https://activities.aliexpress.com/	MEDIUM
	Insecure HTTP Usage	GET	http://activities.aliexpress.com/	MEDIUM
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://activities.aliexpress.com/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://activities.aliexpress.com/	BEST PRACTICE
	Referrer-Policy Not Implemented	GET	https://activities.aliexpress.com/	BEST PRACTICE

SENSITIVE DATA EXPOSURE

- **Insecure HTTP Usage**
- Method : GET
- Severity : Medium

Vulnerabilities

3.1. http://activities.aliexpress.com/

Certainty

Request

```
GET / HTTP/1.1
Host: activities.aliexpress.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Netsparker identified that the target website allows web browsers to access to the website over HTTP and doesn't redirect them to HTTPS.

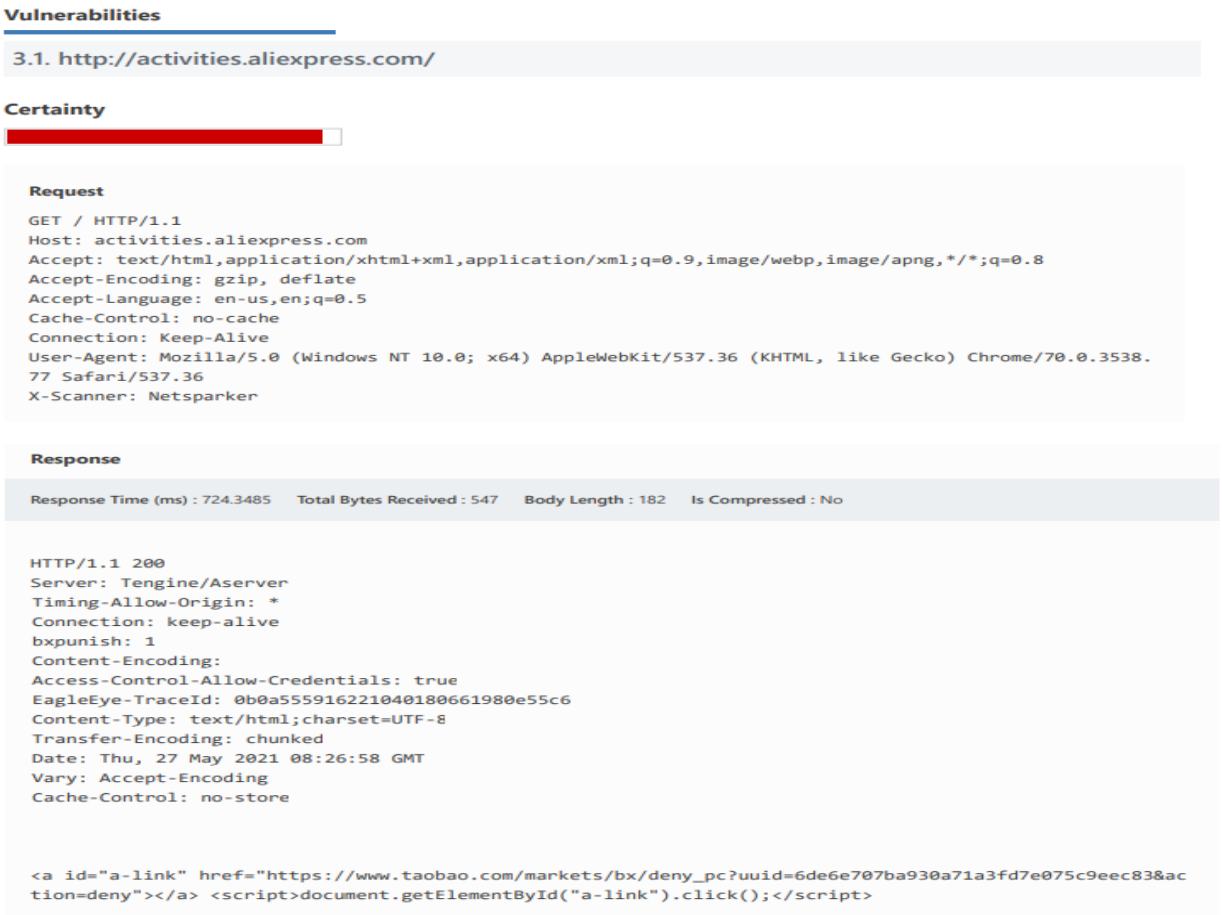
HSTS is implemented in the target website however HTTP requests are not redirected to HTTPS. This decreases the value of HSTS implementation significantly.

For example visitors who haven't visited the HTTPS version of the website previously will not be able to take advantage of HSTS.

Impact

Users will not be able to take advantage of HSTS which almost renders the HSTS implementation useless. Not having HSTS will make MITM attacks easier for attackers.

If there is a client side redirect to HTTPS version of the website (via JavaScript or Meta tags) then you can ignore this vulnerability.



Recommendations

Configure your webserver to redirect HTTP requests to HTTPS.

i.e for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# redirect all HTTP to HTTPS
<VirtualHost *:80>
	ServerAlias *
	RewriteEngine On
	RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>
```

Overview Summary

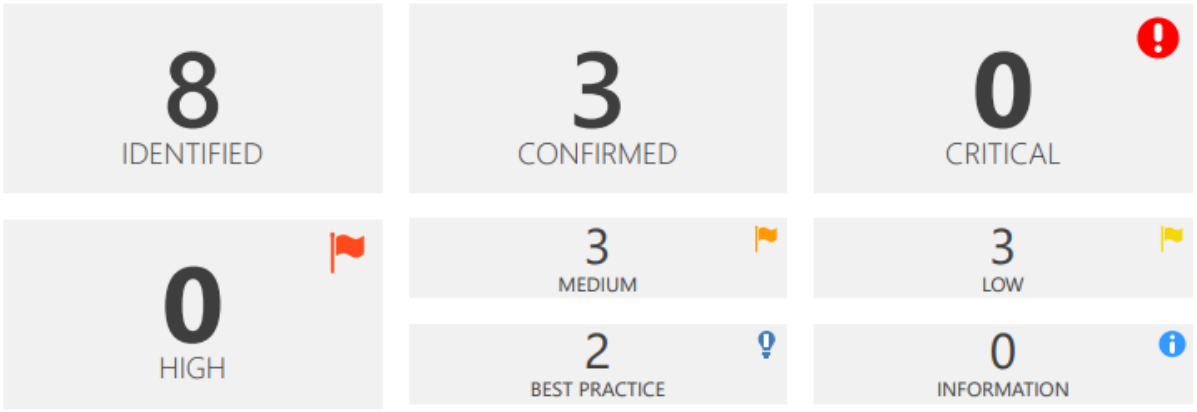
https://activities.aliexpress.com/

Scan Time	: 5/27/2021 1:56:45 PM (UTC+05:30)
Scan Duration	: 00:00:02:47
Total Requests	: 701
Average Speed	: 4.2r/s

Risk Level: MEDIUM

Explanation

This report is generated based on OWASP Top Ten 2017 classification.
There is a vulnerability that is not shown below. Please take a look at the detailed scan report to see it.



