

Sri Lanka Institute of Information Technology



VULNERABILITY ASSESSMENT  
WEB AUDIT

<https://www.aliexpress.com>

AliExpress™



IE2062 - Web Security

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

## **Student Details**

	<b>Student ID</b>	<b>Student Name</b>
1	IT19961118	W.M.J.P.WIJESEKARA

# Table of Contents

<b>Acknowledgement .....</b>	<b>5</b>
<b>Scope .....</b>	<b>5</b>
<b>Top 10 Web Application Security Risks.....</b>	<b>6</b>
A1:2017-Injection .....	6
A2:2017-Broken Authentication: .....	6
A3:2017-Sensitive Data Exposure: .....	6
A4:2017-XML External Entities (XXE): .....	6
A5:2017-Broken Access Control:.....	6
A6:2017-Security Misconfiguration: .....	7
A7:2017-Cross-Site Scripting XSS: .....	7
A8:2017-Insecure Deserialization: .....	7
A9:2017-Using Components with Known Vulnerabilities: .....	7
A10:2017-Insufficient Logging & Monitoring:.....	7
<b>About Domain .....</b>	<b>8</b>
What is AliExpress? .....	8
What is the Alibaba Group? .....	8
<b>HackerOne .....</b>	<b>9</b>
Alibaba Security Response Center .....	10
<b>Reconnaissance Phrase (Information Gathering).....</b>	<b>11</b>
<b>Subdomain Enumeration .....</b>	<b>12</b>
1. Sublist3r .....	12
2. Recon-ng Tool .....	28
3. Crt.sh .....	36
<b>Website Vulnerability Enumeration .....</b>	<b>37</b>
<b>Nikto.....</b>	<b>37</b>
1. 2014.aliexpress.com .....	50

2. activities.aliexpress.com.....	51
3. ajax.aliexpress.com.....	52
4. amacc.aliexpress.com.....	53
5. api.dos.aliexpress.com .....	55
6. best.aliexpress.com .....	55
7. brands.aliexpress.com .....	56
8. connectkeyword.aliexpress.com .....	58
9. message.aliexpress.com .....	58
10. passport.aliexpress.com .....	59
11. womenmenclothes439106.aliexpress.com .....	60
12. zhousyun19930515.aliexpress.com .....	62
<b>Find open ports and running services.....</b>	<b>63</b>
1. Zenmap.....	63
<b>Discovering target domain firewall protection .....</b>	<b>66</b>
1. Wafw00f .....	66
2. Nmap .....	67
<b>DNS enumeration .....</b>	<b>69</b>
1. Dnsrecon.....	69
<b>Public Device Enumeration .....</b>	<b>70</b>
1. Shodan.....	70
2. Censys.....	74
<b>Find Structure of File System .....</b>	<b>79</b>
1. OWASP DirBuster .....	79
2. Dirb Tool .....	90
<b>Netsparker.....</b>	<b>92</b>
https://www.aliexpress.com .....	92
https://www.2014.aliexpress.com .....	99

<a href="https://www.activities.aliexpress.com">https://www.activities.aliexpress.com</a> .....	102
<a href="https://www.ajax.aliexpress.com">https://www.ajax.aliexpress.com</a> .....	105
<a href="https://www.amacc.aliexpress.com">https://www.amacc.aliexpress.com</a> .....	108
<a href="https://www.api.dos.aliexpress.com">https://www.api.dos.aliexpress.com</a> .....	111
<a href="https://www.best.aliexpress.com">https://www.best.aliexpress.com</a> .....	115
<a href="https://www.brands.aliexpress.com">https://www.brands.aliexpress.com</a> .....	118
<a href="https://www.connectkeyword.aliexpress.com">https://www.connectkeyword.aliexpress.com</a> .....	121
<a href="https://www.passport.aliexpress.com">https://www.passport.aliexpress.com</a> .....	124
<b>Conclusion .....</b>	<b>126</b>
<b>References.....</b>	<b>127</b>

## **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.

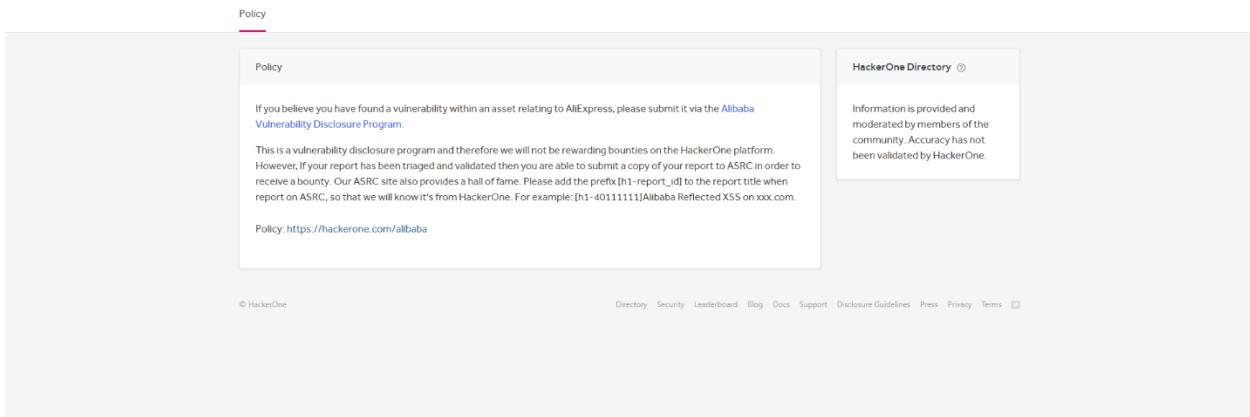
# HackerOne

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.

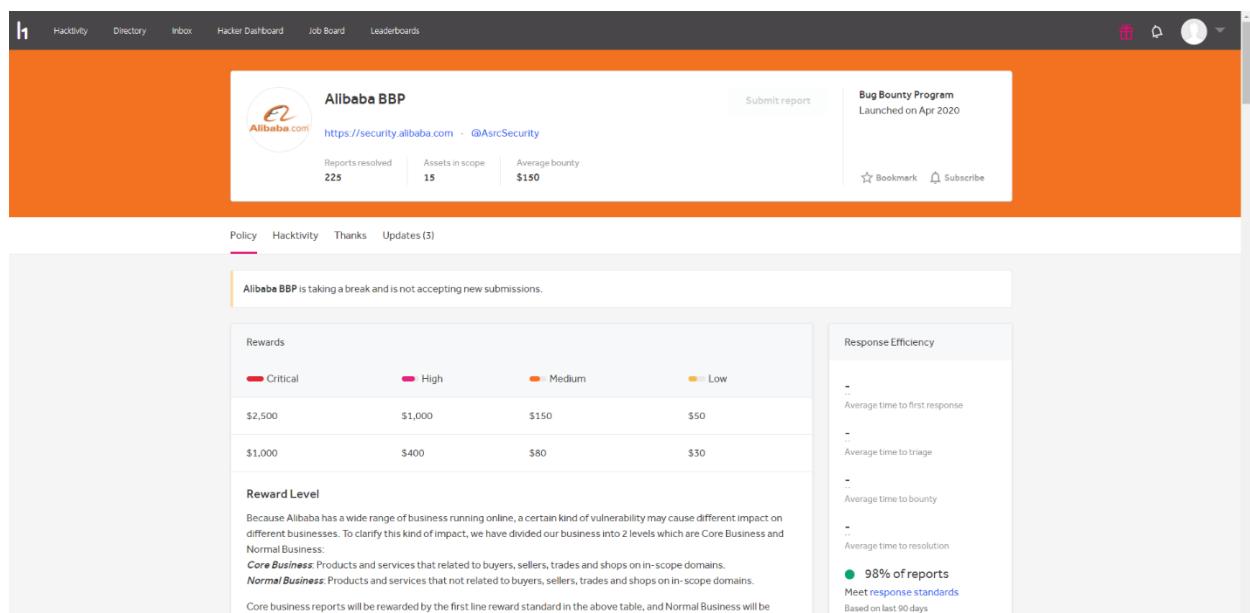
**The following details on the aliexpress domain were collected using information received from the HackerOne website.**



This screenshot shows the Aliexpress page on the HackerOne website. At the top, there is a red header bar with the Aliexpress logo and the text "Alibab Security Response Center". Below the header, there is a "Contact Security Team" button and an "External Program" section with a "Bookmark" link. The main content area has a "Policy" tab selected, which contains instructions for reporting vulnerabilities. To the right, there is a "HackerOne Directory" section with a note about community moderation. At the bottom, there is a navigation bar with links like "Directory", "Security", "Leaderboard", "Blog", "Docs", "Support", "Disclosure Guidelines", "Press", "Privacy", and "Terms".

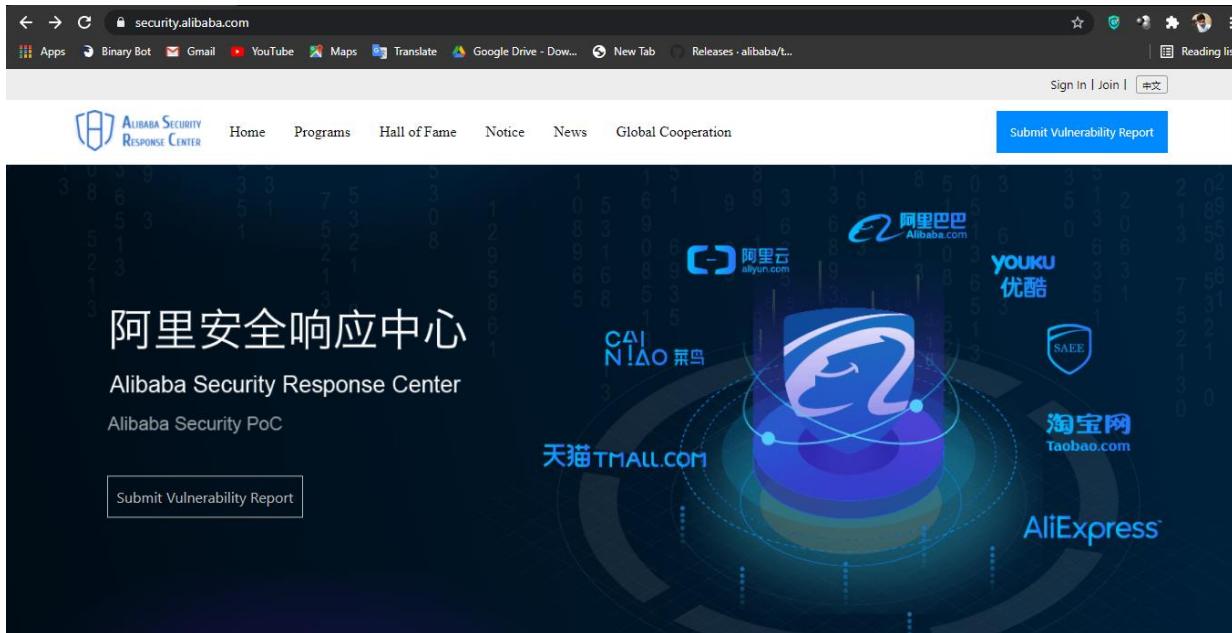


This screenshot shows the Alibaba BBP (Bug Bounty Program) page on the HackerOne website. At the top, there is an orange header bar with the Alibaba logo and the text "Alibaba BBP". Below the header, there is a "Submit report" button and a "Bug Bounty Program" section with a note about its launch date. The main content area has a "Policy" tab selected, which contains instructions for reporting vulnerabilities. To the right, there is a "HackerOne Directory" section with a note about community moderation. At the bottom, there is a navigation bar with links like "Directory", "Security", "Leaderboard", "Blog", "Docs", "Support", "Disclosure Guidelines", "Press", "Privacy", and "Terms".



This screenshot shows the Alibaba BBP (Bug Bounty Program) page on the HackerOne website. At the top, there is an orange header bar with the Alibaba logo and the text "Alibaba BBP". Below the header, there is a "Submit report" button and a "Bug Bounty Program" section with a note about its launch date. The main content area has a "Policy" tab selected, which contains instructions for reporting vulnerabilities. To the right, there is a "HackerOne Directory" section with a note about community moderation. At the bottom, there is a navigation bar with links like "Directory", "Security", "Leaderboard", "Blog", "Docs", "Support", "Disclosure Guidelines", "Press", "Privacy", and "Terms".

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



## Alibaba Security Response Center

A screenshot of the Alibaba Group products and services page. The top navigation bar is identical to the ASRC site. Below it, there's a section titled 'PRODUCTS AND SERVICES OF Alibaba Group' with links to 'AliExpress', 'Alibaba.com', 'Alipay', 'AliCloud', 'Tmall', 'Taobao', and 'Lazada GROUP'. A 'More' link is located at the top right of this section. Further down, there's an 'ABOUT ASRC' section containing text about the center's mission and duties, followed by a detailed paragraph about its responsibilities and daily operations.

# **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.

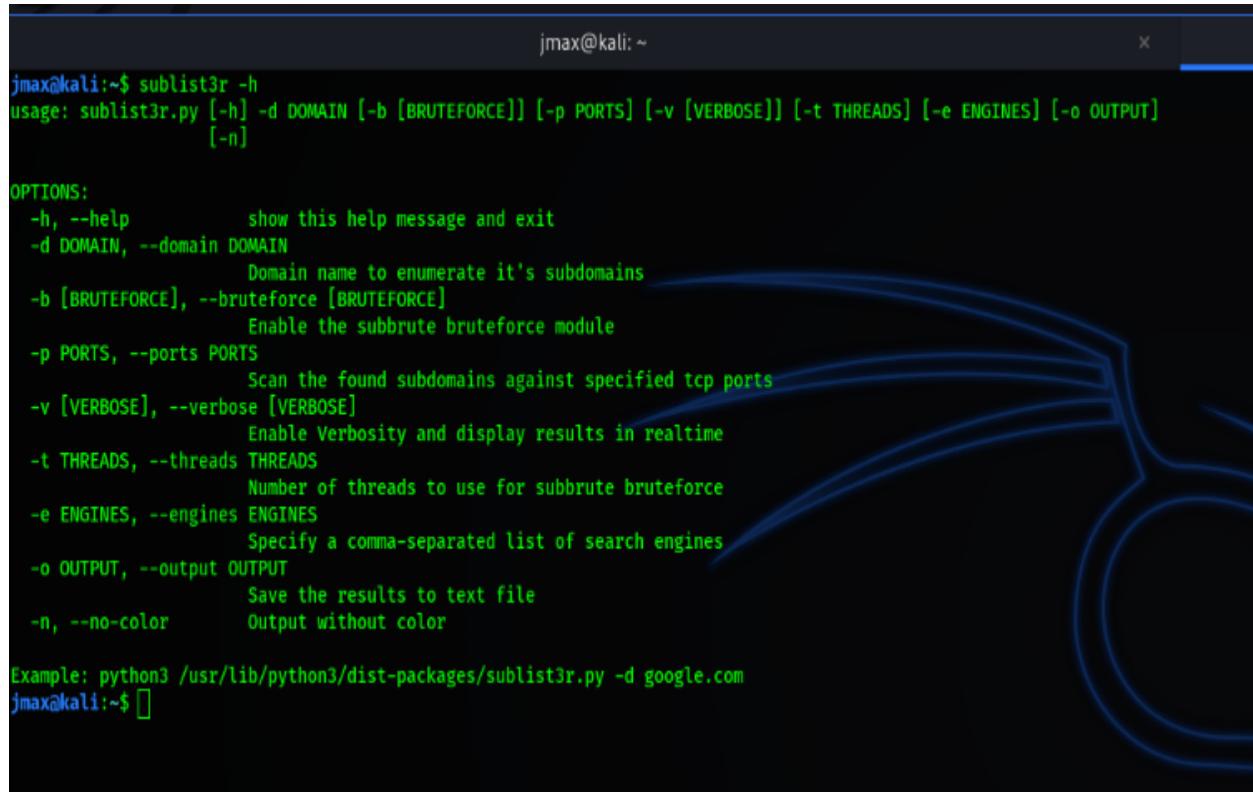
## Subdomain Enumeration

### 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.



```
jmax@kali:~$ sublist3r -h
usage: sublist3r.py [-h] -d DOMAIN [-b [BRUTEFORCE]] [-p PORTS] [-v [VERBOSE]] [-t THREADS] [-e ENGINES] [-o OUTPUT]
                   [-n]

OPTIONS:
-h, --help            show this help message and exit
-d DOMAIN, --domain DOMAIN
                      Domain name to enumerate it's subdomains
-b [BRUTEFORCE], --bruteforce [BRUTEFORCE]
                      Enable the subbrute bruteforce module
-p PORTS, --ports PORTS
                      Scan the found subdomains against specified tcp ports
-v [VERBOSE], --verbose [VERBOSE]
                      Enable Verbosity and display results in realtime
-t THREADS, --threads THREADS
                      Number of threads to use for subbrute bruteforce
-e ENGINES, --engines ENGINES
                      Specify a comma-separated list of search engines
-o OUTPUT, --output OUTPUT
                      Save the results to text file
-n, --no-color         Output without color

Example: python3 /usr/lib/python3/dist-packages/sublist3r.py -d google.com
jmax@kali:~$ []
```

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
# 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
wenzil0086.aliexpress.com
widesea001.aliexpress.com
willzhu2016.aliexpress.com
winic.aliexpress.com
withyou123.aliexpress.com
womenmenclthes439106.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
ybfl23.aliexpress.com
yinweitai520.aliexpress.com
yishowanna620318930.aliexpress.com
```

```
root@Kali: /home
tr.aliexpress.com
m.tr.aliexpress.com
track.aliexpress.com
trade.aliexpress.com
tradel.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
tv6.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
vesonall1987.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
vtcar01.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
sgooaway.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
ssl.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
celebrity001.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
plazza.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
pinuslongaevechina.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
qianggupen1.aliexpress.com
disha1178914.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
obdobj2.aliexpress.com
officel.aliexpress.com
oklili01.aliexpress.com
oklili02.aliexpress.com
oknnkoll.aliexpress.com
onemix.aliexpress.com
onemix666.aliexpress.com
oneedio.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
pkcellbatterv02.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
naikul.aliexpress.com
nanxing1718.aliexpress.com
navimc2.aliexpress.com
neewer.aliexpress.com
nevenkal23.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
longqibaol.aliexpress.com
loverjewelry6.aliexpress.com
loyoul207.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
mlzeng.aliexpress.com
macc.aliexpress.com
magicdiamondpainting19900508.aliexpress.com
magicz-01.aliexpress.com
magoruiarl5.aliexpress.com
manhuilisa001.aliexpress.com
marpou.aliexpress.com
match-upl218.aliexpress.com
maytech.aliexpress.com
mbest.aliexpress.com
mbf2016.aliexpress.com
meanwellonline.aliexpress.com
mecool01.aliexpress.com
mellow.aliexpress.com
mengjqiao33.aliexpress.com
meredithstore1.aliexpress.com
meredithstore2.aliexpress.com
mesinya2.aliexpress.com
messade.aliexpress.com
```

```
root@Kali: /home
kerui.aliexpress.com
keyson-line.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
lephée01.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
litowd008.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
jexxi1925.aliexpress.com
jiajia08.aliexpress.com
jile.aliexpress.com
jjcshop.aliexpress.com
jjrui7777.aliexpress.com
jockmail06.aliexpress.com
john dan johnny08.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
hrxl.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
globalwintoy1.aliexpress.com
globalwintoy3.aliexpress.com
glymg777.aliexpress.com
go123.aliexpress.com
go2boho.aliexpress.com
goddesswiggiestorenl.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
```

```
wuxiyibo2.fr.aliexpress.com
xiaomi.fr.aliexpress.com
xulin.fr.aliexpress.com
yemao.fr.aliexpress.com
yzxinyuan.fr.aliexpress.com
yzxinyuanyzfr.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
```

```
f31cfef1-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
bxthike.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
dxlymyull142093.aliexpress.com
dz-world.aliexpress.com
e87a7b06-2994-4e8f-9a52-56c167f4f183.aliexpress.com
eafengrow2.aliexpress.com
eafengrow3.aliexpress.com
earlykong.aliexpress.com
easunpower.aliexpress.com
edc1991edc1991.aliexpress.com
edifier.aliexpress.com
editexnol.aliexpress.com
ef-ce2.aliexpress.com
eiechip.aliexpress.com
elegant1.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-nol.aliexpress.com
cpu2.aliexpress.com
creality3d.aliexpress.com
crystalcastlerhinestone2.aliexpress.com
cust38.aliexpress.com
cust6.aliexpress.com
cwlspgiveme5.aliexpress.com
czb6721960.aliexpress.com
czel.aliexpress.com
d113845e-3873-4f16-ba5a-a6e9faee1542.aliexpress.com
dalc5f7d-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
bubblewzhmn1072.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
cffdfed4c-55fa-413c-b28f-c89e69220c41.aliexpress.com
cheap2017.aliexpress.com
chinawatch2.aliexpress.com
chowill01.aliexpress.com
chuwanglin5.aliexpress.com
chuwi.aliexpress.com
cl.aliexpress.com
cldxucl708641.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
bamero.aliexpress.com
baoxiu2.aliexpress.com
baodzi520.aliexpress.com
baseus.aliexpress.com
baseus2.aliexpress.com
baseus4.aliexpress.com
baseus6.aliexpress.com
batmax0018.aliexpress.com
best.aliexpress.com
bestbuy2018.aliexpress.com
bestchoicel.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
anyubic3dprinter.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
aruhi2.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
auxmarttopl.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-a137-9f850e6aab7.aliexpress.com
ajax.aliexpress.com
akwzmlly1527.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-9f57-996cef2clae4.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-dldee6da4d23.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-9625-5abe1e2b3b1b2.aliexpress.com
0a0506ea-b8ef-4766-b820-77b0196a5eal.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
123456.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
ybfl23.aliexpress.com
yinweitai520.aliexpress.com
yishowanna620318930.aliexpress.com
yjbc0-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-ing 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 11:48 jmax@kali:~

Sponsored by...  
BLACK HILLS  
www.blackhillsinfosec.com

# PRACTISEC

[recon-ng v5.1.1, Tim Tomes (@lanmaster53)]

[48] Recon modules  
[16] Disabled modules  
[8] Reporting modules  
[4] Import modules  
[22] Exploitation modules  
[3] Discovery modules

[recon-ng][default] > ?