Identified Vulnerabilities

Critical	0
High	0
Medium	3
Low	3
Best Practice	2
Information	0
TOTAL	**8**

Confirmed Vulnerabilities

Critical	0
High	0
Medium	1
Low	1
Best Practice	1
Information	0
TOTAL	**3**

https://www.ajax.aliexpress.com

A6 - SECURITY MISCONFIGURATION

	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://ajax.aliexpress.com/	MEDIUM
	Cookie Not Marked as HttpOnly	GET	https://ajax.aliexpress.com/.well-known/	LOW
	Misconfigured Access-Control-Allow-Origin Header	GET	https://ajax.aliexpress.com/	LOW
	Missing X-Frame-Options Header	GET	https://ajax.aliexpress.com/	LOW

SECURITY MISCONFIGURATION

- **HTTP Strict Transport Security (HSTS) Errors and Warnings**
- Method : GET
- Severity : Medium

Vulnerabilities

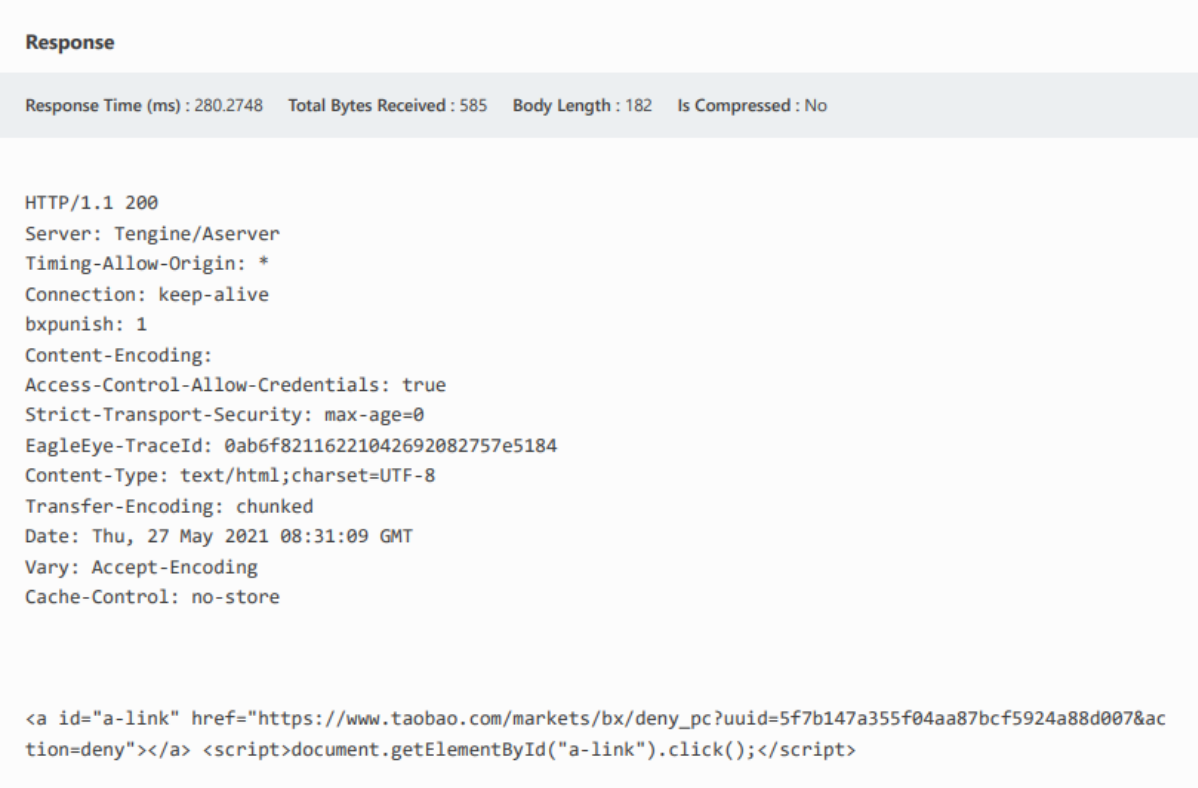
2.1. https://ajax.aliexpress.com/

Error	Resolution
HSTS is explicitly disabled.	Remove header if not necessary.
preload directive not present	Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list.

Certainty

Request

```
GET / HTTP/1.1
Host: ajax.aliexpress.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```



Recommendations

Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that

browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this

list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust

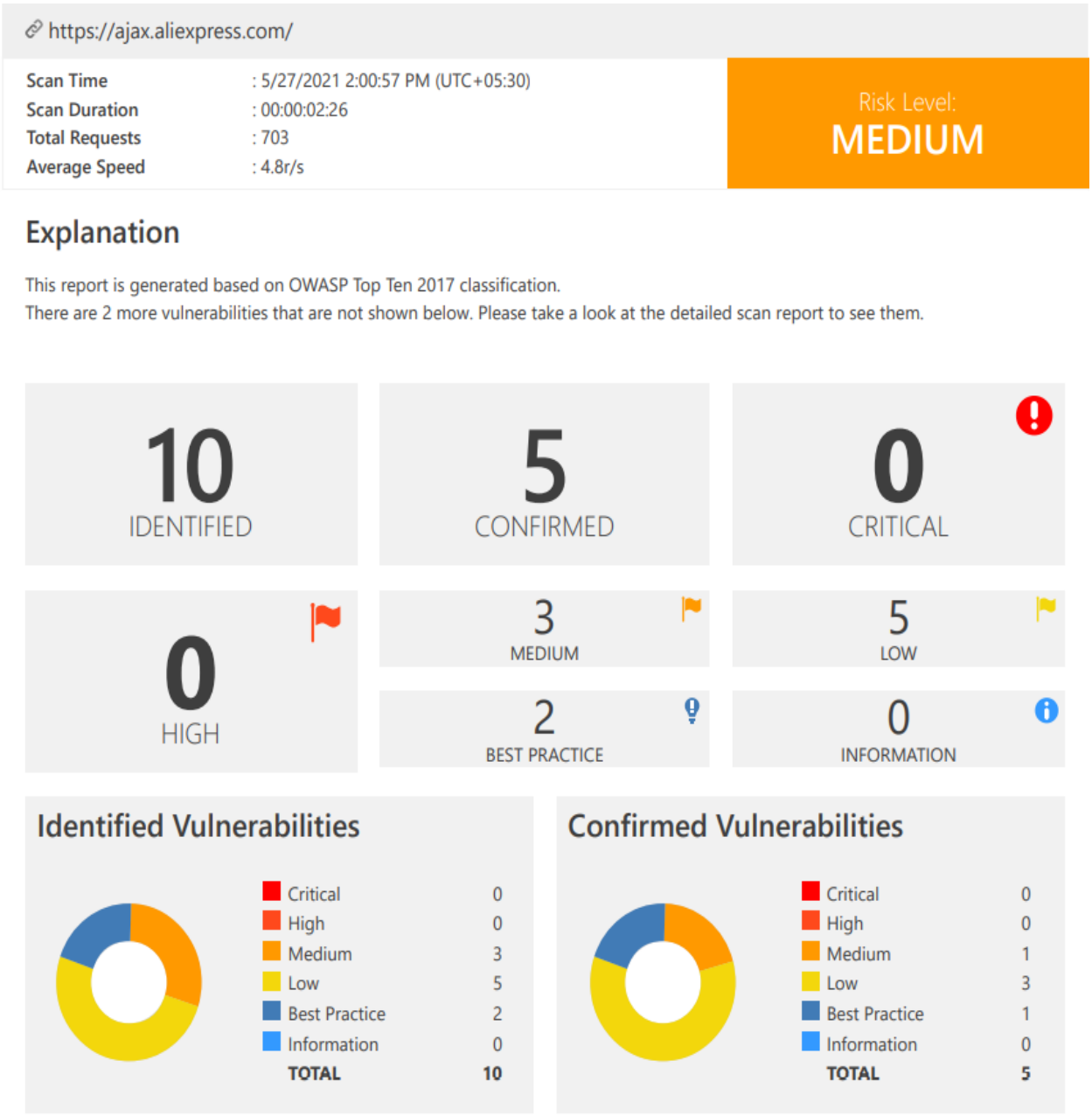
On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the

conditions required to enter the browser's preload list.

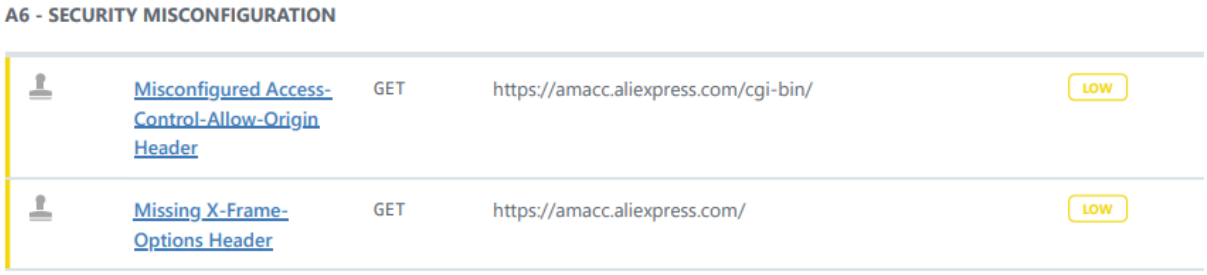
Browser vendors declared:

- Serve a valid certificate
- If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:
    - In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists

- Serve an HSTS header on the base domain for HTTPS requests:
  - The max-agemust be at least 31536000 seconds (1 year)
  - The includeSubDomainsdirective must be specified
  - The preloaddirective must be specified
  -
  - If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)



https://www.amacc.aliexpress.com



SECURITY MISCONFIGURATION

- **Missing X-Frame Options Header**
- Method : GET
- Severity : Low

Netsparker detected a missing X-Frame-Optionsheader which means that this website could be at risk of a clickjacking attack.

The X-Frame-OptionsHTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frameor an iframe. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Response

Response Time (ms) : 1606.2008 Total Bytes Received : 1444 Body Length : 1097 Is Compressed : No

```
HTTP/1.1 403 Forbidden
Server: Tengine
x-alicdn-da-ups-status: endOs,0,403
Connection: keep-alive
Via: cache34.l2cm10-9[37,0], cache5.in14[334,0]
Content-Encoding:
Timing-Allow-Origin: *
Content-Type: text/html
Transfer-Encoding: chunked
Date: Thu, 27 May 2021 08:10:04 GMT
Vary: Accept-Encoding
EagleId: a3b50b99162210300406162 79e

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>403 Forbidden</title></head>
<body bgcolor="white">
<h1>403 Forbidden</h1>
<p>You don't have permission to access the URL on this server. Sorry for the inconvenience.<br/>
Please report this message and include the following information to us.<br/>
Thank you very much!</p>
<table>
<tr>
<td>URL:</td>
<td>https://acs.aliexpress.com:4437/</td>
</tr>
<tr>
<td>Server:</td>
<td>aserver011027032120.center.na62</td>
</tr>
<tr>
<td>Date:</td>
<td>2021/05/27 16:10:04</td>
</tr>
</table>
<hr/>Powered by Tengine/Aserver</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

Impact

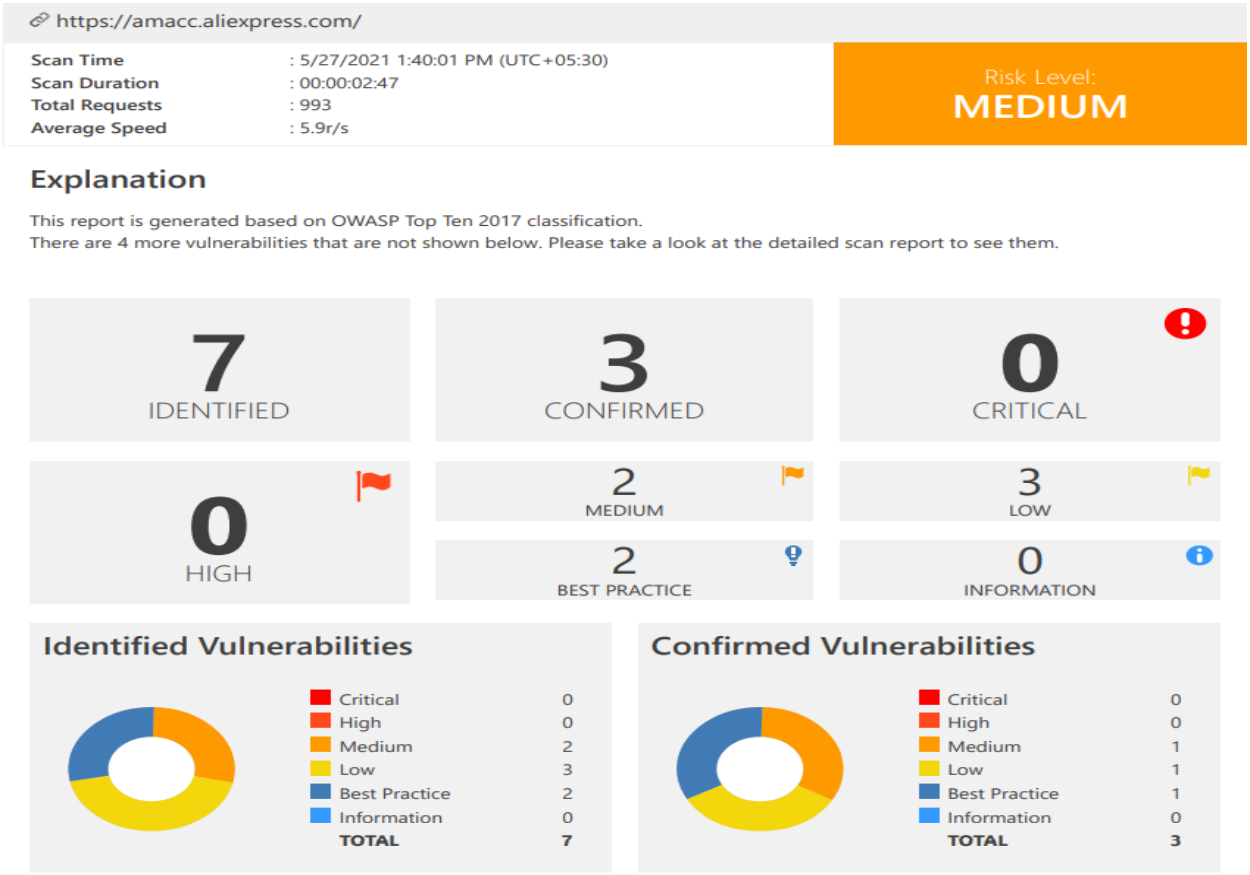
Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top-level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