Commands (type [help]? <topic>):

----

back	Exits the current context
dashboard	Displays a summary of activity
db	Interfaces with the workspace's database
exit	Exits the framework
help	Displays this menu
index	Creates a module index (dev only)
keys	Manages third party resource credentials
marketplace	Interfaces with the module marketplace
modules	Interfaces with installed modules
options	Manages the current context options
jdb	Starts a Python Debugger session (dev only)
script	Records and executes command scripts
shell	Executes shell commands
show	Shows various framework items
snapshots	Manages workspace snapshots
spool	Spools output to a file
workspaces	Manages workspaces

[recon-ng][default] > [ ]

Activities Terminal May 20 11:51 jmax@kali:~

script Records and executes command scripts  
.shell Executes shell commands  
.show Shows various framework items  
.snapshots Manages workspace snapshots  
.spool Spools output to a file  
.workspaces Manages workspaces

[recon-ng][default] > modules search

Discovery

----

discovery/info\_disclosure/cache\_snooper  
discovery/info\_disclosure/interesting\_files

Exploitation

----

exploitation/injection/command\_injector  
exploitation/injection/xpath\_bruter

Import

----

import/csv\_file  
import/list  
import/nasscan  
import/nmap

Recon

----

recon/companies-contacts/bing\_linkedin\_cache  
recon/companies-contacts/pen  
recon/companies-domains/pen  
recon/companies-domains/reverse\_dns  
recon/companies-domains/whosxy\_dns  
recon/companies-multi/github\_miner  
recon/companies-multi/shodan\_org  
recon/companies-multi/whois\_miner  
recon/contacts-contacts/abc  
recon/contacts-contacts/allister  
recon/contacts-contacts/mangle  
recon/contacts-contacts/unmangle  
recon/contacts-credentials/http\_breach  
recon/contacts-credentials/http\_paste  
recon/contacts-credentials/scylla  
recon/contacts-domains/migrate\_contacts  
recon/contacts-profiles/abc\_contact  
recon/credentials-credentials/abc  
recon/credentials-credentials/hazocrack  
recon/credentials-credentials/hashes\_org  
recon/domains-companies/pen  
recon/domains-companies/whosxy\_whois

```

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/ipinfofb
recon/hosts-hosts/ustack
recon/hosts-hosts/resolve
recon/hosts-hosts/reverse_resolve
recon/hosts-hosts/salttools
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/profiles-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_repos
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 domains
[*] Searching installed modules for 'domains'...
[] [] No modules found.
Searches installed modules

Usage: modules search [cagex]

[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/sgp_search
recon/domains-contacts/whois_pocs
recon/domains-contacts/wikileaker
recon/domains-credentials/pwnedlist/api_usage
recon/domains-credentials/pwnedlist/domain_isowned
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/bulitwith
recon/domains-hosts/certificate_transparency
recon/domains-hosts/google_site_web
recon/domains-hosts/hackertarget
recon/domains-hosts/_n_spf_ip
recon/domains-hosts/metacraft
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  alexexpress.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:alexpress.com
[*] Country: None
[*] Host: m.pt.alexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: m.ru.alexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: sell.alexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
Activities Terminal May 20 14:08 • jmax@kali: ~
[recon-ng][default][google_site_web] >
-----[*] AS-ASIA-EUROPE
[*] -----
[*] Country: None
[*] Host: veromoda.ru.alexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: ru.alexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: th.alexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: fr.alexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: es.alexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: ko.alexpress.com
[*] Ip_Address: None
[*] Latitude: None
[*] longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None

```

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

```
Activities Terminal May 20 14:08 • jmax@kali:~  
[x] Country: None  
[x] Host: ar.aliexpress.com  
[x] Ip_Address: None  
[x] Latitude: None  
[x] Longitude: None  
[x] Notes: None  
[x] Region: None  
[x] -----  
[x] Country: None  
[x] Host: best.aliexpress.com  
[x] Ip_Address: None  
[x] Latitude: None  
[x] Longitude: None  
[x] Notes: None  
[x] Region: None  
[x] -----  
[x] Country: None  
[x] Host: m.aliexpress.com  
[x] Ip_Address: None  
[x] Latitude: None  
[x] Longitude: None  
[x] Notes: None  
[x] Region: None  
[x] -----  
[x] Country: None  
[x] Host: nl.aliexpress.com  
[x] Ip_Address: None  
[x] Latitude: None  
[x] Longitude: None  
[x] Notes: None  
[x] Region: None  
[x] -----  
[x] Country: None  
[x] Host: he.aliexpress.com  
[x] Ip_Address: None  
[x] Latitude: None  
[x] Longitude: None  
[x] Notes: None  
[x] Region: None  
[x] -----  
[x] Country: None  
[x] Host: www.aliexpress.com  
[x] Ip_Address: None  
[x] Latitude: None  
[x] Longitude: None  
[x] Notes: None  
[x] Region: None  
[x] -----  
[x] 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:nl.aliexpress.com -site:tr.aliexpress.com -site:vi.aliexpress.com -site:ar.aliexpress.com -site:
```

Activities Terminal • May 20 14:08 • jmax@kali:~

```
aliexpress.com "site:de.aliexpress.com" "site:de.aliexpress.com" "site:it.aliexpress.com" "site:it.aliexpress.com" "site:pt.aliexpress.com" "site:pt.aliexpress.com" "site:vi.aliexpress.com" "site:vi.aliexpress.com" "site:  
best.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  
[+] 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
```







### 3. Crt.sh

Screenshot of crt.sh search results for 'alexpress.com' showing numerous certificates issued to various subdomains of alexpress.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.alexpress.com	1111.alexpress.com act.alexpress.com activities.alexpress.com ajax.alexpress.com alexpress.com api.dos.alexpress.com api.m.alexpress.com best.alexpress.com brands.alexpress.com cdo.alexpress.com cn.m.alexpress.com connectkeyword.alexpress.com desc.alexpress.com es.alexpress.com feedback.alexpress.com fright.alexpress.com group.alexpress.com gtreu.alexpress.com gthz.alexpress.com gttru.alexpress.com gzu.alexpress.com he.alexpress.com hotproducts.alexpress.com ja.alexpress.com lighthouse.alexpress.com logos.alexpress.com macs.alexpress.com m.alexpress.com m.de.alexpress.com m.es.alexpress.com message.alexpress.com m.fra.alexpress.com m.id.alexpress.com m.it.alexpress.com m.ja.alexpress.com m.ko.alexpress.com m.nl.alexpress.com m.pt.alexpress.com m.ru.alexpress.com msale.alexpress.com m.th.alexpress.com m.tr.alexpress.com m.vi.alexpress.com my.alexpress.com passport.alexpress.com promotion.alexpress.com pt.alexpress.com ru.alexpress.com sale.alexpress.com s.click.alexpress.com	C=US_O=DigiCert Inc_CN=DigiCert SHA2 Secure Server CA
	11783779	2016-01-01	2015-12-30	2016-12-27	pcookie.taobao.com	my.alexpress.com promotion.alexpress.com pt.alexpress.com ru.alexpress.com sale.alexpress.com s.click.alexpress.com shoppingcart.alexpress.com shoppingcart1.alexpress.com us.alexpress.com us.cobra.alexpress.com www.alexpress.com	C=US_O="VeriSign, Inc."_OU=VeriSign Trust Network_OU=Terms of use at https://www.verisign.com/reac110.CN=VeriSign Class 3 International Server CA - G3
	11762630	2015-12-31	2015-12-28	2016-12-28	*.alexpress.com	*.alexpress.com *.act.alexpress.com *.activities.alexpress.com *.ajax.alexpress.com *.alexpress.com *.api.dos.alexpress.com *.api.m.alexpress.com *.best.alexpress.com *.brands.alexpress.com *.cdo.alexpress.com *.cn.m.alexpress.com *.connectkeyword.alexpress.com *.desc.alexpress.com *.es.alexpress.com *.feedback.alexpress.com *.fright.alexpress.com *.group.alexpress.com *.gtreu.alexpress.com *.gthz.alexpress.com *.gttru.alexpress.com *.gzu.alexpress.com *.he.alexpress.com *.hotproducts.alexpress.com *.ja.alexpress.com *.lighthouse.alexpress.com *.logos.alexpress.com *.macs.alexpress.com *.m.alexpress.com *.m.de.alexpress.com *.m.es.alexpress.com *.message.alexpress.com *.m.fra.alexpress.com *.m.id.alexpress.com *.m.it.alexpress.com *.m.ja.alexpress.com *.m.ko.alexpress.com *.m.nl.alexpress.com *.m.pt.alexpress.com *.m.ru.alexpress.com *.msale.alexpress.com *.m.th.alexpress.com *.m.tr.alexpress.com *.m.vi.alexpress.com *.my.alexpress.com *.passport.alexpress.com *.promotion.alexpress.com *.pt.alexpress.com *.ru.alexpress.com *.sale.alexpress.com *.s.click.alexpress.com	C=US_O="GlobalSign nv-sa"_CN=GlobalSign Organization Validation CA - SHA256 - G2
	10808443	2015-11-22	2015-06-15	2016-09-10	*.alexpress.com	*.alexpress.com *.act.alexpress.com *.activities.alexpress.com *.ajax.alexpress.com *.alexpress.com *.api.dos.alexpress.com *.api.m.alexpress.com *.best.alexpress.com *.brands.alexpress.com *.cdo.alexpress.com *.cn.m.alexpress.com *.connectkeyword.alexpress.com *.desc.alexpress.com *.es.alexpress.com *.feedback.alexpress.com *.fright.alexpress.com *.group.alexpress.com *.gtreu.alexpress.com *.gthz.alexpress.com *.gttru.alexpress.com *.gzu.alexpress.com *.he.alexpress.com *.hotproducts.alexpress.com *.ja.alexpress.com *.lighthouse.alexpress.com *.logos.alexpress.com *.macs.alexpress.com *.m.alexpress.com *.m.de.alexpress.com *.m.es.alexpress.com *.message.alexpress.com *.m.fra.alexpress.com *.m.id.alexpress.com *.m.it.alexpress.com *.m.ja.alexpress.com *.m.ko.alexpress.com *.m.nl.alexpress.com *.m.pt.alexpress.com *.m.ru.alexpress.com *.msale.alexpress.com *.m.th.alexpress.com *.m.tr.alexpress.com *.m.vi.alexpress.com *.my.alexpress.com *.passport.alexpress.com *.promotion.alexpress.com *.pt.alexpress.com *.ru.alexpress.com *.sale.alexpress.com *.s.click.alexpress.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	*.alexpress.com	*.alexpress.com *.act.alexpress.com *.activities.alexpress.com *.ajax.alexpress.com *.alexpress.com *.api.dos.alexpress.com *.api.m.alexpress.com *.best.alexpress.com *.brands.alexpress.com *.cdo.alexpress.com *.cn.m.alexpress.com *.connectkeyword.alexpress.com *.desc.alexpress.com *.es.alexpress.com *.feedback.alexpress.com *.fright.alexpress.com *.group.alexpress.com *.gtreu.alexpress.com *.gthz.alexpress.com *.gttru.alexpress.com *.gzu.alexpress.com *.he.alexpress.com *.hotproducts.alexpress.com *.ja.alexpress.com *.lighthouse.alexpress.com *.logos.alexpress.com *.macs.alexpress.com *.m.alexpress.com *.m.de.alexpress.com *.m.es.alexpress.com *.message.alexpress.com *.m.fra.alexpress.com *.m.id.alexpress.com *.m.it.alexpress.com *.m.ja.alexpress.com *.m.ko.alexpress.com *.m.nl.alexpress.com *.m.pt.alexpress.com *.m.ru.alexpress.com *.msale.alexpress.com *.m.th.alexpress.com *.m.tr.alexpress.com *.m.vi.alexpress.com *.my.alexpress.com *.passport.alexpress.com *.promotion.alexpress.com *.pt.alexpress.com *.ru.alexpress.com *.sale.alexpress.com *.s.click.alexpress.com	C=US_O="VeriSign, Inc."_OU=VeriSign Trust Network_OU=Terms of use at https://www.verisign.com/reac110.CN=VeriSign Class 3 Secure Server CA - G3
	7136093	2015-06-01	2015-04-27	2016-04-27	pcookie.taobao.com	C=US_O="VeriSign, Inc."_OU=VeriSign Trust Network_OU=Terms of use at https://www.verisign.com/reac110.CN=VeriSign Class 3 International Server CA - G3	
	5646047	2014-11-01	2014-08-08	2015-08-08	*.alexpress.com	*.alexpress.com *.act.alexpress.com *.activities.alexpress.com *.ajax.alexpress.com *.alexpress.com *.api.dos.alexpress.com *.api.m.alexpress.com *.best.alexpress.com *.brands.alexpress.com *.cdo.alexpress.com *.cn.m.alexpress.com *.connectkeyword.alexpress.com *.desc.alexpress.com *.es.alexpress.com *.feedback.alexpress.com *.fright.alexpress.com *.group.alexpress.com *.gtreu.alexpress.com *.gthz.alexpress.com *.gttru.alexpress.com *.gzu.alexpress.com *.he.alexpress.com *.hotproducts.alexpress.com *.ja.alexpress.com *.lighthouse.alexpress.com *.logos.alexpress.com *.macs.alexpress.com *.m.alexpress.com *.m.de.alexpress.com *.m.es.alexpress.com *.message.alexpress.com *.m.fra.alexpress.com *.m.id.alexpress.com *.m.it.alexpress.com *.m.ja.alexpress.com *.m.ko.alexpress.com *.m.nl.alexpress.com *.m.pt.alexpress.com *.m.ru.alexpress.com *.msale.alexpress.com *.m.th.alexpress.com *.m.tr.alexpress.com *.m.vi.alexpress.com *.my.alexpress.com *.passport.alexpress.com *.promotion.alexpress.com *.pt.alexpress.com *.ru.alexpress.com *.sale.alexpress.com *.s.click.alexpress.com	C=US_O="VeriSign, Inc."_OU=VeriSign Trust Network_OU=Terms of use at https://www.verisign.com/reac110.CN=VeriSign Class 3 Secure Server CA - G3
	2492285	2013-07-06	2013-04-23	2015-04-24	styles1.alexpress.com	C=US_O="VeriSign, Inc."_OU=VeriSign Trust Network_OU=Terms of use at https://www.verisign.com/reac110.CN=VeriSign Class 3 International Server CA - G3	
	350332	2013-09-26	2012-12-12	2014-12-19	login.alexpress.com	C=US_O="VeriSign, Inc."_OU=VeriSign Trust Network_OU=Terms of use at https://www.verisign.com/reac110.CN=VeriSign Class 3 International Server CA - G3	

Activate Windows  
Go to Settings to activate Windows.

5:11 PM 5/4/2021

# 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/rw.cgi60: 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/rw.cgi60/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: ../../windows/repair/sam: BadBlue server is vulnerable to multiple remote exploits. See <http://www.securiteam.com/exploits/5HP0M2A60G.html> for more information.
- + OSVDB-721: ../../winnt/repair/sam: BadBlue server is vulnerable to multiple remote exploits. See <http://www.securiteam.com/exploits/5HP0M2A60G.html> for more information.
- + OSVDB-721: ../../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./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./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./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.

```
Activities Terminal May 3 12:44
jmax@kali:~/Crips jmax@kali:~
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: 2100bdd716200245275748323e6f7d
+ 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: aebridge03300189215.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/fform.cgi: Check Phrack 55 for info by RFP, allows to append info to writable files.
+ /cgi-bin/fformx: 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=556a=7
+ /cgi-bin/lwgate.cgi: Check Phrack 55 for info by RFP, http://www.phrack.com/show.php?p=556a=7
+ /cgi-bin/lwgate: Check Phrack 55 for info by RFP
+ /cgi-bin/LNGate: Check Phrack 55 for info by RFP
+ /cgi-bin/perlshop.cgi: v3.1 by ARPAnet.com; check info in Phrack 55 by RFP
+ OSVDB-390: /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. See http://www.attrition.org/~jericho/work/security/greymatter.html for more info.
+ /cgi-bin/guestbook/passwd: GuestBook r4 from lasource.r2.ru stores the admin password in a plain text file.
+ /cgi-bin/photo/protected/manage.cgi: My Photo Gallery management interface. May allow full access to photo galleries and more. Versions before 3.8 allowed anyone to view contents of any directory on systems
+
+ /cgi-bin/wrap.cgi: possible variation: comes with IRIX 6.2; allows to view directories
+ /cgi-bin/wrap: comes with IRIX 6.2; allows to view directories
+ /cgi-bin/visadmin.exe: This CGI allows an attacker to crash the web server. Remove it from the CGI directory.
+ /cgi-bin/html2html.cgi: Html2Wml < 0.4.8 access local files via CGI, and more
+ /cgi-bin/html2wml.cgi: Html2Wml < 0.4.8 access local files via CGI, and more
+ /cgi-bin/guestbook.cgi: May allow attackers to execute commands as the web daemon.
+ /cgi-bin/guestbook.pl: May allow attackers to execute commands as the web daemon.
+ /cgi-bin/ss: Mediahouse Statistics Server may allow attackers to execute remote commands. Upgrade to the latest version or remove from the CGI directory.
+ /cgi-bin/gH.cgi: Web backdoor by gH
+ /cgi-bin/gn-cplog.cgi: GreyMatter log file defaults to mode 666 and contains login and passwords used to update the GM site. See http://www.attrition.org/~jericho/works/security/greymatter.html for more info.
+
+ /cgi-bin/gm.cgi: GreyMatter blogger may reveal user IDs/passwords through a gmrightclick-#####.reg files (# are numbers), possibly in /archive or other archive location. See http://www.attrition.org/~jericho/works/security/greymatter.html for more info.
```

```
Activities Terminal May 3 12:44 jmax@kali: ~
jmax@kali: ~
jmax@kali: ~

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/Aesop
Cookie aliyaml_id created without the httponly flag
IP address found in the 'set-cookie' 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: 21080dd71620024527574748323e8f7d
The 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 'bxpnhish' found, with contents: 1
Retrieved via header: abridge013800189215.deel[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=556a/
+ /cgi-bin/lwgate.cgi: Check Phrack 55 for info by RFP, http://www.phrack.com/show.php?p=556a/
+ /cgi-bin/lwgate: Check Phrack 55 for info by RFP
+ /cgi-bin/lwgate: Check Phrack 55 for info by RFP
+ /cgi-bin/peri�품.cgi: v1.1 by ARPAnet.com; check info in Phrack 55 by RFP
OSVDB-3984: /vti_bin/shmlw.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: Information from Irix Handler has been seen from other CGI scanners.
/cgi-bin/finger.cgi: finger other users, may be other commands?
/cgi-bin/finger.cgi: 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's 'password' file, that controls who can post. This contains login and password information and is installed mode 666 by default. See http://www.attrition.org/~jericho/work
u/security/greymatter.html for more info.
/cgi-bin/guestbook/passwd: GuestBook r4 from lasource.r2.ru stores the admin password in a plain text file.
/cgi-bin/photo/protected/manage.cgi: My Photo Gallery management interface. May allow full access to photo galleries and more. Versions before 3.8 allowed anyone to view contents of any directory on systems
/cgi-bin/wrap.cgi: possible variation: comes with IRIX 6.2; allows to view directories
/cgi-bin/wrap: comes with IRIX 6.2; allows to view directories
/cgi-bin/visadmin.exe: This CGI allows an attacker to crash the web server. Remove it from the CGI directory.
/cgi-bin/html2xml.cgi: Html2xml < 0.4.8 access local files via CGI, and more
/cgi-bin/html2xml.cgi: Html2xml < 0.4.8 access local files via CGI, and more
/cgi-bin/guestbook.cgi: May allow attackers to execute commands as the web daemon.
/cgi-bin/guestbook.pl: May allow attackers to execute commands as the web daemon.
/cgi-bin/ss: Mediahouse Statistics Server may allow attackers to execute remote commands. Upgrade to the latest version or remove from the CGI directory.
/cgi-bin/gt/gt.cgi: Web backdoor by GH
/cgi-bin/gm-cplog.cgi: GreyMatter log file defaults to mode 666 and contains login and passwords used to update the GM site. See http://www.attrition.org/~jericho/works/security/greymatter.html for more inf
0.
/cgi-bin/gm.cgi: GreyMatter blogger may reveal user IDs/passwords through a gmrightclick-#####.reg files (# are numbers), possibly in /archive or other archive location. See http://www.attrition.org/~jeric
```