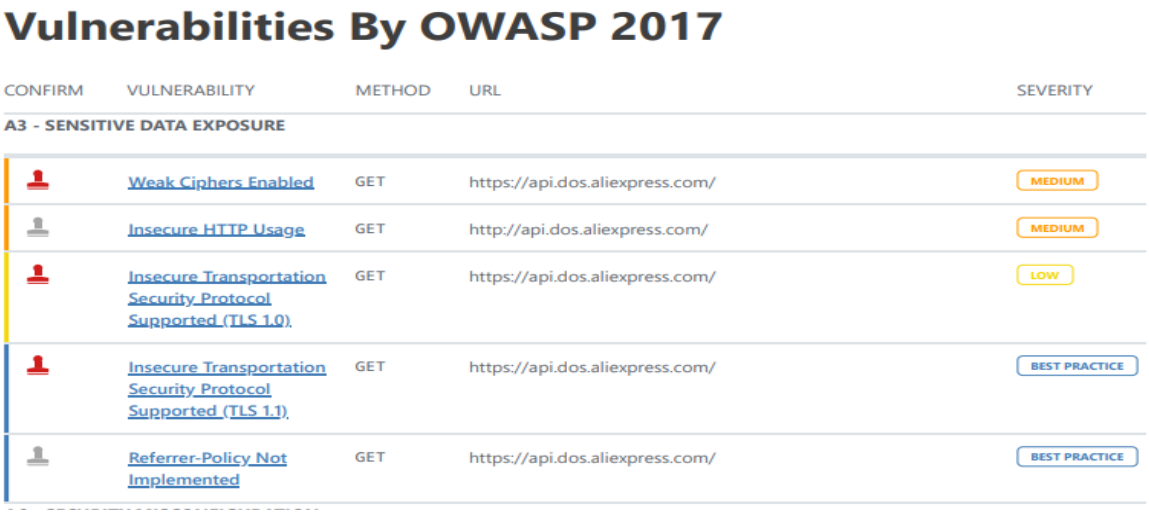
Recommendations

- ✓ Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
    - ✓ X-Frame-Options: DENYIt completely denies to be loaded in frame/iframe.
    - ✓ X-Frame-Options: SAMEORIGINIt allows only if the site which wants to load has a same origin.
    - ✓ X-Frame-Options: ALLOW-FROM URL It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.
- Employing defensive code in the UI to ensure that the current frame is the most top-level window.

Overview Summary

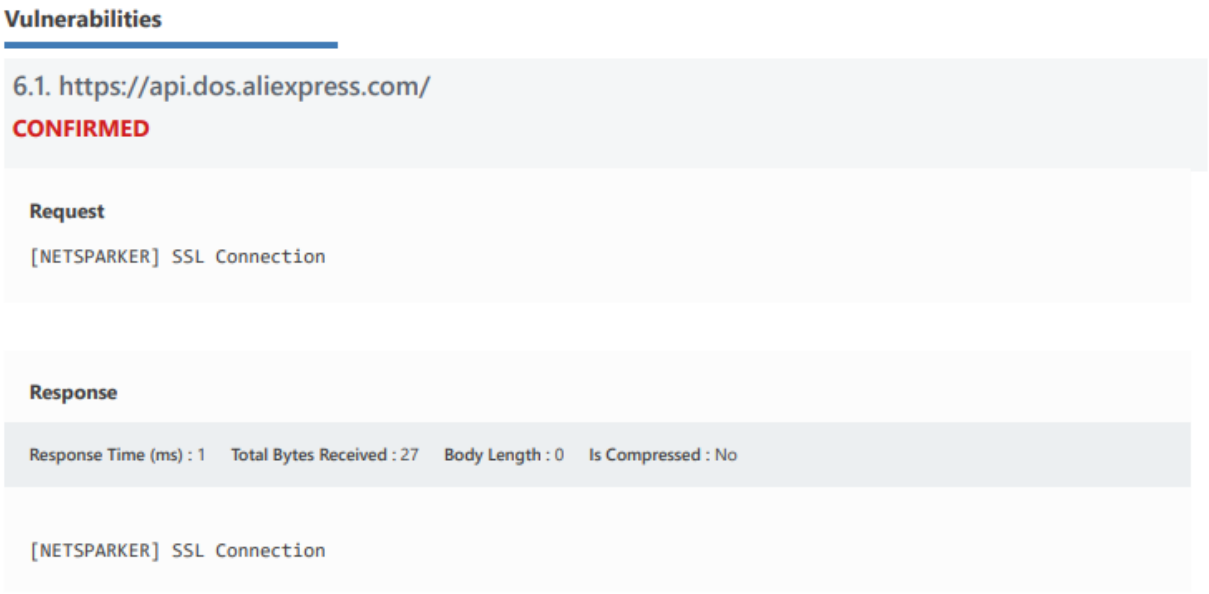


https://www.api.dos.aliexpress.com



SENSITIVE DATA EXPOSURE

- **HTTP Strict Transport Security (HSTS) Errors and Warnings**
- Method : GET
- Severity : Low



Netsparker detected that insecure transportation security protocol (TLS 1.0) is supported by your web server. TLS 1.0 has several flaws. An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS). Websites using TLS 1.0 are considered non-compliant by PCI since 30 June 2018.

Impact

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

Actions to Take

We recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher. See Recommendations section for more details.

Recommendations

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

  SSLProtocol +TLSv1.2

- For Nginx, locate any use of the directive ssl_protocols in the nginx.conffile and remove TLSv1.

  ssl_protocols TLSv1.2;

- For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**
  1. Click on Start and then Run, type `regedt32`or `regedit`, and then click OK.
  2. In Registry Editor, locate the following registry key or create if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\
```

  3. Locate a key named `Server`or create if it doesn't exist.
  4. Under the `Server`key, locate a DWORD value named `Enabled`or create if it doesn't exist and set its value to "0".
- For lighttpd, put the following lines in your configuration file:

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up
ssl.ec-curve = "secp384r1"
```

Overview Summary

https://api.dos.aliexpress.com/

Scan Time	: 5/27/2021 2:05:02 PM (UTC+05:30)
Scan Duration	: 00:00:02:26
Total Requests	: 704
Average Speed	: 4.8r/s

Risk Level:
MEDIUM

Explanation

This report is generated based on OWASP Top Ten 2017 classification.
There is a vulnerability that is not shown below. Please take a look at the detailed scan report to see it.

8 IDENTIFIED	3 CONFIRMED	0 CRITICAL
0 HIGH	3 MEDIUM	3 LOW
	2 BEST PRACTICE	0 INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	3
Low	3
Best Practice	2
Information	0
TOTAL	**8**

Confirmed Vulnerabilities

Critical	0
High	0
Medium	1
Low	1
Best Practice	1
Information	0
TOTAL	**3**

https://www.best.aliexpress.com

Vulnerabilities By OWASP 2017

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A3 - SENSITIVE DATA EXPOSURE				
	Session Cookie Not Marked as Secure	GET	https://best.aliexpress.com/ali/ae-traffic-kn-best-report/0.0.3/index.umd.js	HIGH
	Weak Ciphers Enabled	GET	https://best.aliexpress.com/	MEDIUM
	Cookie Not Marked as Secure	GET	https://best.aliexpress.com/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://best.aliexpress.com/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://best.aliexpress.com/	BEST PRACTICE
	Referrer-Policy Not Implemented	GET	https://best.aliexpress.com/	BEST PRACTICE

SENSITIVE DATA EXPOSURE

- **Session Cookie Not Marked as Secure**
- Method : GET
- Severity : High

Netsparker identified a session cookie not marked as secure, and transmitted over HTTPS. This means the cookie could potentially be stolen by an attacker who can successfully intercept the traffic, following a successful man-in-the-middle attack. It is important to note that Netsparker inferred from the its name that the cookie in question is session related.

Impact

This cookie will be transmitted over a HTTP connection, therefore an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to your website in order to steal the cookie.

Vulnerabilities

1.1. https://best.aliexpress.com/ali/ae-traffic-kn-best-report/0.0.3/index.umd.js

CONFIRMED

Identified Cookie(s)

- JSESSIONID

Cookie Source

- HTTP Header

Request

```
GET /ali/ae-traffic-kn-best-report/0.0.3/index.umd.js HTTP/1.1
Host: best.aliexpress.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: aep_usuc_f=site=glo&b_locale=en_US; e_id=pt60; _bl_uid=CkkntpzU6k7o899pmiOeeehfyhL8; acs_usuc_t
=acs_rt=0d731d9abe6448d7aed516ca76af1e5a&x_csrf=10zvh6wfbywoe; ali_apache_id=10.182.248.30.162210642110
6.449475.2; ali_apache_track=; ali_apache_tracktmp=; xman_f=PR51w7fvYhs0V6iaC8VvVlKFCRNLhSNj9nkTYG3CLAr
H3BFBBeTGJnvfaFjOlKI4588AVf6u7yZAHHzrs/YYvnblYTJD13zoHkC8Bii8fUILnflmQPoOHA==; xman_t=o9s07L4XN9E4YuwpX
WmNbDAJBGWhLM851XnmdM+Bpx+SqJqAt+I5ys6p509YIjyf; xman_us_f=x_l=0&acs_rt=0d731d9abe6448d7aed516ca76af1e5
a; isg=BO_vsmeI08msQtf1kLk0zF3ufgP5lEO2xtZ65gF8i95lUA9SCWTTBu0C1ljuMxsu; tfstk=c4khBuM3pXPCFyFiGpwIvFXo
ArvAwIQUW4uxQY-44uxhciCc715-HjdgzhvGN; l=eBTjmKaRjkv39ugtBOfanurza77OSIRYYuPzaNbMiOCPOB1B5uNPB6sHTLY6C3
MNhs_yR3rzBJrHBeYBq3xonxvT06AbdJMmn
Referer: https://best.aliexpress.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 567.1572 Total Bytes Received : 1181 Body Length : 0 Is Compressed : No

```
HTTP/1.1 404 Not Found
Set-Cookie: xman_us_f=x_locale=en_US&x_l=0&x_c_chg=1&acs_rt=0d731d9abe6448d7aed516ca76af1e5a; Domain=.a
liexpress.com; Expires=Tue, 14-Jun-2089 12:21:56 GMT; Path=/
Set-Cookie: intl_locale=en_US; Domain=.aliexpress.com; Path=/
Set-Cookie: aep_usuc_f=site=glo&c_tp=LKR&region=LK&b_locale=en_US; Domain=.aliexpress.com; Expires=Tue,
 14-Jun-2089 12:21:56 GMT; Path=/
Set-Cookie: intl_common_forever=FxOtZCYzx/0Bx7BMUV0+7DRKFfHfqfAiB8tp1Fzbywpo0zDZPXl3Ug==; Domain=.aliex
press.com; Expires=Tue, 14-Jun-2089 12:21:56 GMT; Path=/; HttpOnly
Set-Cookie: JSESSIONID=88CDC93AD1C81E20C6450D14543303F9; Path=/; HttpOnly