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

```
Activities Terminal - May27 12:22 • jmax@kali: ~ jmax@kali: ~ jmax@kali: ~

jmax@kali: ~ x
jmax@kali: ~ x
jmax@kali: ~ x

OSVDB-2922 /domain/mg_user/info.mis: website has exposure over names & passwords.
OSVDB-2941 /CloudStorage/Changefolder.php: This CGI can contain a backdoor and may allow attackers to change the Carr32 admin password.
OSVDB-3944 /showmail.pl: Gmail WebMail 3.52 allows attacker to read arbitrary user's mailbox. Requires knowing valid user name and appending ?Folder=...//..//victim@somehost.com/mbox/Inbox to the showmail.pl file.
OSVDB-2948 /reademail.pl: Gmail WebMail 3.52 contains an SQL injection that allows attacker to read any email message for any address registered in the system. Example to append to reademail.pl: ?id=666&folderquer%52or%20EmailDatabase
OSVDB-31 /issamples/exair/search/query.asp: Scripts within the Exair package on IIS 4 can be used for a DoS against the server. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0449. RID=193.
OSVDB-3921 /buddies/buddyList: Buddy List?
OSVDB-3922 /buddies/buddyList: Buddy List?
OSVDB-3923 /buddies/buddyList: Buddy List?
OSVDB-3924 /sqlnet.log Oracle log file found.
OSVDB-3925 [access=/]: This might be interesting...
OSVDB-3926 [access=/log]: This might be interesting...
OSVDB-3927 [access=/access]: This might be interesting...
OSVDB-3928 [access=/access.log]: This might be interesting...
OSVDB-3929 [access=/account]: This might be interesting...
OSVDB-3930 [access=/accounting]: This might be interesting...
OSVDB-3931 [access=/activev/]: This might be interesting...
OSVDB-3932 [admin/]: This might be interesting...
OSVDB-3933 [admin/.php]: This might be interesting...
OSVDB-3934 [admin/admin.html]: This might be interesting...
OSVDB-3935 [admin.php]: This might be interesting...
OSVDB-3936 [admin.php3]: This might be interesting...
OSVDB-3937 [admin.shtml]: This might be interesting...
OSVDB-3938 [admin/]: This might be interesting...
OSVDB-3939 [Adminstration/]: This might be interesting...
OSVDB-3940 [Administration/]: This might be interesting...
OSVDB-3941 [Administrativy/]: This might be interesting...
OSVDB-3942 [Admin_file/]: This might be interesting...
OSVDB-3943 [advwebadmin/]: This might be interesting...probably HostingController, www.hostingcontroller.com
OSVDB-3944 [Agent/]: This might be interesting...
OSVDB-3945 [Agents/]: This might be interesting...
OSVDB-3946 [Agent/2]: This might be interesting...
OSVDB-3947 [agents/]: This might be interesting...
OSVDB-3948 [agents/]: This might be interesting...
OSVDB-3949 [analog/]: This might be interesting...
OSVDB-3950 [apache/]: This might be interesting...
OSVDB-3951 [app/]: This might be interesting...
OSVDB-3952 [application/]: This might be interesting...
OSVDB-3953 [application/agent/]: This might be interesting...
OSVDB-3954 [application/agent/2]: This might be interesting...
OSVDB-3955 [archive/]: This might be interesting...
OSVDB-3956 [archive/]: This might be interesting...
OSVDB-3957 [archive/]: This might be interesting...
OSVDB-3958 [archive/]: This might be interesting...
OSVDB-3959 [archive/]: This might be interesting...
```

## 2. activities.aliexpress.com

### 3. ajax.aliexpress.com

```
Activities Terminal May 27 13:58 • jmax@kali: ~
jmax@kali: ~ x jmax@kali: ~ x

jmax@kali: ~$ nmap -h ajax.aliexpress.com
Nmap v2.1.6

Target IP: 198.11.132.250
Target Portrange: 80
Start Time: 2021-05-27 13:46:18 (GMT+5)

Server: Tengine/2.2.1
  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
  Unknown header 'og:image' found, with contents: 0a6bf8ad16271074186008317ech5f
  Unknown header 'og:title' found, with contents: 1

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
  No CGI Directories found (use '-C all' to force check all possible dirs)
  Retrieved via header: t01010101010000.ee.ct[web_302]
    Retrieved access-control-allow-origin header: nikto.example.com
  Web Server returns a valid response with junk HTTP methods, this may cause false positives.
  DEBUG: HTTP verb may show server debugging information. See https://msdn.microsoft.com/en-us/library/e8z01xdn2dys5.8n29.aspx for details.
  /kboard/: KBoard version 0.3.0 and prior have a security problem in forum_edit_post.php, forum_post.php and forum_reply.php
  /lists/admin/: PHPList pre 2.6.2 contains a number of vulnerabilities including remote administrative access, harvesting user info and more. Default login to admin interface is admin/phplist
  /splahost/: Splahost pre 1.2 may have multiple security problems
  /sshone/: SiteSeed pre 1.2 has "major" security problems
  /sshone/: SiteSeed pre 1.4.2 has "major" security problems.
  /tiki/: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin
  /tiki/tiki-install.php: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin
  /scripts/samples/details.idc: See RFP 9901: www.wiretrip.net
  OSVDB-59620: Global.asax.cs: Attackers can crash a Microsoft FrontPage by requesting a DOS device, like shml.exe/aux.htm -- a DoS was not attempted.
  OSVDB-6347: /etc/passwd: Allow reading of "/etc" directory
  /cpl-bin/wranc: Comes with IRIX 6.2.1 allows to view directories
  /forums/admin/config.php: PHP Config file may contain database IDs and passwords.
  /forums/admin/config.php: PHP Config file may contain database IDs and passwords.
  /forums/administrator/config.php: PHP Config file may contain database IDs and passwords.
  /forums/config.php: PHP Config file may contain database IDs and passwords.
  /global.asax.cs: Global.asax.cs reveals sensitive configuration information about its configuration.
  /hookedconfig: PHP-Gastchuck 1.0 Beta reveals the md5 hash of the admin password.
  /help/: Help directory should not be accessible
  OSVDB-2411: /holo-cms/holatmags.php?date1.../sec/data.php: holo-cms-1.2.9-18 may reveal the administrator ID and password.
  OSVDB-8103: /global1.inc: PHP-Survey's inc file should not be available via the web. Configure the web server to ignore .inc files or change this to global.inc.php
  OSVDB-59620: /inc/admin/config_load.php: Bookmark4u v1.0.1 include files are not protected and may contain remote source injection by using the 'prefix' variable.
  OSVDB-59620: /inc/admin/config_load.php: Bookmark4u v1.0.1 include files are not protected and may contain remote source injection by using the 'prefix' variable.
  OSVDB-59620: /inc/charts.php: Bookmark4u v1.6.3 include files are not protected and may contain remote source injection by using the 'prefix' variable.
  Cookie all_apache_id created without the httponly flag
  RFC-1918 IP address found in the '_all_apache_id' cookie. The IP is '10.181.15.98'.
  RFC-1918 IP address found in the 'set-cookie' header. The IP is '10.181.15.98'.
  OSVDB-2703: /geeklog/users.php: Geeklog prior to 1.3.8-1src contains a SQL injection vulnerability that lets a remote attacker reset admin password.
```

```
Activities Terminal May 27 13:58 * jmax@kali: ~

# getAccess: This may be an indication that the server is running getAccess for 550
# Cookie xman_us_f created without the httponly flag
# Cookie acs_usic_l created without the httponly flag
# Cookie int_local created without the httponly flag
# Cookie apg_use_f created without the httponly flag
# Cookie apg_use_s created without the httponly flag
# Uncommon header <application-context> found, with contents: ac-buyer-homepage-f;prod:7001
# </tdcols>/expvala/openfile.cfm: Can use to expose the system/server path.
# /tweb/: Microsoft TSAC Found. http://www.dlswebserver.com/main/fr_index.html?/main/shs-Terminal-Services-Advanced-Client-Configuration.html
/vgn/performance/TM/Vignette CMS admin/maintenance script available.
/vgn/performance/TM/Report/Vignette CMS admin/maintenance script available.
/vgn/performance/TM/Report/XM/Vignette CMS admin/maintenance script available.
/vgn/perfstat: Vignette CMS admin/maintenance script available.
/vgn/poststats: Vignette CMS admin/maintenance script available.
/vgn/previewer: Vignette CMS admin/maintenance script available.
/vgn/record/previewer: Vignette CMS admin/maintenance script available.
/vgn/stylepreview: Vignette CMS admin/maintenance script available.
/vgn/vr/Deleting: Vignette CMS admin/maintenance script available.
/vgn/vr/Editing: Vignette CMS admin/maintenance script available.
/vgn/vr/Adding: Vignette CMS admin/maintenance script available.
/vgn/vr>Select: Vignette CMS admin/maintenance script available.
/scripts/lisadmin/bdir.htm: This default script shows host info, may allow file browsing and buffer a overrun in the chunked Encoding data transfer mechanism, request /scripts/lisadmin/bdir.htm?<c><dirs> . https://docs.microsoft.com/en-us/security-updates/securitybulletins/2002/MS02-028. http://www.cert.org/advisories/CA-2002-09.html.
/scripts/lisadmin/lism.dll: Allows to a brute force attack on passwords
/scripts/tools/crossdomain: This coll allows remote users to view and modify SQL DB contents, server paths, drooroot and more.
/blah/badfile.shtml: Allaire ColdFusion allows ISP source viewed through a vulnerable SSL call.
/OSW08-4910: /vgn/style: Vignette servers may reveal system information through this file.
/OSW08-17053: /SiteServer/admin/commerce/foundation/dominion.asp: Displays known domains of which that server is involved.
/OSW08-17054: /SiteServer/admin/commerce/foundation/driver.asp: Displays a list of installed ODBC drivers.
/OSW08-17055: /SiteServer/admin/commerce/foundation/OSW.asp: Displays all DSNs configured for selected ODBC drivers.
/OSW08-17056: /SiteServer/admin/commerce/foundation/OSWList.asp: Displays a list of all DSNs.
/siteserver/Admin/Windows/edge/default.asp: Used to view current search catalog configurations
/hasilix/mbo-list.php3: Hasilix webmail application prior to 1.1.1 contains a XSS issue in 'message list' function/page
/hasilix/message-read.php3: Hasilix webmail application prior to 1.1.1 contains a XSS issue in 'read message' function/page
/clusterframe.jnlp: Macromedia JRun 4 build 61650 remote administration interface is vulnerable to several XSS attacks.
/1lohamail/blank.htm: IhohMail v1.0.10 contains a XSS vulnerability. Previous versions contain other non-descript vulnerabilities.
/jdb-dmdu/FaxSurvey: This is a Java Shellserv exploit. It contains a backdoor to allow attackers to execute arbitrary commands.
OSW08-4951: /scripts/carelio/carelio.dll: Carelio v1.1 may allow commands to be executed on the server by replacing hidden form elements. This could not be tested by Nikto.
/scripts/tools/dlform.exe: Allows creation of ODBC Data Source
/scripts/tools/dlform.exe: Allows creation of ODBC Data Source
OSW08-17056: /SiteServer/admin/knowledge/dsngc/users/groupManager.asp: Used to create, modify, and potentially delete LDAP users and groups.
OSW08-17057: /SiteServer/admin/knowledge/dsngc/users/userManager.asp: Used to create, modify, and potentially delete LDAP users and groups.
/jrdl/ping: Has MS Network Service 1.0.1.1. A user may be infected with the Nimda virus.
/scripts/htpdcdrd.dll: Possible IIS backdoor found.
/scripts/proxy/wproxy.dll: MSProxy v1.0 installed
```

4. amacc.aliexpress.com

```
Activities Terminal May 27 14:32 •
jmax@kali: ~ jmax@kali: ~
+ OSVDB-9332: /cgi-bin/scoadminreg.cgi: This script (part of Unixware WebTop) may have a local root exploit. It is also an system admin script and should be protected via the web.
+ OSVDB-4663: /cgi-bin/SCB_DIR/superquestconfig: Super GuestBook 1.8 from lasource.r2.ru stores the admin password in a plain text file.
+ /cgi-bin/iscat: Multiple versions of icat allow attackers to read arbitrary files. Make sure the latest version is running.
+ /cgi-bin/nph-showlogs.pl?files=.../.filter=&#submit=GooLine&refresh=0: ncUBE Server Manager 1.0 nph-showlogs.pl directory traversal bug
+ OSVDB-6192: /cgi-bin/update.dpgs: Duma Photo Gallery System may allow remote users to write to any file on the system. See http://boiler.eyonsecurity.net for details. This could not be re
motely tested.
+ /cgi-bin/view-source: This may allow remote arbitrary file retrieval.
+ /cgi-bin/wrap: This CGI lets users read any file with 755 perms. It should not be in the CGI directory.
+ /cgi-bin/cgiwrap: Some versions of cgiwrap allow anyone to execute commands remotely.
+ /cgi-bin/count.cgi: This may allow attackers to execute arbitrary commands on the server
+ /cgi-bin/echobat: This CGI may allow attackers to execute remote commands.
+ OSVDB-4517: /cgi-bin/ImageFolio/admin/admin.cgi: ImageFolio (default account Admin/ImageFolio) may allow files to be deleted via URLs like: ?cgi=remove.pl?uid=111.111.111.111&rmstep=2&catg
ory=.../.&.../.&.../.etc
+ /cgi-bin/info.cgi: This CGI allows attackers to execute commands.
+ /cgi-bin/intron.cgi: This CGI allows attackers to execute commands.
+ /cgi-bin/listrec.pl: This CGI allows attackers to execute commands on the host.
+ /cgi-bin/mailnews.cgi: Some versions allow attacker to execute commands as http daemon. Upgrade or remove.
+ /cgi-bin/mstmdtod.cgi: May allow attacker to execute remote commands. Upgrade to version 3.0.26 or higher.
+ /cgi-bin/pagelog.cgi: Some versions of this allow you to create system files. Request 'pagelog.cgi?name=.../.../.../.../tmp/filename' to try.
+ /cgi-bin/perl?-v: Perl is installed in the CGI directory. This essentially gives attackers a system shell. Remove Perl from the CGI dir.
+ /cgi-bin/perl-exe.v: Perl is installed in the CGI directory. This essentially gives attackers a system shell. Remove perl.exe from the CGI dir.
+ /cgi-bin/perl.exe: Perl is installed in the CGI directory. This essentially gives attackers a system shell. Remove perl from the CGI dir.
+ /cgi-bin/perl: Perl is installed in the CGI directory. This essentially gives attackers a system shell. Remove Perl from the CGI dir.
+ /cgi-bin/plasmal: This CGI may allow attackers to execute commands remotely.
+ OSVDB-10944: /cgi-bin/scripts/slxweb.dll/getfile?type=library&file=invalidfilename: salesLogix WebClient may allow attackers to execute arbitrary commands on the host. See http://www.sec
urityfocus.com/archive/1/378637
+ OSVDB-10944: /cgi-bin/scripts/slxweb.dll/getfile?type=library&file=invalidfileNikto: salesLogix WebClient may allow attackers to execute arbitrary commands on the host. See http://www.sec
urityfocus.com/archive/1/378637
+ /cgi-bin/smartssearch.cgi?keywords=/bin/cat%20/etc/passwd!: To check for remote execution vulnerability use 'keywords=/bin/l' or your favorite command
+ /cgi-bin/smartssearch.cgi?keywords=/bin/cat%20/etc/passwd!: To check for remote execution vulnerability use 'keywords=/bin/l' or your favorite command
+ OSVDB-50241: /cgi-bin/vipclient.cgi?username=: This CGI may be vulnerable to command injection by sending 8000 X 'A' characters. Check to see if you get a 500 error message)
+ OSVDB-10598: /cgi-bin/sscd/suncount.cgi: Sunscope CD script may allow users to execute arbitrary commands. The script was confirmed to exist, but the test was not done.
+ OSVDB-11981: /cgi-bin/viratolar.cgi: May be vulnerable to command injection, upgrade to 0.9pre2 or newer. This flaw could not be confirmed.
+ OSVDB-4454: /cgi-bin/virgil.cgi: The Virgil CGI Scanner 0.9 allows remote users to gain a system shell. This could not be confirmed (try syntax like virgil.cgi?tar-lp$zielport=31337 to op
en a connection on port 31337)
+ OSVDB-2088: /cgi-bin/vpasswd.cgi: Some versions of this CGI allow attackers to execute commands on your system. Verify this is the latest version available.
+ OSVDB-236: /cgi-bin/webgais: The webgais allows attackers to execute commands.
+ OSVDB-227: /cgi-bin/websendmail.cgi: This CGI may allow attackers to execute arbitrary commands remotely.
+ /cgi-bin/whois.cgi?action=LoadWhois=&#38;id: This script allows commands to be executed remotely.
+ /cgi-bin/wwwais: wwwais has a vulnerability that lets attackers run commands as http daemon owner. Request 'CGIDIR/wwwais?version=version=1236' and 4096 bytes of garbage.
+ /cgi-bin/common/listrec.pl: This CGI allows attackers to execute commands on the host.
+ /cgi-bin/handler: Comes with IRIX 5.3 - 6.4; allows to run arbitrary commands
+ OSVDB-235: /cgi-bin/webdist.cgi: Comes with IRIX 5.0 - 6.3; allows to run arbitrary commands
```