Expires: 0
X-Content-Type-Options: nosniff
Server: Tengine/Aserver
Pragma: no-cache
X-XSS-Protection: 1; mode=block
Content-Length: 0
X-Frame-Options: DENY
P3P: CP="CAO PSA OUR"
Location: https://best.aliexpress.com?lan=affiliate/home&&aff_platform=default&commercial_type=bestPage
Connection: keep-alive
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Application-Context: ae-traffic-affiliateweb-f:prod,us:7001
Date: Thu, 27 May 2021 09:07:49 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
```

Actions to Take

1. See the remedy for solution.

2. Mark all cookies used within the application as secure. (If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure.)

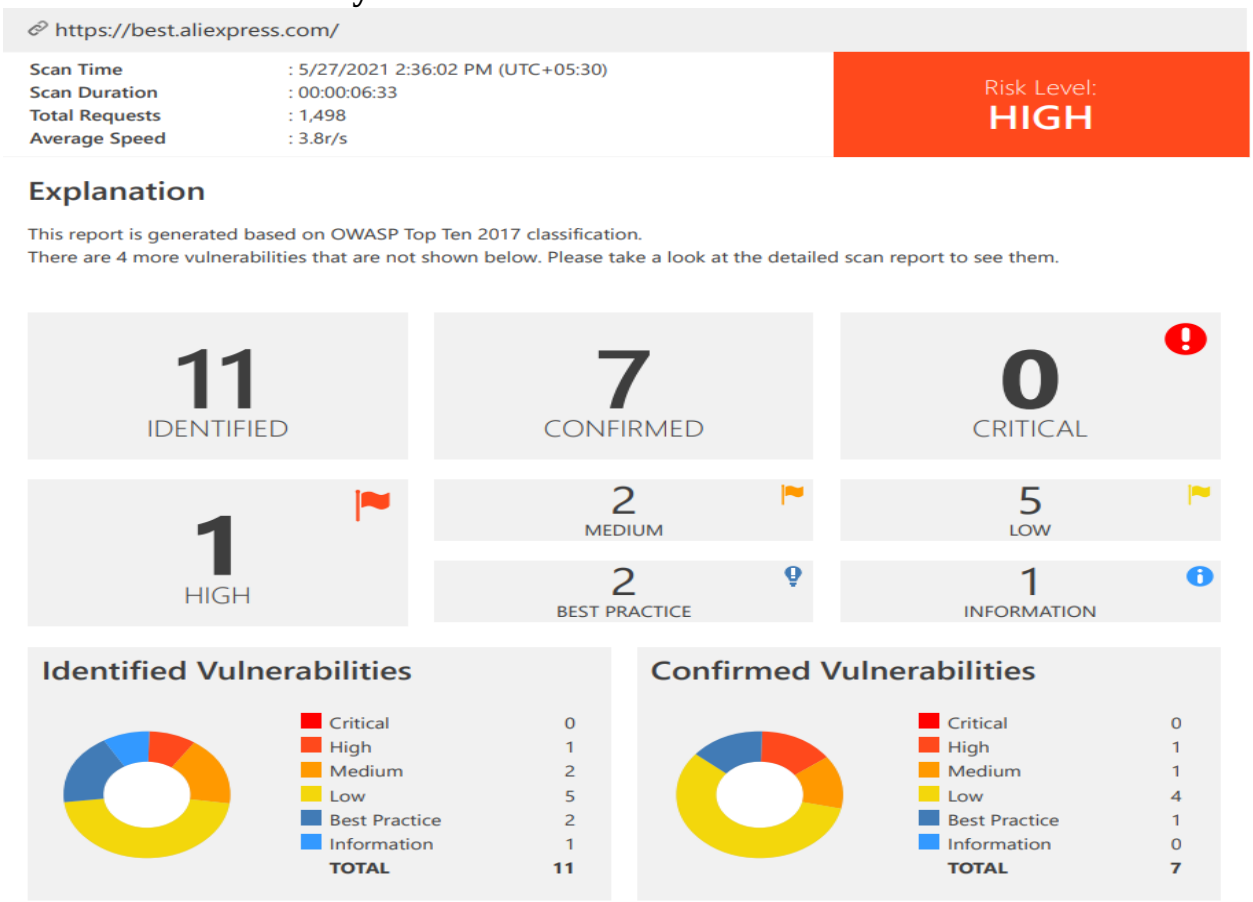
Recommendations

Mark all cookies used within the application as secure.

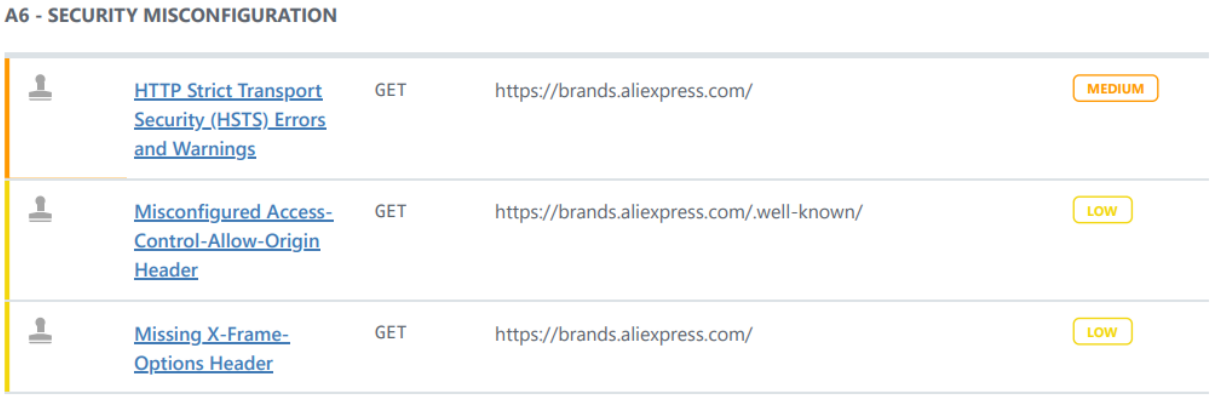
Required Skills for Successful Exploitation

To exploit this issue, the attacker needs to be able to intercept traffic. This generally requires local access to the web server or to the victim's network. Attackers need to understand layer 2 and have gained access to a system between the victim and the web server.

Overview Summary



https://www.brands.aliexpress.com



SECURITY MISCONFIGURATION

- **Missing X-Frame-Options Header**
- Method : GET
- Severity : Low

Netsparker detected a missing X-Frame-Optionsheader which means that this website could be at risk of a clickjacking attack.

The X-Frame-OptionsHTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frameor an iframe. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both. Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Vulnerabilities

4.1. https://brands.aliexpress.com/

Certainty

Request

```
GET / HTTP/1.1
Host: brands.aliexpress.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

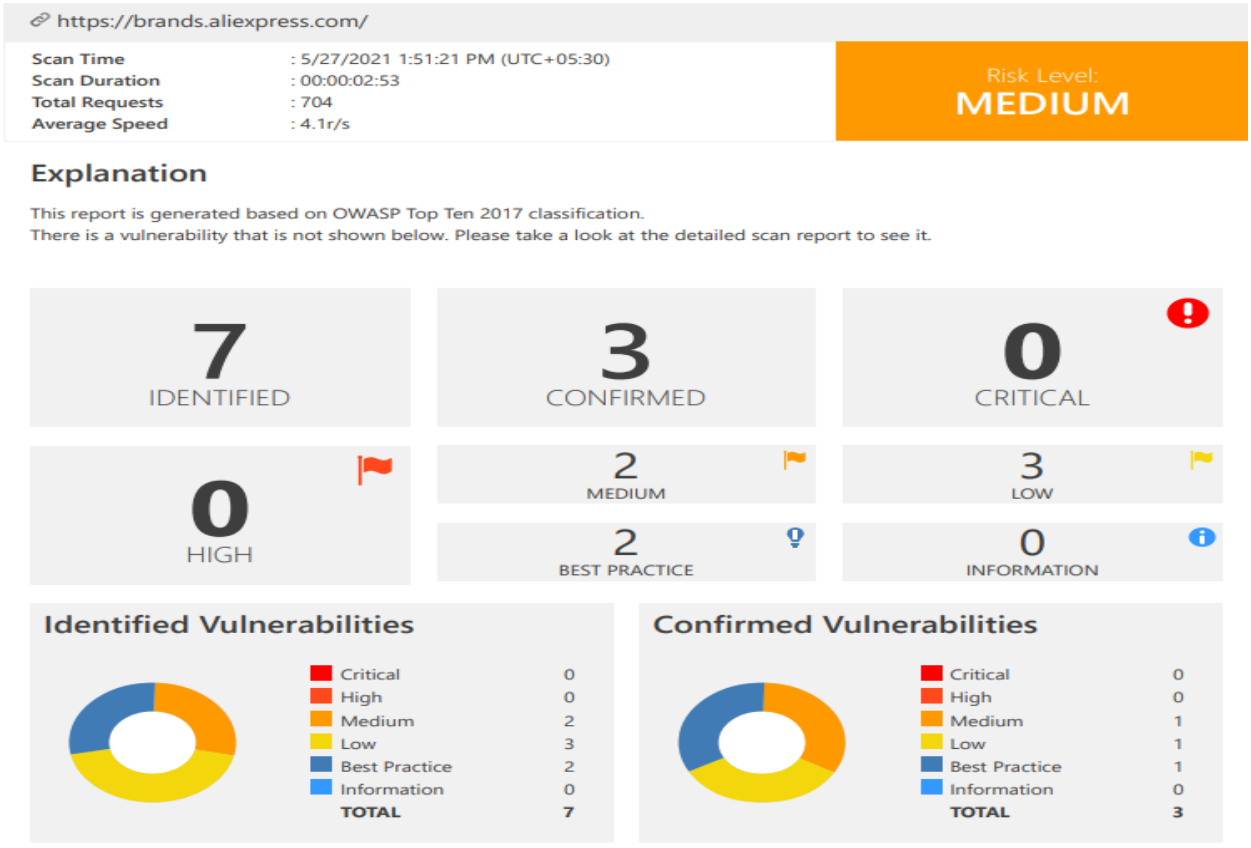
Response Time (ms) : 1496.0732 Total Bytes Received : 592 Body Length : 182 Is Compressed : No

```
HTTP/1.1 200
Server: Tengine/Aserver
Timing-Allow-Origin: *
Connection: keep-alive
bxpunish: 1
Content-Encoding:
Access-Control-Allow-Credentials: true
Strict-Transport-Security: max-age=31536000
EagleEye-TraceId: 0b0a5558162210368361121 67e62b4
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Date: Thu, 27 May 2021 08:21:23 GMT
Vary: Accept-Encoding
Cache-Control: no-store


<a id="a-link" href="https://www.taobao.com/markets/bx/deny_pc?uuid=0e39e0fa1340796f99cfc8b8ac587a9c&ac
tion=deny"></a> <script>document.getElementById("a-link").click();</script>
```