## 5. api.dos.aliexpress.com

```
Activities Terminal May 27 14:00 • jmax@kali:~
```

```
jmax@kali:~ x jmax@kali:~
```

```
maxKali:~$ nikto -h api.dos.aliexpress.com
Nikto v2.1.6

-----
```

```
Target IP: 47.254.143.107
Target Hostname: api.dos.aliexpress.com
Timestamp: 2021-05-27 13:47:14 (GMT+5)
Start Time: 2021-05-27 13:47:14 (GMT+5)

Server: Tengine/2.3.0
The anti-clickjacking X-Frame-Options header is not present.
The X-XSS-Protection header is not defined, no header can hint to the user agent to protect against some forms of XSS
Uncommon header 'X-Content-Type-Options' found, with contents: 'nosniff'
Uncommon header 'Expect' found, with contents: '100-continue'
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
No CGI Directories found (use '-C all' to force check all possible dirs)
Retrieved via header: wagnboard010000175a.allyun-pvc-de.devlib.net
Retrieved via header: wagnboard010000175a.allyun-pvc-de.devlib.net
Multiple index files found: /index.html, /index.aspx, /index.shtml, /index.php3, /index.php4, /index.php7, /index.pl, /default.asp, /index.cfm, /index.asp, /index.jsp, /index.php5, /index.htm

Web Server returns a valid response with junk HTTP methods, this may cause false positives.
DEBUG: HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e0e81ed1z0v5.08z29.aspx for details.
/kboard/: Kboard Forum 0.9.0 and prior have a security problem in forum_edit_post.php, forum_post.php and forum_reply.php
/listAdmin/: PHPInfo prior 2.0.0 contains numerous vulnerabilities including remote administrative access, harvesting user info and more. Default login to admin interface is admin/plist
/kboard/: Kboard Forum 0.9.0 and prior have a security problem in forum_edit_post.php, forum_post.php and forum_reply.php
/sites/: Sitepass pre 1.4.2 has multiple security problems
/sites/: Sitepass pre 1.4.2 has 'major' security problems.
/tiki/: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin
/tiki/tiki-install.php: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin
/index.php: index.php prior 1.1.1 contains a SQL injection vulnerability allowing an attacker to gain access to the MySQL database
covia-3961: /vti_birch/html.exe: Attackers may be able to crash FrontPage by requesting a DOS device, like shtml.exe/aux.htm -- a DoS was not attempted.
covia-3971: /root/: Allowed to browse root's home directory.
/cgi-bin/wrap comes with IRIX 6.2; allows to view directories
/.forums//admin/config.php: PHP Config file may contain database IDs and passwords.
/.forums//admin/config.php: PHP Config file may contain database IDs and passwords.
/.forums//admin/config/config.php: PHP Config file may contain database IDs and passwords.
/.forums//config/config.php: PHP Config file may contain database IDs and passwords
/questionbook/questionbookdat: PHP-Guestbook 1.60 Beta reveals sensitive information about its configuration.
/questionbook/pwd: PHP-Guestbook 1.60 Beta reveals the md5 hash of the admin password.
/help/: Help directory may not be accessible.
OSVDB-2411: /holo/admin/cms/htatags.php?data=/etc/data.php: Holo CMS 1.2.9-1.0 may reveal the administrator ID and password.
COVIA-4918: /inc/config_inc.php: inc/config_inc.php file could not be available via the web. Configure the web server to ignore inc files or change this to global.inc.php
OSVDB-59620: /inc/config_inc.php: Bookmark4U v1.8.3 include files are not protected and may contain remote source injection by using the 'prefix' variable.
OSVDB-59610: /inc/config_inc.php: Bookmark4U v1.8.3 include files are not protected and may contain remote source injection by using the 'prefix' variable.
OSVDB-59618: /inc/dbase.php: Bookmark4U v1.8.3 include files are not protected and may contain remote source injection by using the 'prefix' variable.
OSVDB-2703: /geeklog/users.php: Geeklog prior to 1.3.8-1sr2 contains a SQL injection vulnerability that lets a remote attacker reset admin password.
OSVDB-4246: /gb/index.php/login=true: gb uses may allow admin login by setting the value 'login' equal to 'true'.
/index.php: index.php without extension may allow arbitrary file execution
/geekaddress: This may be an indication that the server is using getaddrx for SSO
```

```
Activities Terminal May 27 14:01 • jmax@kali:~
```

```
jmax@kali:~ x jmax@kali:~
```

```
/scripts/tools/class.ide: This CGI allows remote users to view and modify SQL DB contents, server paths, docroot and more.
/.bigconf.cgi: BigIP Configuration CGI.
/.blah.htmlfile.shtml: Blah Coldfusion allows JSP source viewed through a vulnerable SSI call.
-.osvdb-4918: /vnx/style: Vignette server may reveal system information through this file.
OSVDB-17653: /SiteServer/admin/domain/domain.asp: Displays known domains of which that server is involved.
OSVDB-17654: /SiteServer/admin/commerce/foundation/driver.asp: Displays a list of installed ODBC drivers.
OSVDB-17652: /SiteServer/admin/odbcmgr/default.asp: Gives a list of selected ODBC drivers.
OSVDB-17652: /SiteServer/admin/FindServer: Used to view current search catalog configurations
/.basilli/xbox-list.php3: Basillix webmail application prior to 1.1.1 contains a XSS issue in 'message_list' function/page
/.basilli/message-read.php: Basillix webmail application prior to 1.1.1 contains a XSS issue in 'read message' page
/.clusterframe.jsp: Macromedia JRun 4 Build 61050 remote administration interface is vulnerable to several XSS attacks.
/.fb-blanks/: Blanks prior to 0.4.5 contains a XSS issue in 'fb_index' page. Previous versions contain other non-descript vulnerabilities.
/.fh-admin/submit.cgi: fh-admin may allow arbitrary command execution.
/.cartcart.cgi: If this is Dancie Shopping Cart 3.0.8 or earlier, it contains a backdoor to allow attackers to execute arbitrary commands.
OSVDB-6591: /scripts/Careollo/Careollo.dll: Careollo 1.3 may allow commands to be executed on the server by replacing hidden form elements. This could not be tested by Nikto.
/.scripts/tools/dsform.exe: Allows creation of ODBC Data Source
/.scripts/tools/dsform: Allows creation of ODBC Data Source
OSVDB-17657: /SiteServer/admin/knowledge/dang/GroupManager.asp: Used to create, modify, and potentially delete LDAP users and groups.
OSVDB-17657: /SiteServer/admin/knowledge/dang/UsersManager.asp: Used to create, modify, and potentially delete LDAP users and groups.
/.ondt/i/pgen/: iMS Merchant Server 1.0
/.readme.eml: Remote server may be infected with the Nima virus.
/.scripts/httpdabc.dll: MSProxy v1.0 Installers
/.index.php: index.php prior 1.3.2 contains a default account. Default account may be 'LDAP_Anonymous', pass is 'ldapPassword1' - see http://www.wiretrip.net/rfp/p/doc.asp?id=609.htm
/sitesee/: Sitepass pre 1.4.2 has 'major' security problems.
/.ncursesqladm/: lncs/diconnect.ine: This file should not be accessible, as it contains database connectivity information. Upgrade to version 1.2.5 or higher.
/.lisadmin/: Access to lisadmin should be restricted to localhost or allowed hosts only.
/.PG_Cart/oder.log: Shopping cart software log
/.owasp/RestrictedWebDir/: OWASP may allow restricted files to be viewed by replacing a character with its encoded equivalent.
/.neuinfo/Resin 2.1.2/Resin_2.1.2/Resin_2.1.2%00/.jsp allows any file on the system to be viewed by using \.\ directory traversal. This script may be vulnerable.
/.w-agora/.w-agora pre 4.1.6 may allow a remote user to execute arbitrary PHP scripts via URL includes in include/*.php and user/*.php files. Default account is 'admin' but password set during install.
OSVDB-42600: /vidr.php3: MySimpleNews may allow deleting of news items without authentication.
OSVDB-6181: /oficescan/cgi/egicMhMasterPw.exe: Trend Micro Officescan allows you to skip the login page and access some CGI programs directly.
/.phaser/phaser.dll: This may contain a buffer overflow. http://www.microsoft.com/technet/security/bulletin/https://docs.microsoft.com/en-us/security-updates/securitybulletins/2000/ms00-094.asp
/.pharfiled/include/ctfconv/ctfconv.php: pharfiled includes a bug where it will upload any file of any file type simply putting '.jpg' before the real file extension.
/.phbeventCalendar/file_upload.php: phbeventCalendar 1.1 and prior are vulnerable to file upload bug.
/.service/cpshost.dll: Posting acceptor possibly allows you to upload files
/.upload.asp: An ASP page that allows attackers to upload files to server
/.upload.asp: An ASP page that allows attackers to upload files to server
/.uplod.asp: An ASP page that allows attackers to upload files to server
/.uaexec: An ASP page that allows attackers to upload files to server
/.basilli/compose-attach.php3: Basillix webmail application prior to 1.1.1 contains a non-descript security vulnerability in compose-attach.php3 related to attachment uploads
/.server/: Possibly Macromedia JRun or CRX WebDAV upload
/.vgn/ac/data: Vignette CMS admin/maintenance script available.
/.vgn/ac/Delete: Vignette CMS admin/maintenance script available.
```

## 6. best.aliexpress.com



```
Activities Terminal May 27 14:53 • jmax@kali:~ [4]
jmax@kali:~ x jmax@kali:~ x jmax@kali:~ x jmax@kali:~ x jmax@kali:~ x
jmax@kali:~$ nikto -h best.aliexpress.com
Nikto v2.1.6
=====
+ Target IP:      104.84.182.239
+ Target Hostname: best.aliexpress.com
+ Target Port:    80
+ Start Time:   2021-05-27 14:02:52 (GMT5.5)
=====
+ Server: Tengine/Aserver
+ Cookie aep_usuc_f created without the httponly flag
+ Cookie e_id created without the httponly flag
+ 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: 0bb0624416221044125432907e3fa2
+ 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://best.aliexpress.com/?new_site=1
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'Tengine/Aserver' to 'AkamaiGHost' which may suggest a WAF, load balancer or proxy is in place
+ IP address found in the 'x-akamai-fwd-auth-data' header. The IP is "23.43.48.229".
+ IP address found in the 'x-akamai-fwd-auth-data' header. The IP is "212.104.236.90".
+ Uncommon header 'x-akamai-fwd-auth-sha' found, with contents: FA3A2340D7A726B51B862320685E5C7FB200AD01CE019C0803700478AC5CF00
+ Uncommon header 'x-akamai-fwd-auth-data' found, with contents: 1354871063, 23.43.48.229, 1622104542, 212.104.236.90
+ Uncommon header 'x-akamai-fwd-auth-sign' found, with contents: e1uhpLb1HxzLEG8swKvnv0XOsjnenvFO5xh09ry2qr1Kq3FECjyMnRhw0LZzBNTRHF0ic45/HV5r198Cb690DLA+cbnfmkLTsNe/c0I=
+ Cookie ali_apache_id created without the httponly flag
+ IP address found in the 'ali_apache_id' cookie. The IP is "11.10.85.99".
+ Uncommon header 'bpunish' found, with contents: 1
+ 7864 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:      2021-05-27 14:45:00 (GMT5.5) (2928 seconds)
=====
+ 1 host(s) tested
jmax@kali:~$
```

## 7. brands.aliexpress.com

```
Activities Terminal May 27 14:31 •
jmax@kali:~ jmax@kali:~ jmax@kali:~ jmax@kali:~ jmax@kali:~ jmax@kali:~ jmax@kali:~ jmax@kali:~
jmax@kali:~$ nikto -h brands.aliexpress.com
- Nikto v2.1.0
=====
+ Target IP: 47.246.137.5
+ Target Hostname: brands.aliexpress.com
+ Target Port: 80
+ Message: Multiple IP addresses found: 47.246.137.5, 47.246.137.4, 47.246.136.72, 47.246.136.71
+ Start Time: 2021-05-27 13:45:28 (GMT5.5)

+ Server: Tengine/2.3.0
+ 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: 0bb062326221033677057648ec08b
+ 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://brands.aliexpress.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Retrieved via header: global-buffer@11176099801.us08/web/302
+ Uncommon header 'x-punish' found, with contents:
+ OSVDB-28260: /vti_bin/shtml.dll/_vti_rpc?method=server+version3a482e032e282e2611: Gives info about server settings. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0413, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0749, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0710, http://www.securityfocus.com/bid/1608, http://www.securityfocus.com/bid/1174.
+ OSVDB-28260: /vti_bin/shtml.exe/_vti_rpc?method=server+version3a482e032e282e2611: Gives info about server settings.
+ OSVDB-3092: /vti_bin/_vti_au/author.dll?method=list+documents3a482e032e282e1706&serviceX5fname=&listHiddenDocs=true&listExplorerDocs=true&listRecurse=false&listFiles=true&listFolders=true&listLinkInfo=true&listIncludeParent=true&listDerivedF=false&listBorders=false: We seem to have authoring access to the FrontPage web.
+ Cookie ali_apache_id created without the httponly Flag
+ IP address found in the 'ali_apache_id' cookie. The IP is "11.176.98.51".
+ IP address found in the 'set-cookie' header. The IP is "11.176.98.51".
+ 7863 requests: 0 error(s) and 32 item(s) reported on remote host
+ End Time: 2021-05-27 14:26:10 (GMT5.5) (2442 seconds)

+ 1 host(s) tested
jmax@kali:~$
```

## 8. connectkeyword.aliexpress.com

```
Activities Terminal May 27 14:31 • jmax@kali: ~
jmax@kali:~$ nikto -h connectkeyword.aliexpress.com
Nikto v2.1.6
=====
+ Target IP:      47.254.143.107
+ Target Hostname: connectkeyword.aliexpress.com
+ Target Port:    80
+ Start Time:   2021-05-27 13:54:17 (GMT5.5)
=====
+ Server: Tengine/Aserver
+ 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: 21009dcf162210108978203144e9ead
+ 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://connectkeyword.aliexpress.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Retrieved via header: global-buffer011176098047.us08[web,302]
+ Uncommon header 'bpxunish' found, with contents: 1
+ OSVDB-28260: /_vti_bin/shtml.dll/_vti_rpc?method=serverversion%3a%2e%02e%2e2611: Gives info about server settings. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0413, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0710, http://www.securityfocus.com/bid/1608, http://www.securityfocus.com/bid/1174.
+ OSVDB-28260: /_vti_bin/shtml.exe/_vti_rpc?method=serverversion%3a%2e%02e%2e2611: Gives info about server settings.
+ OSVDB-3092: /_vti_bin/_vti_aut/author.dll?method=list+documents%3a%3e%02e%2e1706service%5fname=&listHiddenDocs=true&listExplorerDocs=true&listRecurse=false&listFiles=true&listLinkInfo=true&listIncludeParent=true&listDerivedT=false&listBorders=false: We seem to have authoring access to the FrontPage web.
+ OSVDB-3092: /_vti_bin/_vti_aut/author.exe?method=list+documents%3a%3e%02e%2e1706service%5fname=&listHiddenDocs=true&listExplorerDocs=true&listRecurse=false&listFiles=true&listLinkInfo=true&listIncludeParent=true&listDerivedT=false&listBorders=false: We seem to have authoring access to the FrontPage web.
+ 7803 requests: 0 errors(s) and 10 item(s) reported on remote host
+ End Time:    2021-05-27 14:26:54 (GMT5.5) (1997 seconds)

- 1 host(s) tested
jmax@kali:~$
```

## 9. message.aliexpress.com

```
Activities Terminal May 27 17:31 • jmax@kali: ~
jmax@kali:~$ nikto -h message.aliexpress.com
Nikto v2.1.6
=====
+ Target IP:      47.246.137.4
+ Target Hostname: message.aliexpress.com
+ Target Port:    80
+ Message:       Multiple IP addresses found: 47.246.137.4, 47.246.136.71, 47.246.136.72, 47.246.137.5
+ Start Time:   2021-05-27 13:55:18 (GMT5.5)
=====
+ Server: Tengine/Aserver
+ 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: 0bb0623d16221039584776813e1c1e
+ 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://message.aliexpress.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Retrieved via header: global-buffer011176098047.us08[web,302]
+ Uncommon header 'bpxunish' found, with contents: 1
+ OSVDB-28260: /_vti_bin/shtml.dll/_vti_rpc?method=server+version%3a%4%2e%0%2e2%2e2611: Gives info about server settings. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0413, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0710, http://www.securityfocus.com/bid/1608, http://www.securityfocus.com/bid/1174.
+ OSVDB-28260: /_vti_bin/shtml.exe/_vti_rpc?method=server+version%3a%4%2e%0%2e2%2e2611: Gives info about server settings.
+ OSVDB-3092: /_vti_bin/_vti_aut/author.dll?method=list+documents%3a%3e%02e%2e1706service%5fname=&listHiddenDocs=true&listExplorerDocs=true&listRecurse=false&listFiles=true&listLinkInfo=true&listIncludeParent=true&listDerivedT=false&listBorders=false: We seem to have authoring access to the FrontPage web.
+ OSVDB-3092: /_vti_bin/_vti_aut/author.exe?method=list+documents%3a%3e%02e%2e1706service%5fname=&listHiddenDocs=true&listExplorerDocs=true&listRecurse=false&listFiles=true&listLinkInfo=true&listIncludeParent=true&listDerivedT=false&listBorders=false: We seem to have authoring access to the FrontPage web.
+ 1 host(s) tested
jmax@kali:~$
```

## 10. passport.aliexpress.com

Activities Terminal May 27 12:26 • jmax@kali:~

```
* OSVDB-3093: /include/customize.php: This might be interesting... has been seen in web logs from an unknown scanner.
nikto v2.1.6 ~ Home
Target IP: 23.15.155.44
Target Hostname: passport.aliexpress.com
Dns Server: 127.0.0.1
Start Time: 2021-05-27 12:23:46 (GMT5.5)
Server: Tengine/2.4.4
The anti-clickjacking X-Frame-Options header is not present.
The X-XSS-Protection header is not set. This header can hint to the user agent to protect against some forms of XSS
Uncommon header 'X-pingback' found, with contents: 1
Uncommon header 'edgekey-traceid' found, with contents: 0be3745c1622098460388230e97e1
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
Uncommon header 'hw-host' found, with contents: us1lhabalogin03822083231.rg.ru.ru151
Uncommon header 'htrace-id' found, with contents: 0be3745c1622098460388230e97e1
Uncommon header 'http://www.iana.org/assignments/port-numbers'
/alive.htm [HTTP/1.1] [200]
* Site map [HTTP/1.1] [200]
* Potentially interesting archive/cert file found
* Server banner has changed from 'Tengine/2.4.4' to 'AlaminoHost' which may suggest a WAF, load balancer or proxy is in place
* passportaliexpress.jks: Potentially interesting archive/cert file found.
* passport.aliexpress.com.zip: Potentially interesting archive/cert file found.
* 23.15.155.44.pem: Potentially interesting archive/cert file found.
* passportaliexpress.tar.gz: Potentially interesting archive/cert file found.
* passportaliexpress.com.alz: Potentially interesting archive/cert file found.
* 23.15.155.44.zip: Potentially interesting archive/cert file found.
* passport.aliexpress.com.tgz: Potentially interesting archive/cert file found.
* Alipaypress.cer: Potentially interesting archive/cert file found.
* passport.aliexpress.com.cer: Potentially interesting archive/cert file found.
* Alipaypress.tar.gz: Potentially interesting archive/cert file found.
* 23.15.155.44.tar.gz: Potentially interesting archive/cert file found.
* passportaliexpress.com.pem: Potentially interesting archive/cert file found.
* passport.sql: Potentially interesting archive/cert file found.
* passport.1ma: Potentially interesting archive/cert file found.
* 23.15.155.44.sdi: Potentially interesting archive/cert file found.
* site.egg: Potentially interesting archive/cert file found.
* Alipaypress.pem: Potentially interesting archive/cert file found.
* 23.15.155.44.sql: Potentially interesting archive/cert file found.
* backup.war: Potentially interesting archive/cert file found.
* .site.tgt: Potentially interesting archive/cert file found.
* passportaliexpress.ssl: Potentially interesting archive/cert file found.
* com.pem: Potentially interesting archive/cert file found.
* passport.jks: Potentially interesting archive/cert file found.
* passport.war: Potentially interesting archive/cert file found.
* passport.aliexpress_com.pjw: Potentially interesting archive/cert file found.
* passport.aliexpress.com.cgi: Potentially interesting archive/cert file found.
```