Recommendations

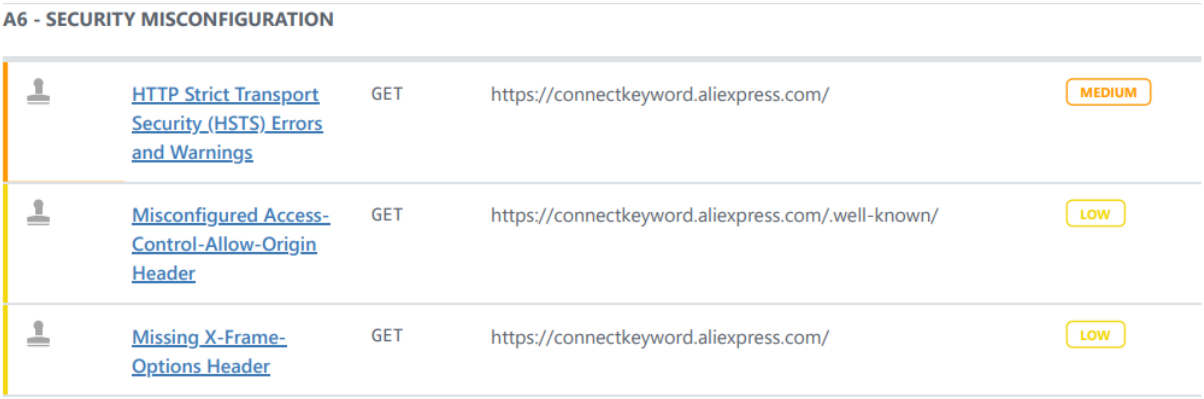
- ✓ Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
    - ✓ X-Frame-Options: DENYIt completely denies to be loaded in frame/iframe.
    - ✓ X-Frame-Options: SAMEORIGINIt allows only if the site which wants to load has a same origin.
    - ✓ X-Frame-Options: ALLOW-FROM URL It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.
- Employing defensive code in the UI to ensure that the current frame is the most top-level window.
- **Overview Summary**



https://www.connectkeyword.aliexpress.com

SECURITY MISCONFIGURATION

- **Misconfigured Access-Control-Allow-Origin Header**
- Method : GET
- Severity : Medium



Netsparker detected a possibly misconfigured Access-Control-Allow-Origin header in resource's HTTP response.

Cross-origin resource sharing (CORS) is a mechanism that allows resources on a web page to be requested outside the domain through XMLHttpRequest.

Unless this HTTP header is present, such "cross-domain" requests are forbidden by web browsers, per the same-origin security policy.

Impact

This is generally not appropriate when using the same-origin security policy. The only case where this is appropriate when using the same-origin policy is when a page or API response is considered completely public content and it is intended to be accessible to everyone.

Vulnerabilities

3.1. https://connectkeyword.aliexpress.com/.well-known/

Method	Parameter	Value
GET	URI-BASED	

Access-Control-Allow-Origin

- http://r87.com

Note

- Access-Control-Allow-Credentials is set to true which means credentials are sent via cross-domain requests and response can be read. If this is not intended, you can send this header for only trusted third parties.

Certainty

Recommendations

If this page is intended to be accessible to everyone, you don't need to take any action. Otherwise please follow the guidelines for different architectures below in order to set this header and permit outside domain.
Apache

- Add the following line inside either the <directory>, <location>, <files> or <virtualhost> sections of your server config (usually located in httpd.conf or apache.conf), or within a .htaccess file.

```
Header set Access-Control-Allow-Origin "domain"
```

IIS6

1. Open Internet Information Service (IIS) Manager
2. Right click the site you want to enable CORS for and go to Properties
3. Change to the HTTP Headers tab
4. In the Custom HTTP headers section, click Add
5. Enter Access-Control-Allow-Origin as the header name
6. Enter domainas the header value

IIS7

- Merge the following xml into the web.config file at the root of your application or site:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <system.webserver>
    <httpprotocol>
      <customheaders>
        <add name="Access-Control-Allow-Origin" value="domain" />
      </customheaders>
    </httpprotocol>
  </system.webserver>
</configuration>
```

ASP.NET

- If you don't have access to configure IIS, you can still add the header through ASP.NET by adding the following line to your source pages:

```
Response.AppendHeader("Access-Control-Allow-Origin", "domain");
```

Overview Summary

https://connectkeyword.aliexpress.com/

Scan Time	: 5/27/2021 2:23:27 PM (UTC+05:30)
Scan Duration	: 00:00:02:33
Total Requests	: 704
Average Speed	: 4.6r/s

Risk Level: MEDIUM

Explanation

This report is generated based on OWASP Top Ten 2017 classification.
There is a vulnerability that is not shown below. Please take a look at the detailed scan report to see it.

7 IDENTIFIED	3 CONFIRMED	0 CRITICAL
0 HIGH	2 MEDIUM	3 LOW
	2 BEST PRACTICE	0 INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	2
Low	3
Best Practice	2
Information	0
TOTAL	**7**

Confirmed Vulnerabilities

Critical	0
High	0
Medium	1
Low	1
Best Practice	1
Information	0
TOTAL	**3**

https://www.passport.aliexpress.com

SECURITY MISCONFIGURATION

- **Referrer-Policy Not Implemented**
- Method : Get
- Severity : Best Practice

Netsparker detected that no Referrer-Policy header implemented.

Referrer-Policy is a security header designed to prevent cross-domain Referer leakage.

Impact

Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.

The lack of Referrer-Policy header might affect privacy of the users and site's itself

Response

Response Time (ms) : 12129.2518 Total Bytes Received : 580 Body Length : 182 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Tengine/Aserver
Timing-Allow-Origin: *
Connection: keep-alive
Date: Thu, 27 May 2021 07:20:13 GMT
Content-Length: 176
Access-Control-Allow-Credentials: true
Strict-Transport-Security: max-age=0
EagleEye-TraceId: 0ab6f83a16221000131063577e2aa8
Content-Type: text/html;charset=UTF-8
Content-Encoding:
bxpunish: 1
Vary: Accept-Encoding
Cache-Control: no-store
```

```
<a id="a-link" href="https://www.taobao.com/markets/bx/deny_pc?uuid=c237fe18696f091856028c084b27d78a&ac
tion=deny"></a> <script>document.getElementById("a-link").click();</script>
```

Actions to Take

In a response header:

```
Referrer-Policy: no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading
```

In a META tag

```
<meta name="Referrer-Policy" value="no-referrer | same-origin"/>
```

In an element attribute

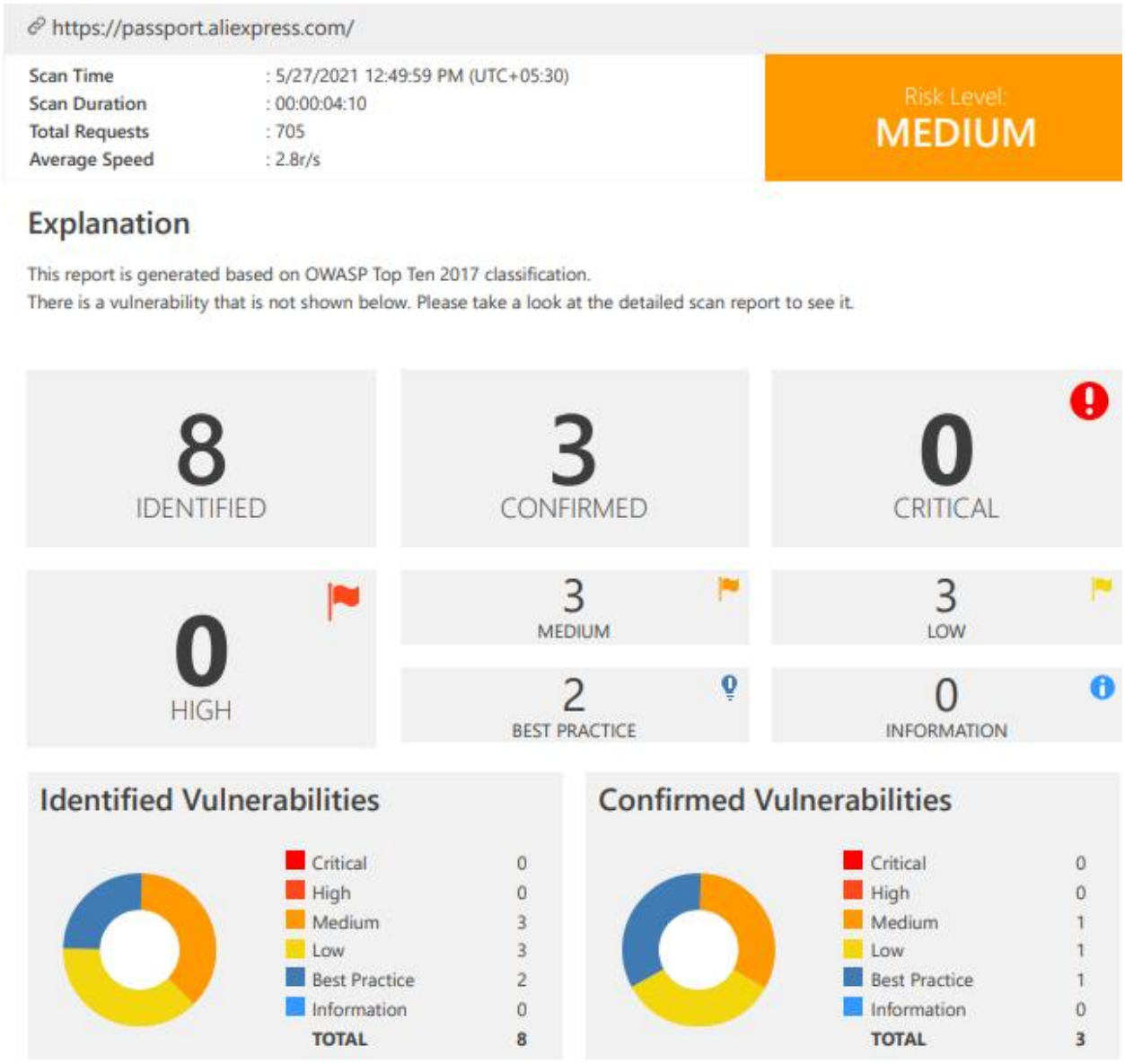
```
<a href="http://crosssite.example.com" rel="noreferrer"></a>
```

or

```
<a href="http://crosssite.example.com" referrerpolicy="no-referrer | same-origin | origin | strict-
```

```
origin | no-origin-when-downgrading"></a>
```

Overview Summary



Conclusion

This report has demonstrated the vulnerabilities and essential recommendations for the www.aliexpress.com domain. Vulnerabilities are categorized by severity under critical, high, medium, low, and informational. And also I have significantly explained what tools I have used for this security audit for each reconnaissance, vulnerability analysis phrases.

References

- .NET Cookie.Secure Property
- How to Create Totally Secure Cookies
- Netsparker - Security Cookies - Secure Flag
- https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_(OWASP-CM-008)
- https://www.w3.org/Protocols/rfc2616/rfc2616-sec9.html
- https://www.w3.org/TR/referrer-policy/
- https://www.netsparker.com/whitepaper-http-security-headers/#ReferrerPolicyHTTPHeader
- https://caniuse.com/#search=referrer%20policy
- https://www.netsparker.com/whitepaper-http-security-headers/#HTTPStrictTransportSecurityHSTSHTTPHeader
- https://hstspreload.org/
- https://owasp.org/www-project-top-ten/
- https://github.com/nahamsec/Resources-for-Beginner-Bug-Bounty-Hunters/blob/master/assets/vulns.md
- https://thehackerish.com/bug-bounty-tools-from-enumeration-to-reporting/
- https://medium.com/@hackbotone/10-recon-tools-for-bug-bounty-bafa8a5961bd
- https://www.acunetix.com/vulnerabilities/web/clickjacking-x-frame-options-header-missing/
- https://www.geeksforgeeks.org/http-headers-x-xss-protection/