Screenshot from 2021-05-02 20-16-03.png

Screenshot from 2021-05-03 12-25-09.png

Activities Terminal May 27 12:29 • jmax@kali:~

```
* shopa_sessionlist.asp: VP-ASP shopping cart test application is available from the web. This page may give the location of .mdb files which may also be available.
* typoconf/: This may contain sensitive TVP03 files.
* /site/typoconf/: This may contain sensitive TVP03 files.
* /typo3/vhost/typo3conf/: This may contain sensitive TVP03 files.
* /vhosts/typo3conf/database.sql: TVP03 SQL file found.
* /typo3conf/database.sql: TVP03 SQL file found.
* /typo3conf/localconf.php: TVP03 config file found.
* /site/typo3conf/localconf.php: TVP03 config file found.
* /typo3/typo3conf/config.php: TVP03 config file found.
* /typo3/typo3conf/ext/t3lib/class/t3lib_file.php: TVP03 config file found.
* /typo3/typo3conf/ext/t3lib/class/t3lib_file_ext.php: TVP03 config file found.
* /webcart-lite/orders/report.txt: This may allow attackers to read credit card data. Reconfigure to make this file not accessible via the web.
* /webcart/config/: This may allow attackers to read credit card data. Reconfigure to make this dir not accessible via the web.
* /webcart/orders/: This may allow attackers to read credit card data. Reconfigure to make this dir not accessible via the web.
* /ws_ftp.ini: Can contain saved passwords for FTP sites.
* /perl/cgi-bin/cgi-bin.cgi: This is the default cgi-bin (CGI) schema, including host and port.
* /ws_ftp/: /usr/local/bsm/ftp: Expose various LAMP service and backend configuration parameters
OSVDB-17059: /scripts/Admin/Account/Change.asp: Expose various LAMP service and backend configuration parameters
OSVDB-17062: /SiteServer/Admin/knowledge/personal/VspFnrdn1.asp: Expose various LAMP service and backend configuration parameters
OSVDB-17062: /SiteServer/Admin/knowledge/personal/VspFnrdn1.asp: Expose various LAMP service and backend configuration parameters
OSVDB-17062: /SiteServer/Admin/knowledge/personal/VspFnrdn1.asp: Expose various LAMP service and backend configuration parameters
OSVDB-17062: /SiteServer/Admin/knowledge/personal/VspFnrdn1.asp: Expose various LAMP service and backend configuration parameters
* whatever.htm: May reveal physical path. http files may also be vulnerable to an off-by-one overflow that allows remote command execution (see https://docs.microsoft.com/en-us/security-updates/securitybulletins/2002/M002-018)
* /nsm/dlr/ShowVolume: You can use ShowVolume and ShowDirectory directly on the Novell server (NDS).1 to view the filesystem without having to log in
* /nsm/blank.html: iMail4Mail 0.8.10 contains an XSS vulnerability. Previous versions contain other non-descript vulnerabilities.
* /servlet/jrunsever/execute: It may be possible to crash Java by requesting '/cgi/cgisproc'. (not attempted). Upgrade to version 2.0.0 or later.
* /perl/-e$20print$20Hello1: The Perl Interpreter on the Novell system may allow any command to be executed. See http://www.securityfocus.com/bid/5520. Installing Perl 5.6 might fix this issue.
OSVDB-6446: /quikstore.cgi: Shopping cart config file, http://www.quikstore.com/, http://www.mindsec.com/advisories/post2.txt
* /securecontrolpanel/: Web Server Control Panel
* /webmail1/: web based mail package installed.
* /webmail1/~/: Pan directory found.
* /cabinet/~/Pan directory found.
Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
* /nsm/_33CuUtil/del.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
* /nsm/_33CuUtil/dbsrawse.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
* /nsm/_33CuUtil/lancard.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
* /nsm/_33CuUtil/rdbas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
* /nsm/_33CuUtil/selb.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
* /nsm/_33CuUtil/slstat.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
* /nsm/_33CuWeb/fdir.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
* /nsm/_33CuWebdemofdir.bas: Netbase util access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
* /rnd/_33CuServer: Can allow directory listings by requesting /rnd/directory. Upgrade to a later version and secure according to the documents on the NDS web site.
* /vtree: NDS Server reveals the entire web root structure and files via this URL. Upgrade to a later version and secure according to the documents on the NDS web site.
* /contents/extensions/asp1/: The IIS system may be vulnerable to a DOS, see https://docs.microsoft.com/en-us/security-updates/securitybulletins/2002/M002-018 for details.
* /cgi-bin/ncsh: nsh.exe: win-e-sample.exe has a buffer overflow
* /msf//wint/win.ini: this win.ini file can be downloaded.
* /cgi-bin/cgi-process: WASD reveals a lot of system information in this script. It should be removed.
* /vtree: WASD Server reveals the entire web root structure and files via this URL. Upgrade to a later version and secure according to the documents on the WASD web site.
* /Contents/extensions/asp1/: The IIS system may be vulnerable to a DOS, see https://docs.microsoft.com/en-us/security-updates/securitybulletins/2002/M002-018 for details.
* /cgi-bin/ncsh: nsh.exe: win-e-sample.exe has a buffer overflow
* /msf//wint/win.ini: this win.ini file can be downloaded.
```

## 11. womenmenclothes439106.aliexpress.com

```

Activities Terminal May 27 13:33 • jmax@kali:-
jmax@kali:~ nikto -h womenmenclothes439106.aliexpress.com
- Nikto v2.1.6
-----[REDACTED]-----[REDACTED]
+ Target IP: 47.254.143.112
+ Target Hostname: womenmenclothes439106.aliexpress.com
+ Target Port: 80
+ Start Time: 2021-05-27 13:26:03 (GMT5.5)
+ Server: engine/AsServer
+ 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 'x-punish-traceid' found, with contents: 2100bb5116221022028e92134ed4aa
+ 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
+ No CGI Directories found (use '-c all' to force check all possible dirs)
+ Retrieved via header: sebridge033000189227.de81[web_302]
+ Retrieved access-control-allow-origin header: example.com
+ Multiple index files found: /index.cfm, /index.xml, /index.do, /index.shtml, /index.cgi, /index.pl, /index.jsp, /default.asp, /default.aspx, /index.aspx, /index.php5, /index.asp, /index.php, /index.php3, /index.htm, /index.shtml, /index.php4, /index.html, /default.htm, /index.php7
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdhx28VS.80%29.aspx for details.
+ /kboard/: Kboard Forum 0.3.0 and prior have a security problem in forum_edit_post.php, forum_post.php and forum_reply.php
+ /lists/admin/: PHPList pre 2.6.4 contains a number of vulnerabilities including remote administrative access, harvesting user info and more. Default login to admin interface is admin/phpList
+ /splashAdmin.php: Cobalt Cube 3 admin is running. This may have multiple security problems as described by www.scan-associates.net. These could not be tested remotely.
+ /ssdefns/: Siteseed pre 1.4.2 has 'major' security problems.
+ /sshone/: Siteseed pre 1.4.2 has 'major' security problems.
+ /tiki/: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin
+ /tiki/tiki-install.php: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin
+ /scripts/samples/details.idc: See RFP 9901: www.wiretrip.net
+ 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.
+ OSVDB-637: /root/: Allowed to browse root's home directory.
+ /cgi-bin/wrap: come with IRIX 6.2; allows to view directries
+ /forums/admin/config.php: PHP Config file may contain database IDs and passwords.
+ /forums/admin/config.php: PHP Config file may contain database IDs and passwords.
+ /forums/admin/config.php: PHP Config file may contain database IDs and passwords.
+ /forums/admin/config.php: PHP Config file may contain database IDs and passwords.
+ /forums/config.php: PHP Config file may contain database IDs and passwords.
+ /guestbook/guestbookdat: PHP-Gastebuch 1.0 Beta reveals sensitive information about its configuration.
+ /guestbook/pwd: PHP-Gastebuch 1.0 Beta reveals the md5 hash of the admin password.
+ /help/: Help directory should not be accessible
+ OSVDB-2411: /hola/admin/cms/htmltags/dateis.../sec/dateis.php: hola-cms 1.2.9-10 may reveal the administrator ID and password.
+ OSVDB-8103: /globalinc: PHP-Survey's include file should not be available via the web. Configure the web server to ignore .inc files or change this to global.inc.php
+ OSVDB-59620: /inc/common_load.php: Bookmark4U v1.8.3 include files are not protected and may contain remote source injection by using the 'prefix' variable.
+ OSVDB-59621: /inc/common_load.php: Bookmark4U v1.8.3 include files are not protected and may contain remote source injection by using the 'prefix' variable.

```

```

Activities Terminal May 27 13:34 • jmax@kali:-
jmax@kali:~ jmax@kali:~ jmax@kali:-
-----[REDACTED]-----[REDACTED]
+ OSVDB-15971: /MIDICART/midicart.mdb: MIDICART database is available for browsing. This should not be allowed via the web server.
+ OSVDB-41850: /mpcssoftweb_guestbook/database/mpcssoftweb_guestdata.mdb: MPCSoftWeb Guest book passwords retrieved.
+ /news/news.mdb: Web Wiz Site News release v3.00 admin password database is available and unencrypted.
+ OSVDB-53413: /shopping300.mdb: VP-ASP shopping cart application allows .mdb files (which may include customer data) to be downloaded via the web. These should not be available.
+ OSVDB-53413: /shopping400.mdb: VP-ASP shopping cart application allows .mdb files (which may include customer data) to be downloaded via the web. These should not be available.
+ OSVDB-15971: /shoppingdirectory/midicart.mdb: MIDICART database is available for browsing. This should not be allowed via the web server.
+ OSVDB-3398: /database/4dbase.mdb: Mac Web Portal database is available remotely. It should not be moved from the default location to a directory outside the web root.
+ /admin/config/config.php: Config file may contain database IDs and passwords.
+ /admin/config.php: PHP Config file may contain database IDs and passwords.
+ /administrator/config.php: PHP Config file may contain database IDs and passwords.
+ /contents.php?new_language=elvish&mode=select: Requesting a file with an invalid language selection from DC Portal may reveal the system path.
+ OSVDB-6467: /ow/stormgr.pws: Encrypted ID/Pass for Mercantec's SoftCart, http://www.mercantec.com/, see http://www.mindsec.com/advisories/post2.txt for more information.
+ /servlet/com.livesoftware.jrun.jsp: Allaire ColdFusion allows JSP source viewed through a vulnerable SSL filter.
+ /shopa_sessionlist.asp: VP-ASP shopping cart test application is available from the web. This page may give the location of .mdb files which may also be available.
+ OSVDB-53303: /simplesb/users/users.php: Simple BBS 1.0.6 allows user information and passwords to be viewed remotely.
+ /typo3conf/: This may contain sensitive TYPO3 files.
+ /cms/typo3conf/: This may contain sensitive TYPO3 files.
+ /site/typo3conf/: This may contain sensitive TYPO3 files.
+ /typo3/typo3conf/: This may contain sensitive TYPO3 files.
+ /typo3/typo3conf/: This may contain sensitive TYPO3 files.
+ /typo3conf/database.sql: TYPO3 SQL file found.
+ /cms/typo3conf/database.sql: TYPO3 SQL file found.
+ /site/typo3conf/database.sql: TYPO3 SQL file found.
+ /typo3/typo3conf/database.sql: TYPO3 SQL file found.
+ /typo3/typo3conf/database.sql: TYPO3 SQL file found.
+ /typo3/typo3conf/localconf.php: TYPO3 config file found.
+ /cms/typo3conf/localconf.php: TYPO3 config file found.
+ /site/typo3conf/localconf.php: TYPO3 config file found.
+ /typo3/typo3conf/localconf.php: TYPO3 config file found.
+ /typo3/typo3conf/localconf.php: TYPO3 config file found.
+ OSVDB-53380: /vchat/msg.txt: vchat allows user information to be retrieved.
+ OSVDB-53380: /vchat/msg.txt: vchat allows user information to be retrieved.
+ /webcart/lite/sign/license: Signetech server license file found.
+ /webcart/lite/orders/import.txt: This may allow attackers to read credit card data. Reconfigure to make this file not accessible via the web.
+ /webcart/carts/: This may allow attackers to read credit card data. Reconfigure to make this dir not accessible via the web.
+ /webcart/config/: This may allow attackers to read credit card data. Reconfigure to make this dir not accessible via the web.
+ /webcart/orders/: This may allow attackers to read credit card data. Reconfigure to make this dir not accessible via the web.
+ /webcart/orders/import.txt: This may allow attackers to read credit card data. Reconfigure to make this file not accessible via the web.
+ /webcart/orders/: This may allow attackers to read credit card data. Reconfigure to make this dir not accessible via the web.
+ /ws_ftp.ini: Can contain saved passwords for FTP sites
+ /WS_FTP.ini: Can contain saved passwords for FTP sites
+ /_mc_bin/auoconfig.asp: Displays the default AD (LDAP) schema, including host and port.
+ OSVDB-17659: /SiteServer/Admin/knowledge/persmbr/vs.asp: Expose various LDAP service and backend configuration parameters

```

```
+ 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...
```

## 12.zhouyun19930515.aliexpress.com

```
Activities Terminal • May 27 13:19 • jmax@kali: ~
jmax@kali: ~
jmax@kali: ~
jmax@kali: ~

jmax@kali: -# nmap -n zhouyun19930515.aliexpress.com
nmap v2.1.6
[...]
Target IP: 47.254.143.107
Target Hostname: zhouyun19930515.aliexpress.com
Start Port: 80/tcp
Start Time: 2021-05-27 13:00:00 (GMT5.5)
[...]
Server: Tengine/2.2.0
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
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
Uncommon header 'eagles-traceid' found, with contents: 0bba9db462e22f01127790599e5a7
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
CGI Directories found (use '-C all' to force check all possible dirs)
Retrieved via header: adebridge@3:0001@0236.debian:web_302
Retrieved via header: adebridge@3:0001@0236.debian:web_302
Multiple unique file origins found: niko:example.com
Multiple unique file origins found: index.php, /index.php4, /index.asp, /index.xml, /index.php3, /default.htm, /index.aspx, /index.jsp, /index.shtml, /index.pl, /default.aspx, /index.htm, /index.cgi, /index.do, /default.asp, /index.html, /index.php7, /index.php
Web Server returns a valid response with junk HTTP methods, this may cause false positives.
DEBUG: HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/ee281652.aspx for details.
[...]
Folder is Empty
```

```
Activities Terminal • May 27 13:21 • jmax@kali: ~
jmax@kali: ~
jmax@kali: ~
jmax@kali: ~

jmax@kali: ~
jmax@kali: ~
jmax@kali: ~

+ OSVDB-3093: /topic/enetice.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /topsitesdir/edit.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /ttforum/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /tutos/file/file_new.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /tutos/file/file_select.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /typo3/dev/translations.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /typo3/dev/translations.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /typo3/dev/translations.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /typo3fc/MultiFileUploadHandler.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /url.jsp: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /vbulletin/submit.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /vars.inc: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /vbulletin/add-subject.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /vbulletin/profile.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /vbulletin/reply.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /webcalendar/login.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /webmail/lib/emailruler_execute_on_each_page.inc.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /web_app/WEB-INF/webapp.properties: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /XMBforum/buddy.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /XMBforum/member.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /stat_admin.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /ybabsse/Reminder.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /ybabsse/Passcode.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /ycctrack/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /_head.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /ows-bin/oakskill.exe?7abcde.exe: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /ows-bin/oaknetconf.exe?7-lz20-sx2e0lahMlh: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3093: /www.aci: Contains authorization information
+ OSVDB-3093: /.www_aci: Contains authorization information
+ OSVDB-3093: /.htpasswd: Contains authorization information
+ OSVDB-3093: /.access: Contains authorization information
+ OSVDB-3093: /addressbook: PINE addressbook, may store sensitive e-mail address contact information and notes
+ OSVDB-3093: /.bashrc: User home dir was found with a shell config file. This may reveal file and path information.
+ OSVDB-3093: /.forward: File found in user's home directory, may reveal where the user's mail is being forwarded to.
+ OSVDB-3093: /.history: User's home directory may be sent to the web host, the shell history was retrieved. This should not be accessible via the web.
+ OSVDB-3093: /.htaccess: Contains configuration and/or authorization information
+ OSVDB-3093: /.lynx_cookies: User home dir found with LYNX cookie file. May reveal cookies received from arbitrary web sites.
```

# 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.

The screenshot shows the Zenmap interface with the following details:

- Activities**: Zenmap
- Date/Time**: May 3 15:37
- Scan Type**: Intense scan
- Target**: 47.254.177.101
- Command**: nmap -T4 -A -v 47.254.177.101
- Host Status**: OS: 47.254.177.101
- Log Output** (scrollable):
  - Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-03 13:52 +0530
  - NSE: Loaded 153 scripts for scanning.
  - NSE: Script Pre-scanning.
  - Initiating NSE at 13:52
  - Completed NSE at 13:52, 0.00s elapsed
  - Initiating NSE at 13:52
  - Completed NSE at 13:52, 0.00s elapsed
  - Initiating NSE at 13:52
  - Completed NSE at 13:52, 0.00s elapsed
  - Initiating NSE at 13:52
  - Completed NSE at 13:52, 0.00s elapsed
  - Initiating Ping Scan at 13:52
  - Scanning 47.254.177.101 [4 ports]
  - Completed Ping Scan at 13:52, 0.04s elapsed (1 total hosts)
  - Initiating Parallel DNS resolution of 1 host. at 13:52
  - Completed Parallel DNS resolution of 1 host. at 13:52, 3.09s elapsed
  - Initiating SYN Stealth Scan at 13:52
  - Scanning 47.254.177.101 [1000 ports]
  - Discovered open port 21/tcp on 47.254.177.101
  - Discovered open port 80/tcp on 47.254.177.101
  - Discovered open port 443/tcp on 47.254.177.101
  - Completed SYN Stealth Scan at 13:52, 16.71s elapsed (1000 total ports)
  - Initiating Service scan at 13:52
  - Scanning 3 services on 47.254.177.101
  - Completed Service scan at 13:55, 156.47s elapsed (3 services on 1 host)
  - Initiating OS detection (try #1) against 47.254.177.101
  - Retrying OS detection (try #2) against 47.254.177.101
  - Initiating Traceroute at 13:55
  - Completed Traceroute at 13:55, 0.02s elapsed
  - Initiating Parallel DNS resolution of 2 hosts. at 13:55
  - Completed Parallel DNS resolution of 2 hosts. at 13:55, 2.92s elapsed
  - NSE: Script scanning 47.254.177.101.
  - Initiating NSE at 13:55
  - Completed NSE at 13:56, 62.36s elapsed
  - Initiating NSE at 13:56
  - Completed NSE at 13:57, 70.31s elapsed
  - Initiating NSE at 13:57
  - Completed NSE at 13:57, 0.00s elapsed
  - Nmap scan report for 47.254.177.101
  - Host is up (0.0025s latency).
  - 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
- Services Table**:

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	
80/tcp	open	http	Tengine httpd Aserver
443/tcp	open	ssl/http	Tengine httpd Aserver

```

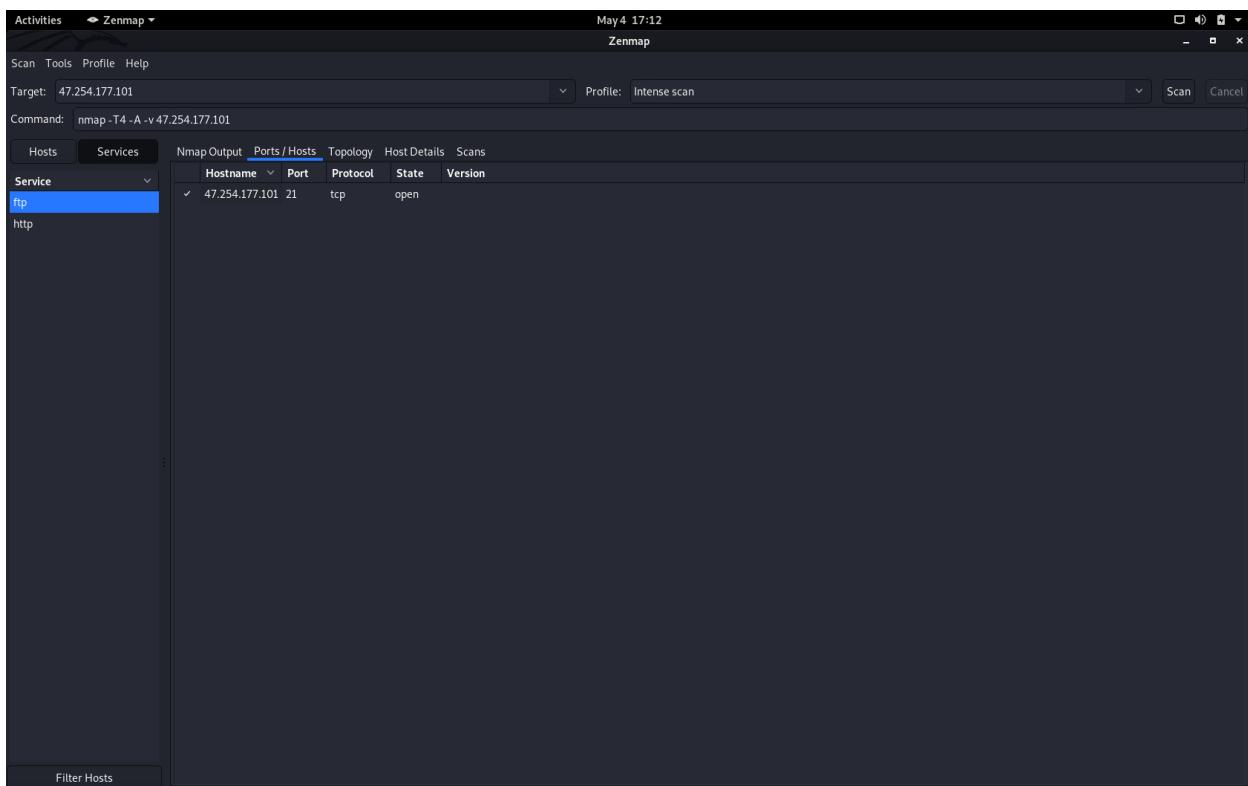
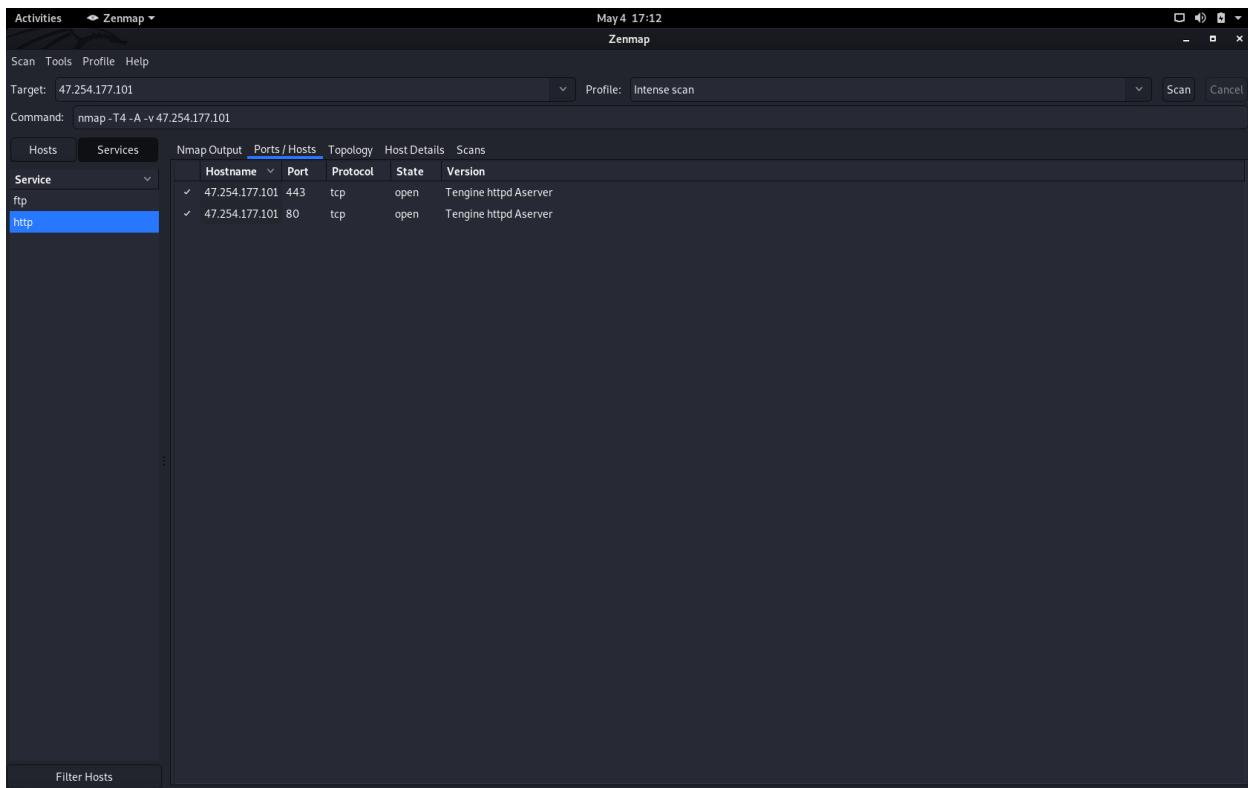
Activities → Zenmap ▾ May 3 15:37
Scan Tools Profile Help
Target: 47.254.177.101 Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v 47.254.177.101
Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans
OS Host Not shown: 997 filtered ports
PORT STATE SERVICE VERSION
47.254.177.101
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.1ntao.com,DNS=click.mz.simba.taobao.com,DNS=click.tz.simba.taobao.com,DNS=gsp.mystg.taobao.com,DNS=pre-unzyun.api.xspace.taobao.com,DNS=lijiapiao.trip.taobao.com,DNS=jipiao.trip.taobao.com,DNS=showcase.display.taobao.com,DNS=smatch.simba2.taobao.com,DNS=trace.ctaobao.com,DNS=ugc.preview.com,DNS=unzyun.api.xspace.taobao.com,DNS=110.100.100.100,DNS=123.taobao.com,DNS=admin.dataset.taobao.com,DNS=alicom.taobao.com,DNS=alidesign.taobao.com,DNS=alidetail.taobao.com,DNS=alimail.taobao.com,DNS=alihealth.taobao.com,DNS=aliijk.taobao.com,DNS=alimebot.taobao.com,DNS=alimebot.taobao.ts,DNS=alilinqin.taobao.com,DNS=alisp.admin.taobao.com,DNS=alisports.taobao.com,DNS=alisc.taobao.com,DNS=aliscd.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
1100cfm.taobao.com,DNS=astore-alsc.taobao.com,DNS=astore-multitenant.taobao.com,DNS=buks.m.taobao.com,DNS=budcase-es-old.taobao.com,DNS=bciahuina.taobao.com,DNS=bxiaolian.taobao.com,DNS=bhs.taobao.com,DNS=bhctg.taobao.com,DNS=bhfeedback.taobao.com,DNS=bhops.taobao.tw,DNS=bot.taobao.com,DNS=brand.taobao.com,DNS=branding.taobao.com,DNS=bs.browser.taobao.com,DNS=buildsite.taobao.com,DNS=caipiao.taobao.com,DNS=cbsb.taobao.com,DNS=cdn.taobao.com,DNS=china.taobao.com,DNS=chuangyi.taobao.com,DNS=click.taobao.com,DNS=cloud.taobao.com,DNS=cloudmall.taobao.com,DNS=config.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=datarenmcn.taobao.com,DNS=daxue.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=dianyting.taobao.com,DNS=dmp.taobao.com,DNS=dongfeng.taobao.com,DNS=ds.taobao.com,DNS=dsc.taobao.com,DNS=fengchao.dtm.taobao.com,DNS=fliggy.taobao.com,DNS=fuwu.taobao.com,DNS=fuwebapp.taobao.com,DNS=game.taobao.com,DNS=gds.taobao.com,DNS=global.j56.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=156.taobao.com,DNS=intl.taobao.com,DNS=istore.taobao.com,DNS=item.taobao.com,DNS=jilangu.taobao.com,DNS=jiu.taobao.com,DNS=juadmin.taobao.com,DNS=julang.taobao.com,DNS=lazada.taobao.com,DNS=lba.taobao.com,DNS=life.taobao.com,DNS=lingshou.taobao.com,DNS=linking-test.taobao.com,DNS=luban.taobao.com,DNS=lz.taobao.com,DNS=ma.taobao.com,DNS=manager.taobao.com,DNS=marketingbox.taobao.com,DNS=mpop.taobao.com,DNS=mta.taobao.com,DNS=meta.search.taobao.com,DNS=maojie.taobao.com,DNS=ml.taobao.com,DNS=movie.taobao.com,DNS=mymall.taobao.com,DNS=mymallonline.taobao.com,DNS=nextbit.taobao.com,DNS=now.taobao.com,DNS=ny.taobao.com,DNS=o2o.taobao.com,DNS=o2ooverseas.taobao.com,DNS=o2oweb.taobao.com,DNS=pan.taobao.com,DNS=password.taobao.com,DNS=pay.taobao.com,DNS=pinpai.taobao.com,DNS=pmcrm.taobao.com,DNS=polaris.taobao.com,DNS=prada.taobao.com,DNS=pre-huoxue.taobao.com,DNS=pre-repol-git-jae.taobao.com,DNS=pre-tcgv.taobao.com,DNS=prerealhealth.taobao.com,DNS=prepmb.taobao.com,DNS=prepub.taobao.com,DNS=proxy.taobao.com,DNS=publish.taobao.com,DNS=qlanni.tao.com,DNS=qtaobao.com,DNS=qtaobao.com,DNS=qtaobao.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=secondlife.taobao.com,DNS=seller.taobao.com,DNS=sellercenter-staging.taobao.tw,DNS=sellercenter.taobao.com,DNS=settle.taobao.com,DNS=sh.taobao.com,DNS=shop.taobao.com,DNS=shuyuan.taobao.com,DNS=simba.taobao.com,DNS=solar.taobao.com,DNS=sopabi.taobao.com,DNS=specch.taobao.com,DNS=stadium.taobao.com,DNS=survey.taobao.com,DNS=sync.ct.taobao.com,DNS=solar.taobao.com,DNS=tai.taobao.com,DNS=tai.e.taobao.com,DNS=taiqlive.cp.taobao.com,DNS=tiaopiopiao.com,DNS=tiaosheshui.taobao.com,DNS=tiaotv.taobao.com,DNS=tiaoxiagpu.taobao.com,DNS=tfcgw.taobao.com,DNS=itemai.taobao.com,DNS=tft.taobao.com,DNS=themis.taobao.com,DNS=timesheet.taobao.com,DNS=trade.tw.taobao.com,DNS=train.taobao.com,DNS=trip.taobao.com
Issuer: commonName=GlobalSign Organization Validation CA - SHA256 - G2/OrganizationName=GlobalSign nv-sa/countryName=BE
Public Key type: ecP
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 f4aa b464 f843 850c 9eef fida e4e0
SHA-1: 53ea 3472 a057 59d9 dcdf 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%), OEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), OEMU 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)

```

```

Activities → Zenmap ▾ May 4 17:11
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
47.254.177.101
taopiao.piao.com,DNS=taosheshui.taobao.com,DNS=tiaoxiaoapu.taobao.com,DNS=tcmg.taobao.com,DNS=tmai.taobao.com,tf.taobao.com,DNS=themis.taobao.com,DNS=timesheet.taobao.com,DNS=trade.tw.taobao.com,DNS=train.taobao.com,DNS=trip.taobao.com,try.taobao.com,DNS=tv.taobao.com,DNS=tw.taobao.com,DNS=tuland.taobao.com,DNS=tump.taobao.com,DNS=tupload.taobao.com,ut.taobao.com,DNS=tuz.taobao.com,DNS=video.taobao.com,DNS=tvip.taobao.com,DNS=tvirtualbuy.taobao.com,DNS=twangpu.taobao.com,webapp.taobao.com,DNS=twork.taobao.com,DNS=tworld.taobao.com,DNS=tws-nextbit.taobao.com,DNS=twuli.tao.com,weipixi.taobao.com,DNS=twox.taobao.com,DNS=txsconsultant.taobao.com,DNS=tuxue.taobao.com,DNS=txw.tao.com,DNS=tuxiangqing.taobao.com,DNS=tuxue.taobao.com,yingxiao.taobao.com,DNS=tuerkou.taobao.com,DNS=tukeke.taobao.com,DNS=tuleiba.taobao.com,DNS=tun.yt.taobao.com,bb.taobao.com,DNS=tunzhni.taobao.com,DNS=tupiopiao.com,DNS=tzamii.com,DNS=tobac.com
Issuer: commonName=GlobalSign Organization Validation CA - SHA256 - G2/OrganizationName=GlobalSign nv-sa/countryName=BE
Public Key type: ecP
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 f4aa b464 f843 850c 9eef fida e4e0
SHA-1: 53ea 3472 a057 59d9 dcdf 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%), OEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), OEMU 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)

```



# 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.

```
Activities Terminal May 22 17:19 • jmax@kali: ~
wafw00f: error: No valid target specified. jmax@kali: ~ | Download Nessus | Term | GitHub - EnableSecurity | + [+] https://github.com/EnableSecurity/wafw00f
example: wafw00f http://www.victim.org/
[Kali Linux] [Kali Training] [Kali Tools] [Kali Docs] [Kali Forums] [NetHunter] [Offensive Security] [Exploit-DB] [GHDDB] [MSFU]
Options:
-h, --help show this help message and exit
--version print version information, multiple --version options increase verbosity
-a, --findall Find all WAFs which match the signatures, do not stop testing on the first one. Actions
--noredirect Do not follow redirections given by 3xx responses
-t TEST, --test=TEST Test for one specific WAF
-o OUTPUT, --output=OUTPUT Write output to csv, json or text file depending on file extension. For stdout, specify - as filename
-i INPUT, --input=FILE<INPUT>
Read targets from a file. Input format can be csv, json or text, for csv and JSON, 'waf' column name or element is required.
-l, --list List all WAFs that WAFW00F is able to detect
-p PROXY, --proxy=PROXY
Use an HTTP proxy to perform requests, examples:
http://hostname:8080, socks5://hostname:1080,
http://user:pass@hostname:8080
-V, --version Print out the current version of WAFW00F and exit.
-H HEADERS, --headers=HEADERS
Pass custom headers via a text file to overwrite the default header set.
jmax@kali: ~$ wafw00f https://aliexpress.com
[+] Checking https://aliexpress.com
[*] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
jmax@kali: ~

Activities Terminal May 22 17:26 • jmax@kali: ~
-V, --version Print out the current version of WAFW00F and exit.
-H HEADERS, --headers=HEADERS
Pass custom headers via a text file to overwrite the default header set.
jmax@kali: ~$ wafw00f https://aliexpress.com
[+] Checking https://aliexpress.com
[*] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
jmax@kali: ~$ wafw00f https://ymdk.aliexpress.com
[+] Checking https://ymdk.aliexpress.com
[*] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
jmax@kali: ~$ wafw00f https://ask.aliexpress.com
[+] Checking https://ask.aliexpress.com
[*] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7
jmax@kali: ~
```

## 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.

Advanced Web application firewall detection

Web Application Firewall Detection Discover the security protecting your target

https://www.aliexpress.com Detect

Host	Ip	WAF Detected
https://www.aliexpress.com		No waf found

Some common web application firewall

- CloudFront
- Cloudflare
- Incapsula
- MaxCDN
- Edgecast
- Distil Networks
- Sucuri
- Reblaze

Osint Tools

Bug Bounty Tools

Resources

Type here to search

Advanced Web application firewall detection

Web Application Firewall Detection Discover the security protecting your target

https://www.aliexpress.com Detect

Host	Ip	WAF Detected
https://www.aliexpress.com		No waf found

Some common web application firewall

- CloudFront
- Cloudflare
- Incapsula
- MaxCDN
- Edgecast
- Distil Networks
- Sucuri
- Reblaze

Osint Tools

Bug Bounty Tools

Resources

Type here to search

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



```
Activities Terminal May22 18:35 •
jmax@kali:~$ nmap -p443 --script http-waf-detect www.aliexpress.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-22 18:34 +0530
Nmap scan report for www.aliexpress.com (104.84.182.239)
Host is up (0.11s latency).
DNS record for 104.84.182.239: a104-84-182-239.deploy.static.akamaitechnologies.com

PORT      STATE SERVICE
443/tcp    open  https
| http-waf-detect: IDS/IPS/WAF detected:
|_ www.aliexpress.com:443/?p4y104d3<script>alert(document.cookie)</script>

Nmap done: 1 IP address (1 host up) scanned in 4.44 seconds
jmax@kali:~$ nmap -p80 --script http-waf-detect www.aliexpress.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-22 18:35 +0530
Nmap scan report for www.aliexpress.com (104.84.182.239)
Host is up (0.14s latency).
DNS record for 104.84.182.239: a104-84-182-239.deploy.static.akamaitechnologies.com

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 8.42 seconds
jmax@kali:~$
```

# 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 its behavior using help command.

```
Activities Terminal • May 22 19:59 • Screenshots from 2021-05-22 11:38-10.png
max@kali:~$ dnsrecon -h
usage: dnsrecon [-h] [-D DOMAIN] [-F RANGE] [-D DICTIONARY] [-F] [-o] [-s] [-b] [-y] [-k] [-w] [-l] [-t threads THREADS] [--lifetime LIFETIME] [--tcp] [--db DB] [-x XML] [-c CSV] [-j JSON] [--lw]
                 [-r] [-s SERVER] [--disable_check_recursion] [--disable_check_bindversion] [-v] [-t TYPE]
optional arguments:
-h, --help            show this help message and exit 22:19...
--version             show program's version number and exit
-D DOMAIN, --domain DOMAIN
                     Target domain.
-n NS_SERVER, --name_server NS_SERVER
                     Domain server to use. If none is given, the SOA of the target will be used. Multiple servers can be specified using a comma separated list.
--r RANGE, --range RANGE
                     IP range for reverse lookup brute force in formats (first-last) or in (range/bitmask), and wildcards.
-D DICTIONARY, --dictionary DICTIONARY
                     Dictionary file of subdomain and hostnames to use for brute force. Filter out of brute force domain lockup, records that resolve to the wildcard defined IP address when saving records.
-F Filter out domain lockup records, records that resolve to the wildcard defined IP address when saving records.
-o Output XML file to save found records.
-s st_SrvProbe, --st_SrvProbe
                     Perform a reverse lookup of IP ranges in the SPF record with standard enumeration.
-y Perform Bing enumeration with standard enumeration.
-v Perform Yandex enumeration with standard enumeration.
-w Perform crt.sh enumeration with standard enumeration.
-x Perform crt.sh deep whois record analysis and reverse lookup of IP ranges found through Whois when doing a standard enumeration.
-t threads THREADS
                     Number of threads to use in reverse lookups, forward lookups, brute force and SRV record enumeration.
--lifetime LIFETIME
                     Time to wait for a server to respond to a query, default is 3 seconds.
--tcp
                     Use TCP protocol to make queries.
--db DB
                     SQLite 3 file to save found records.
--x XML, --xml XML
                     XML file to save found records.
--c CSV, --csv CSV
                     Save output to a comma separated value file.
--j JSON, --json JSON
                     Save output to a JSON file.
--lw
                     Continue brute forcing a domain even if a wildcard records are discovered, wait for a server to respond to a query, default is 3 seconds.
--disable_check_recursion
                     Disables check for recursion on name servers.
--disable_check_bindversion
                     Disables check for BIND version on name servers.
-v
                     Enable verbose output.
-t TYPE, --type TYPE
                     Type of enumeration to perform: std: SOA, NS, A, AAAA, MX and SRV; rvl: Reverse lookup of a given CIDR or IP range; brt: Brute force domains and hosts using a given dictionary; srv: Perform SRV record enumeration for subdomains and hosts; yand: Perform Yandex search for subdomains and hosts; crt: Perform crt.sh enumeration for subdomains and hosts; snoop: Perform WHOIS enumeration for subdomains and hosts; zonewalk: Perform a DNSSEC zone walk using NSEC records.
```

After scanning I could enumerate following Domain name services.

```
Activities Terminal May 22 19:50 •
jmax@Kali:~$ dnsrecon -d aliexpress.com
[*] Performing General Enumeration of Domain: aliexpress.com
[+] Wildcard resolution is enabled on this domain
[+] Aliexpress.com is resolved to adwildcardproxy.aliexpress.com
[+] Aliexpress.com will resolve this domain
[-] DNSSEC is not configured for aliexpress.com
[*] SOA ns1.alibabadns.com 198.11.138.254
[*] SOA ns1.alibabadns.com 106.11.35.19
[*] SOA ns1.alibabadns.com 140.205.07.252
[*] SOA ns1.alibabadns.com 140.205.322.66
[*] NS ns1.alibabadns.com 198.11.138.254
[*] NS ns1.alibabadns.com 106.11.35.19
[*] NS ns1.alibabadns.com 140.205.67.252
[-] Recursion enabled
NS Server 140.205.67.252
NS ns1.alibabadns.com 140.205.122.66
NS ns2.alibabadns.com 198.11.138.252
NS ns2.alibabadns.com 106.11.35.19
NS ns2.alibabadns.com 140.205.67.254
NS ns2.alibabadns.com 140.205.322.77
MX mx2.mail.aliyun.com 140.205.94.14
[*] A aliexpress.com 67.254.177.10
[*] TXT aliexpress.com google-site-verification=qEklI0sHgVZshePC5G6c0dQOTHPhxwacj-wzUxxHUWv
[*] TXT aliexpress.com mailru-verification:c9Feb214b0705f91
[*] TXT aliexpress.com spf1.alibabahq.com include:spf1.service.alibaba.com include:spf2.ocm.aliyun.com -all
[*] TXT aliexpress.com SpringsoftLndswrvTwcr4zghk2sy6dt5
[*] TXT aliexpress.com v=DMARCI; p=quarantine; rua=mailto:dmarc-ap@service.alibaba.com; ruf=mailto:dmarc-ap@service.alibaba.com
[*] Enumerating SRV Records
[+] 0 Records Found
jmax@Kali:~$
```

# 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

The screenshot shows four separate Shodan search results for AliExpress.com, each displaying a 302 Found error and an SSL Certificate analysis. The results are as follows:

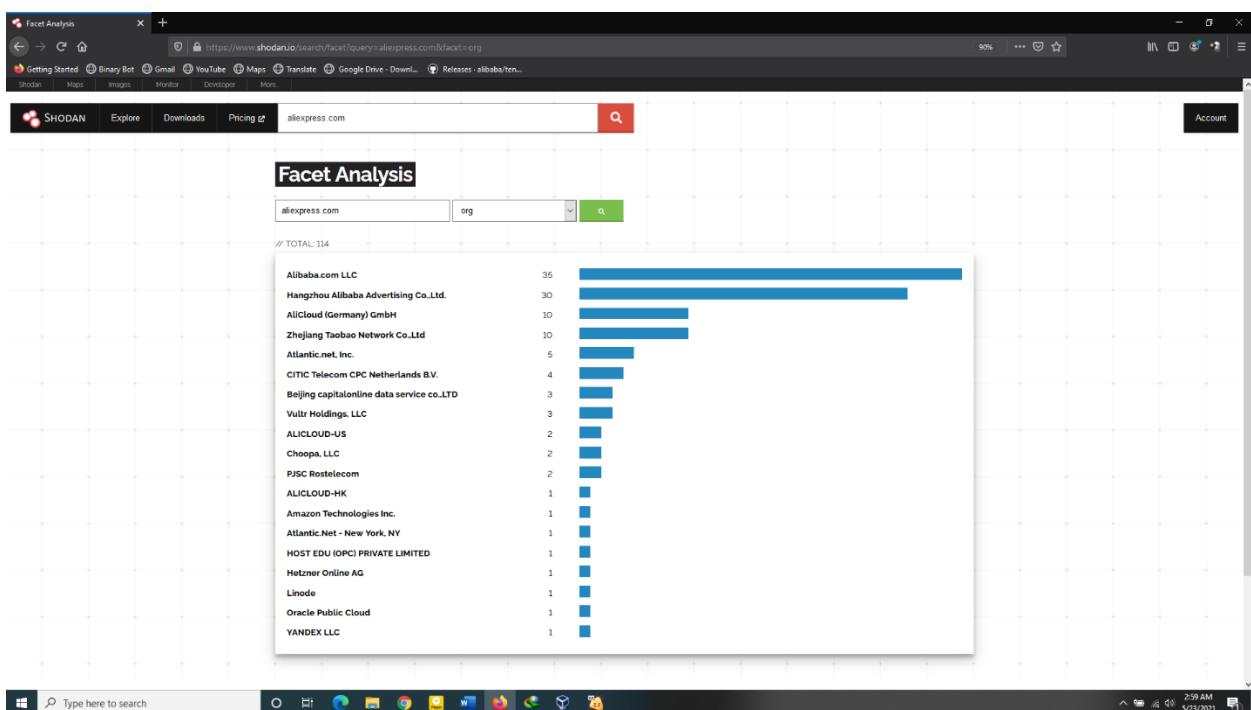
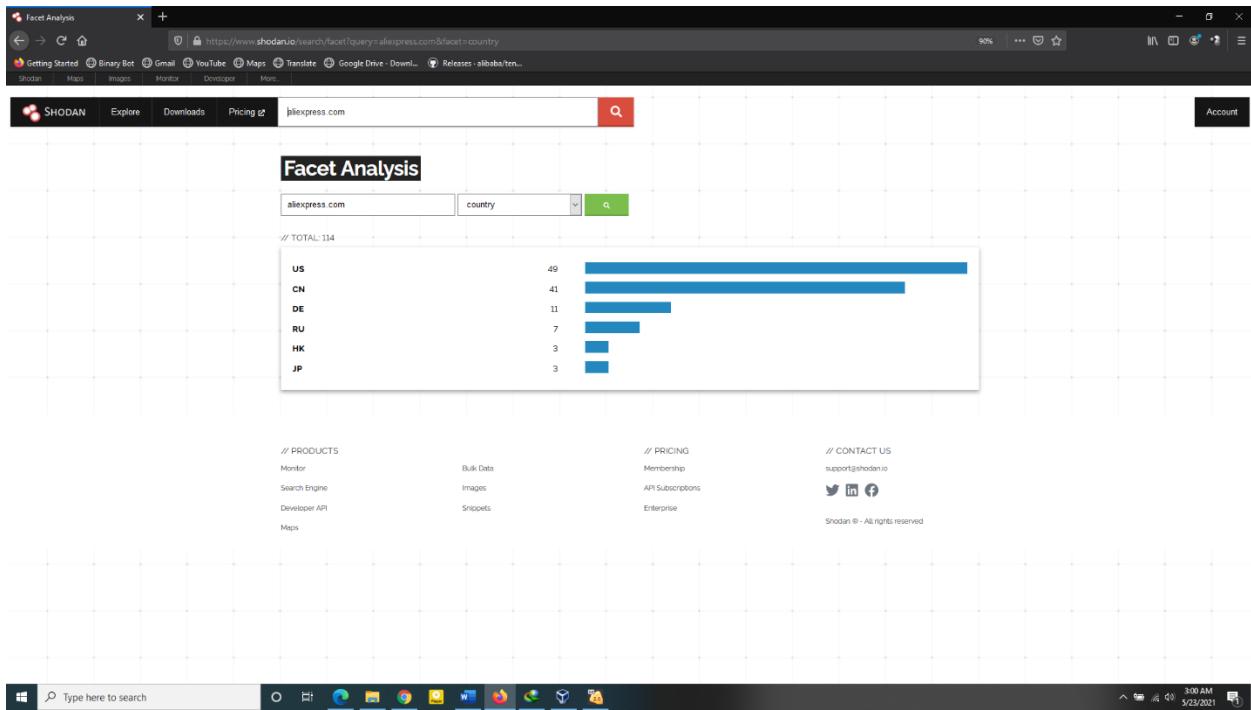
- Result 1 (Top):** IP 45.32.77.107, Hostname: aliexpress.com, Location: United States, Foster City. SSL Certificate details:
  - Issued By: GlobalSign Organization
  - Common Name: aliexpress.com
  - Validation CA: SHA256 - G2
  - Organization: GlobalSign nv-sa
  - Subject Alternative Name: \*aliexpress.com
  - Organization: Alibaba (China) Technology Co., Ltd.
  - Issued To: Let's Encrypt
  - Common Name: share-a-project.vip
  - Supported SSL Versions: TLSv1.2, TLSv1.3, TLSv1.1, TLSv1.0
- Result 2 (Second from Top):** IP 47.254.143.76, Hostname: ALICloud(Germany) GmbH, Location: Germany, Frankfurt am Main. SSL Certificate details:
  - Issued By: GlobalSign Organization
  - Common Name: ALICloud(Germany) GmbH
  - Validation CA: SHA256 - G2
  - Organization: GlobalSign nv-sa
  - Subject Alternative Name: \*aliexpress.com
  - Organization: Alibaba (China) Technology Co., Ltd.
  - Issued To: Let's Encrypt
  - Common Name: share-a-project.vip
  - Supported SSL Versions: TLSv1.2, TLSv1.3, TLSv1.1, TLSv1.0
- Result 3 (Third from Top):** IP 62.128.98.11, Hostname: CMC Telecom CPC Netherlands B.V., Location: Russian Federation, Moscow. SSL Certificate details:
  - Issued By: GlobalSign Organization
  - Common Name: aliexpress.com
  - Validation CA: SHA256 - G2
  - Organization: GlobalSign nv-sa
  - Subject Alternative Name: \*aliexpress.com
  - Organization: Alibaba (China) Technology Co., Ltd.
  - Issued To: Let's Encrypt
  - Common Name: share-a-project.vip
  - Supported SSL Versions: TLSv1.2, TLSv1.3, TLSv1.1, TLSv1.0
- Result 4 (Bottom):** IP 141.205.175.1, Hostname: Zhejiang Taobao Network Co., Ltd., Location: Hong Kong, Hong Kong. SSL Certificate details:
  - Issued By: GlobalSign Organization
  - Common Name: aliexpress.com
  - Validation CA: SHA256 - G2
  - Organization: GlobalSign nv-sa
  - Subject Alternative Name: \*aliexpress.com
  - Organization: Alibaba (China) Technology Co., Ltd.
  - Issued To: Let's Encrypt
  - Common Name: share-a-project.vip
  - Supported SSL Versions: TLSv1.2, TLSv1.3, TLSv1.1, TLSv1.0

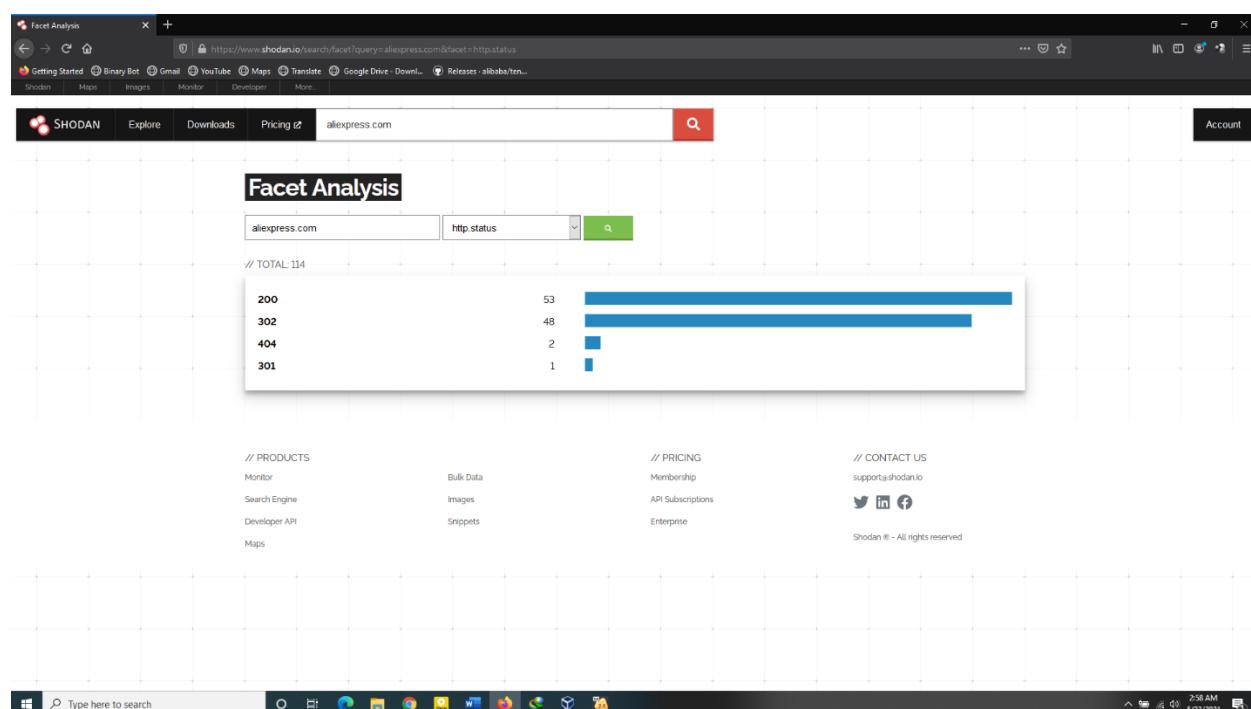
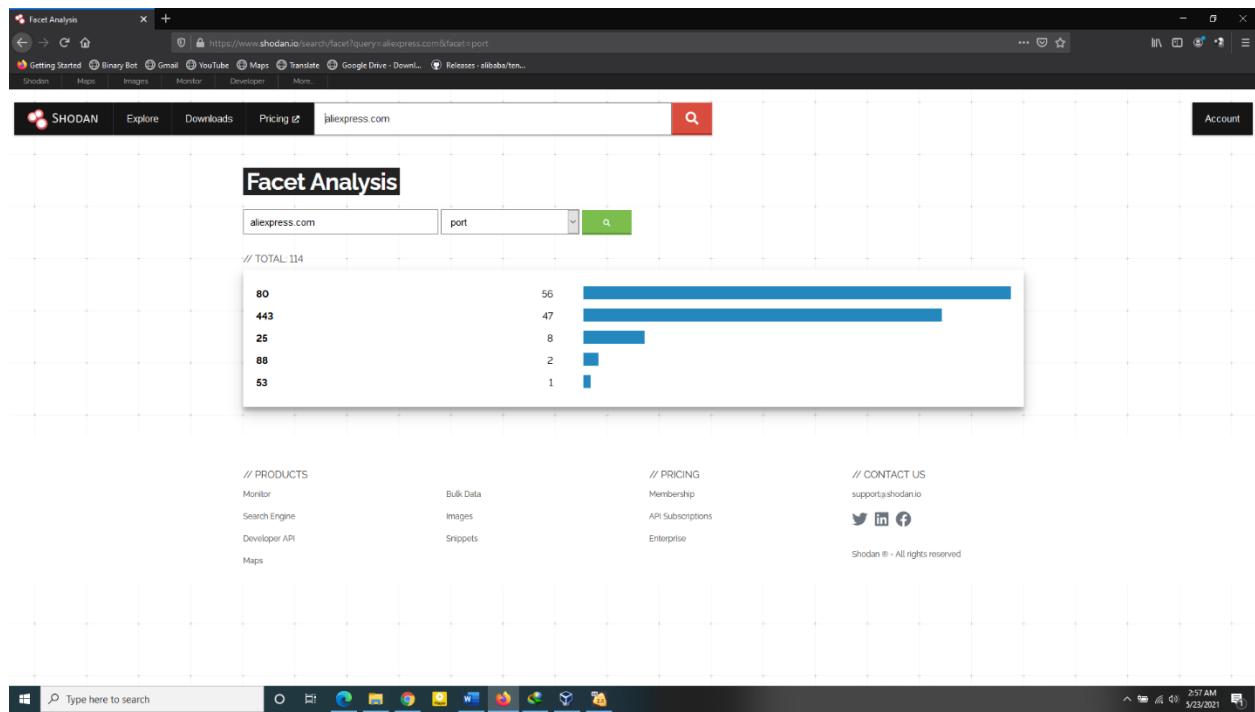
The screenshot shows a Shodan search result for 'aliexpress.com'. The results page includes detailed network information such as headers, SSL certificates, and supported SSL versions. Below this, a screenshot of the AliExpress homepage is shown, featuring products, pricing, and contact information.

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

The screenshot shows Shodan details for the IP address 45.32.77.107. It provides general information about the host, including its location (Los Angeles, United States) and the organization (Vultr Holdings, LLC). The 'Open Ports' section shows three ports: 22, 80, and 443. A terminal window on the right shows a ping to the host and an nmap scan. The nmap output identifies the host as running OpenSSH 7.6p1 Ubuntu-4ubuntu0.3 on an Ubuntu 20.04 system.

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





## 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>

The screenshot shows the Censys search interface with the query "www.aliexpress.com" entered. The results page displays a list of hosts found, categorized by their IP addresses and port numbers. Each entry includes details such as the host name, location, and various service ports (HTTP, SSH, MySQL, etc.) that are open. The results are paginated, with the current page being 1 of 1.

Host	Location	Ports
43.225.45.51	Hong Kong	21/FTP, 80/HTTP, 110/POP3, 143/IMAP, 993/IMAP, 22/SSH, 3306/MySQL
39.104.71.171	China	80/HTTP, 3690/UNKNOWN, 8180/HTTP, 8181/HTTP, 8888/HTTP, 11211/MEMCACHED
18.221.237.35 (ec2-18-221-237-35.us-east-2.compute.amazonaws.com)	Ohio, United States	22/SSH, 80/HTTP, 88/HTTP, 443/HTTP
13.251.186.6 (ec2-13-251-6.ap-southeast-1.compute.amazonaws.com)	Singapore	22/SSH, 80/HTTP, 443/HTTP
101.251.243.132	China	22/SSH, 88/HTTP, 3306/MySQL, 3690/UNKNOWN
202.182.114.138 (202.182.114.138.vultr.com)		
202.182.114.138 (202.182.114.138.vultr.com)	Tokyo, Japan	21/FTP, 80/HTTP, 443/HTTP, 993/HTTP, 994/HTTP
78.141.208.237 (78.141.208.237.vultr.com)	United States	22/SSH, 110/POP3, 143/IMAP, 993/POP3, 5252/SMTP, 3306/MySQL
101.251.243.130	China	80/HTTP, 88/HTTP, 443/HTTP, 444/UNKNOWN
178.154.226.201	Russia	22/SSH, 80/HTTP, 123/NTP, 443/HTTP
120.79.107.140	Guangdong, China	80/HTTP, 88/HTTP, 443/HTTP
211.149.245.223	China	21/FTP, 80/HTTP, 443/HTTP, 888/HTTP, 3000/HTTP, 3306/MySQL, 8080/HTTP, 8088/HTTP, 8222/HTTP, 8888/HTTP
45.32.77.107 (45.32.77.107.vultr.com)		

www.aliexpress.com - Host Search | Censys

https://search.censys.io/search?resource=hosts&q=www.aliexpress.com

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

**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
- services.tls.response.body: " /> <meta property="og:url" content="//www.aliexpress.com" /> <meta property="og:image" content="https://www.aliexpress.com/item/1005602582376337.htm" />

**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
- services.tls.response.body: "bxSlider" > <li><a href="https://www.aliexpress.com/item/1005602582376337.htm" />

**163.172.42.87 (163-172-42-87.rev.poneytelecom.eu)**

- Online SAS (12876) France
- 22/SSH 53/DNS 80/HTTP 123/NTP 2222/HTTP
- services.tls.response.body: " name =\"url\" value =\"https://www.aliexpress.com/item/4000243584724.html\" />

**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
- services.tls.certificates.leaf.\_data.subject.organization: www.aliexpress.com
- services.tls.certificates.leaf.\_data.subject.common\_name: www.aliexpress.com
- services.tls.certificates.leaf.\_data.issuer.common\_name.raw: www.aliexpress.com
- services.tls.certificates.leaf.\_data.names.raw: www.aliexpress.com
- services.tls.certificates.leaf.\_data.subject.common\_name.raw: www.aliexpress.com
- services.tls.certificates.leaf.\_data.issuer.common\_name: www.aliexpress.com
- services.tls.certificates.leaf.\_data.subject.common\_name.raw: www.aliexpress.com
- services.tls.certificates.leaf.\_data.names: www.aliexpress.com
- services.tls.certificates.leaf.\_data.subject.organization.raw: www.aliexpress.com
- services.tls.certificates.leaf.\_data.issuer.dn.C=SG, ST=Singapore, O=www.aliexpress.com, CN=www.aliexpress.com, i
- services.tls.certificates.leaf.\_data.issuer.organization.raw: www.aliexpress.com
- services.tls.certificates.leaf.\_data.issuer.organization: www.aliexpress.com
- services.tls.certificates.leaf.\_data.subject.dn.C=SG, ST=Singapore, O=www.aliexpress.com, CN=www.aliexpress.com,
- services.banner: HTTP/1.1 301 Moved Permanently Location: https://www.aliexpress.com/ Server: nginx/1.1

**www.aliexpress.com - Host Search | Censys**

https://search.censys.io/search?resource=hosts&q=www.aliexpress.com

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

**Register** Sign in

**80/HTTP 443/HTTP**

services.tls.certificates.leaf.\_data.subject.dn:C=CN, ST=<浙江省, L=<杭州市, O=Alibaba Cloud Computing Ltd., CN=www.i

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.subject.common\_name: www.aliexpress.com

services.tls.certificates.leaf.\_data.names.raw: www.aliexpress.com

services.tls.certificates.leaf.\_data.subject.common\_name.raw: www.aliexpress.com

services.tls.certificates.leaf.\_data.names: www.aliexpress.com

services.tls.certificates.leaf.\_data.subject.common\_name: www.aliexpress.com

services.tls.certificates.leaf.\_data.names.raw: www.aliexpress.com

**104.85.69.225 (a104-85-69-225.deploy.static.akamaitechnologies.com)**

- AKAMAI-AS (16625) Central and Western District, Hong Kong
- 80/HTTP 443/HTTP
- services.tls.certificates.leaf.\_data.subject.dn:C=CN, ST=<浙江省, L=<杭州市, O=Alibaba Cloud Computing Ltd., CN=www.i
- 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.common\_name: www.aliexpress.com
- 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.common\_name: www.aliexpress.com
- services.tls.certificates.leaf.\_data.names.raw: www.aliexpress.com

**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.i
- 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

**205.204.101.33**

The screenshot shows two side-by-side browser windows displaying Censys search results for the host 'www.aliexpress.com'. Both windows have identical URLs: https://search.censys.io/search?resource=hosts&q=www.aliexpress.com. The top window shows results for port 80, while the bottom window shows results for port 443. The results list various IP addresses and their associated services, including ports 80, 443, 22, 3306, and 888. Services listed include Apache, MySQL, and Nginx. The results are paginated, with 'PREVIOUS' and 'NEXT' buttons visible at the bottom of each window.

www.aliexpress.com - Host Search

Welcome to Search 2.0 Beta! See our launch announcement. Looking for Search 1.0? Find it here.

Censys

Hosts: www.aliexpress.com

services.banner:HTTP/1.1 301 Moved Permanently Location: https://www.aliexpress.com/ Server: nginx/1.1

193.8.83.159

HKFGL-AS-AP HK Kwalfong 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/105001639312364.html" )else{ window.location.href="https://www.aliexpress.com/item/105001639312364.html" }

120.24.93.248

CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd. (37965) China

80/HTTP 8888/HTTP 40000/HTTP

services.http.response.body.width="5%"> <a target=\_blank href="https://www.aliexpress.com/item/105001639312364.html" style="color: #0000ff; font-size: 14px;">View Details

45.63.56.64 (45.63.56.64.vultr.com)

AS-CHOOPOS (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/ Server: Tengine/As

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/As

62.66.177.121 (3w.dk)

TELENO-DANMARK\_AS (9158) Capital Region, Denmark

80/HTTP 443/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

services.tls.certificates.leaf\_data.subject\_dn=CnCN, ST=浙江省, L=杭州市, O=Alibaba Cloud Computing Ltd., CN=www.aliexpress.com

104.92.51.86 (a104-92-51-86.deploy.static.akamaitechnologies.com)

TDCN 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=CnCN, ST=浙江省, L=杭州市, O=Alibaba Cloud Computing Ltd., CN=www.aliexpress.com

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=CnCN, ST=浙江省, L=杭州市, O=Alibaba Cloud Computing Ltd., CN=www.aliexpress.com

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/As

© 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 Search 2.0

Hosts: 43.225.45.51

Register Sign In

110/POP3 TCP

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	fd5541106c3d5231afbc1f26a265917a945bc3b5effdde1c978f2ffa4e9e79
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	OS_APPLICATION_LAYER
services.extended_service_name	POP3S
services.transport_fingerprint.raw	14000,255,false,MNWNNNS,1460/false/false
services.pop3.banner	+OK Dovecot DA ready.
services.pop3.starttls	+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	fd5541106c3d5231afbc1f26a265917a945bc3b5effdde1c978f2ffa4e9e79
services.tls.certificates_leaf_data.subject_dn	C=GB, ST=Someprovince, L=Somewhere, O=none, OU=none, CN=localhost,

43.225.45.51 - Censys 43.225.45.51/ +

Getting Started Binary Bot Gmail YouTube Maps Translate Google Drive - Download Releases alibaba/ten...

Dear friends, I look forward to our cooperation.  
My name is Butch. Please contact me via whatversapp 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:

# Find Structure of File System

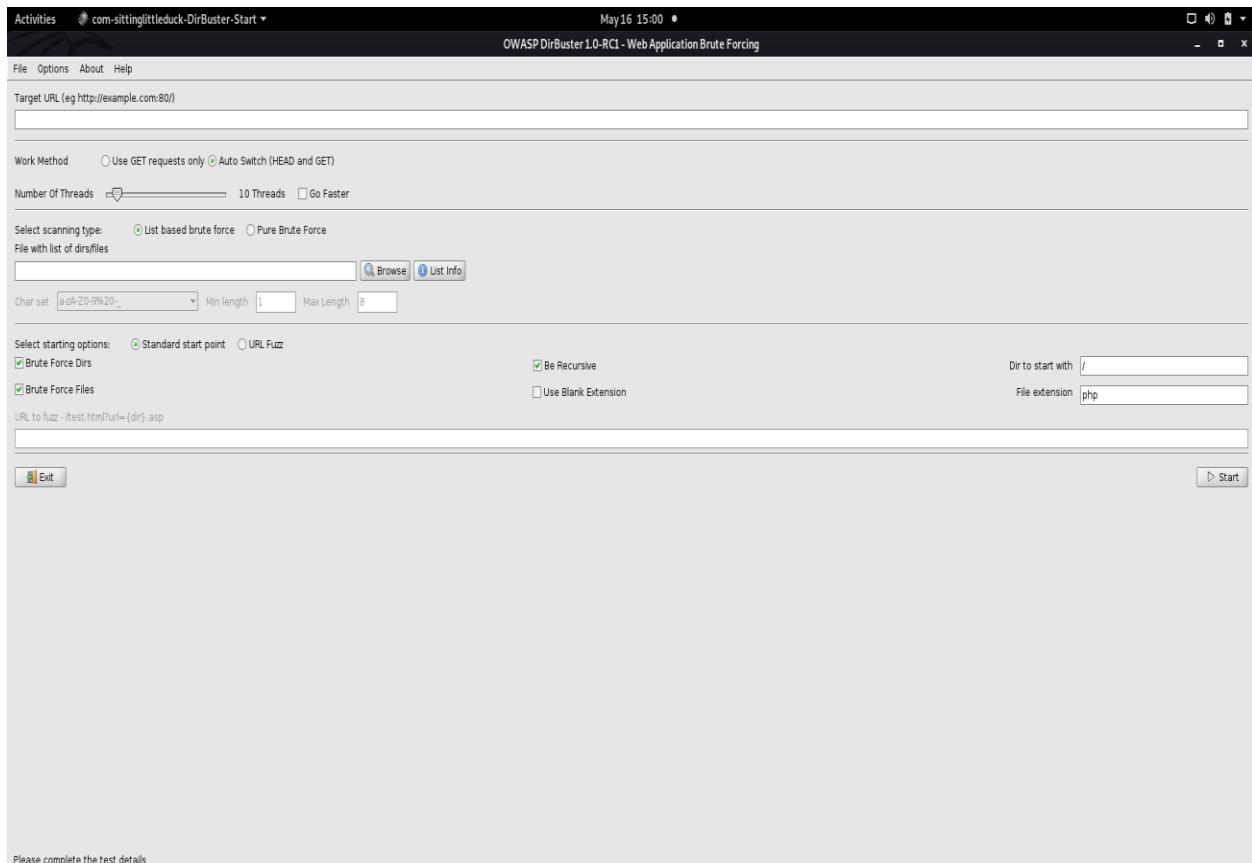
## 1. OWASP DirBuster

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.

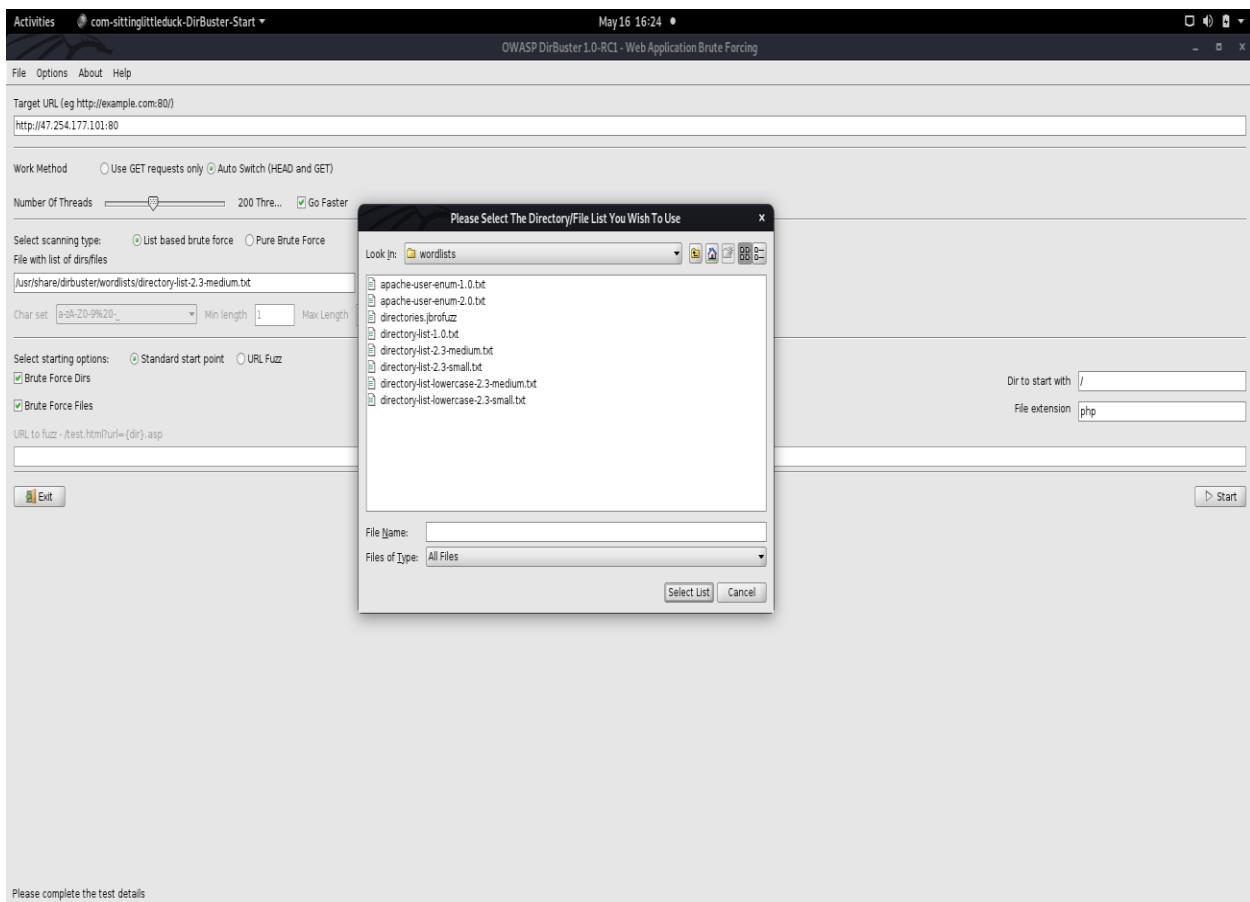
I tried few times using above test results. Following screenshots are express the DirBuster Test Results. This test takes about 10-20 minutes to complete. That time varies depending on the number of filters.

The following is the typical interface of DirBuster Tool.



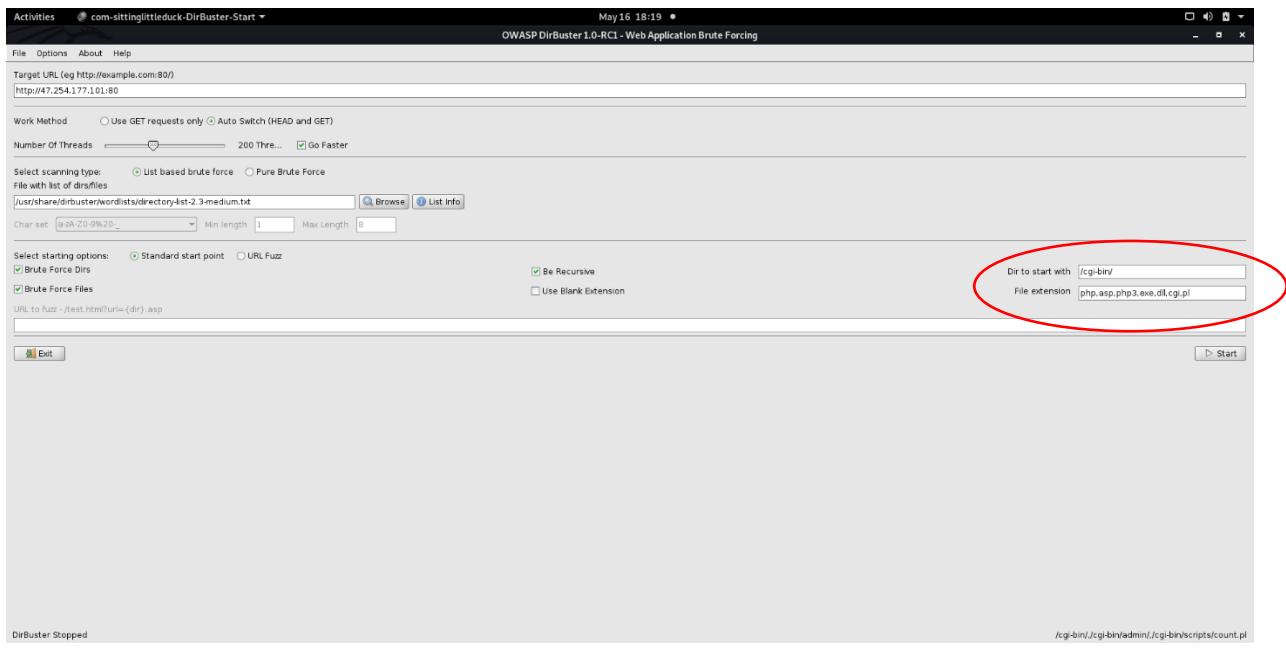
According to the screenshot above, first the URL should be entered along with the required domain and the port number according to the sample given there. Then select the scan type. List based brute force should be selected and it was not successful in selecting Pure Brute Force. When selecting a thread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

```
Activities Terminal May 3 12:45 jmax@kali: ~
jmax@kali: ~/Crips
jmax@kali: ~
OSVDB-17111: /cgi-bin/auth_data/auth_user_file.txt: The DCShop installation allows credit card numbers to be viewed remotely. See dcscripts.com for fix information.
/cgi-bin/mt-static/mt-check.cgi: Movah! Type weblog diagnostic script found. Reveals docroot path, operating system, Perl version, and modules.
/cgi-bin/mt/mt-check.cgi: Movah! Type weblog diagnostic script found. Reveals docroot path, operating system, Perl version, and modules.
/cgi-bin/banner.cgi: This CGI may allow attackers to read any file on the system.
/cgi-bin/bannereditor.cgi: This CGI may allow attackers to read any file on the system.
/cgi-bin/architext_query.cgi: Versions older than 1.1 of Excite for Web Servers allow attackers to execute arbitrary commands.
/cgi-bin/bizdb1-search.cgi: This CGI may allow attackers to execute commands remotely. See http://www.hack.co.za/daemon/cgi/cgi/bizdb.htm
/cgi-bin/blog/: A blog was found. May contain security problems in CGIs, weak passwords, and more.
/cgi-bin/blog/mt-load.cgi: Movah! Type weblog installation CGI found. May be able to reconfigure or reload.
OSVDB-2878: /cgi-bin/moin.cgi?test: MoinMoin 1.1 and prior contain at least two XSS vulnerabilities. Version 1.0 and prior also contains a XSLT related vulnerability
/cgi-bin/astrocam.cgi: Astrocam 1.4.1 contained buffer overflow http://www.securityfocus.com/bid/6884. Prior to 2.1.3 contained unspecified security bugs
/cgi-bin/badmin.cgi: BannerWheel v1.0 is vulnerable to a local buffer overflow. If this is version 1.0 it should be upgraded.
OSVDB-2017: /cgi-bin/bootz/admin/index.cgi?section=$&input1: Bootz CGI may have a buffer overflow. Upgrade to a version newer than 0.9.8alpha.
/cgi-bin/exadmin.cgi: Some versions of this CGI are vulnerable to a buffer overflow.
/cgi-bin/exboard.cgi: Some versions of this CGI are vulnerable to a buffer overflow.
/cgi-bin/exman.cgi: Some versions of this CGI are vulnerable to a buffer overflow.
OSVDB-1746: /cgi-bin/Foxweb.dll: FoxWeb 2.5 and below is vulnerable to a buffer overflow (not tested or confirmed). Verify Foxweb is the latest available version.
OSVDB-1747: /cgi-bin/Foxweb.exe: FoxWeb 2.5 and below is vulnerable to a buffer overflow (not tested or confirmed). Verify Foxweb is the latest available version.
/cgi-bin/mgrw.cgi: This CGI may be vulnerable to Magic Filesize bug. Version 8.0.5 and earlier is vulnerable to multiple buffer overflows. Upgrade to 9.x.
/cgi-bin/wcomctrl.dll: It may be possible to overflow this file with 1024 bytes of data.
/cgi-bin/upload.exe: This CGI allows attackers to upload files to the server and then execute them.
/cgi-bin/fpsvadm.exe: Potentially vulnerable CGI program.
/cgi-bin/coahalt: May allow remote admin of CGI scripts.
OSVDB-35707: /forum/admin/weforum.mdb: Web Wiz Forums password database found.
/fpb/shop.mdb: Metacart2 is an ASP shopping cart. The database of customers is available via the web.
OSVDB-52975: /guestbook/admin/012guest.mdb: Ocean2 ASP Guestbook Manager allows download of SQL database which contains admin password.
OSVDB-15971: /midicart.mdb: MIDICART database is available for browsing. This should not be allowed via the web server.
OSVDB-15971: /MIDICART/midicart.mdb: MIDICART database is available for browsing. This should not be allowed via the web server.
OSVDB-41850: /mpcsoftweb_guestbook/database/mpcsoftweb_guestdata.mdb: MPCSoftWeb Guest Book passwords retrieved.
/news/admin.mdb: Web Wiz Site News release v1.06 admin password database is available and unencrypted.
OSVDB-53412: /shopping80.mdb: VP-ASP shopping cart application allows .mdb files (which may include customer data) to be downloaded via the web. These should not be available.
OSVDB-53412: /shopping80.mdb: VP-ASP shopping cart application allows .mdb files (which may include customer data) to be downloaded via the web. These should not be available.
OSVDB-15971: /shoppingdirectory/midicart.mdb: MIDICART database is available for browsing. This should not be allowed via the web server.
OSVDB-4398: /database/H2B2000.mdb: Max Web Portal database is available remotely. It should be moved from the default location to a directory outside the web root.
OSVDB-319: /cgi-bin/vsplit.pl: Sambar may allow anonymous email to be sent from any host via this CGI.
/cgi-bin/.access: Contains authorization information
OSVDB-11871: /cgi-bin/MsMskMask.exe: MsMskSearch 4.4 may allow source code viewing by requesting MsMskMask.exe?mask=/filename.asp where 'filename.asp' is a real ASP file.
/forum/admin/weforum.mdb: Web Wiz Forums pre 7.5 is vulnerable to Cross-Site Scripting attacks. Default login/pass is Administrator/letmein
/cgi-bin/wcomctrl.dll: This CGI may allow attackers to retrieve document source.
/cgi-bin/aglimpse.cgi: This CGI may allow attackers to execute remote commands.
/cgi-bin/aglimpse: This CGI may allow attackers to execute remote commands.
/cgi-bin/architext_query.cgi: Versions older than 1.1 of Excite for Web Servers allow attackers to execute arbitrary commands.
/cgi-bin/cmdi.exe/cdir: cmdi.exe can execute arbitrary commands
/cgi-bin/cmdi.exe/cdir: cmdi.exe can execute arbitrary commands
/nsn/.%SUtil/typ.bas: NetUtil basic access is possible which means that several utility scripts might be run (including directory listings, NDS tree enumeration and running .bas files on server
/cgi-bin/archie: Gateway to the unix command, may be able to submit extra commands
/cgi-bin/calendar.pl: Gateway to the unix command, may be able to submit extra commands
/cgi-bin/calendar: Gateway to the unix command, may be able to submit extra commands
/cgi-bin/date: Gateway to the unix command, may be able to submit extra commands
/cgi-bin/fortune: Gateway to the unix command, may be able to submit extra commands
/cgi-bin/redirect: Redirects via URL from form
```

```
Activities Terminal May 3 12:47 jmax@kali: ~
jmax@kali: ~
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-338: /cgi-bin/imagemap: imagemap was found. Many versions from different vendors contain flaws.
OSVDB-3380: /cgi-bin/imagemap: imagemap.exe was found. Many versions from different vendors contain flaws.
OSVDB-3568: /cgi-bin/hmimage.exe: hmimage.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.microsoft.com/bulletin/MS00-028
OSVDB-3514: /vti_bin/vote.cgi: Mike's Vote CGI contained a bug which allowed arbitrary command execution (version 1.2), see http://freshmeat.net/projects/mikesurveycgi/
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/mikespic/
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/3286.
OSVDB-4171: /ASP/cart/database/metcart.mdb: Metacart2 is an ASP shopping cart. The database of customers is available via the web.
OSVDB-4171: /database/metcart.mdb: Metacart2 is an ASP shopping cart. The database of customers is available via the web.
OSVDB-4171: /mcartcart/database/metcart.mdb: Metacart2 is an ASP shopping cart. The database of customers is available via the web.
OSVDB-4171: /shop/shop/metcart.mdb: Metacart2 is an ASP shopping cart. The database of customers is available via the web.
OSVDB-4171: /shoponline/fpdh/shop.mdb: Metacart2 is an ASP shopping cart. The database of customers is available via the web.
OSVDB-4171: /shopping/database/metcart.mdb: Metacart2 is an ASP shopping cart. The database of customers is available via the web.
OSVDB-4192: /cgi-bin/gettransitmap: Su Answerbook2 is vulnerable to a buffer overflow in the gettransitmap 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/VSetCookie.exe: A flaw in VSetCookie.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.nextgens.com/advisories/webnews.txt for more info.
OSVDB-4301: /cgi-bin/webnews.pl: Webnews may contain some default users in the binary: testweb/testnews, alw13845/imaptest, alw13845/wtest4297, testweb2/wtest4809
OSVDB-4301: /cgi-bin/sensepost.exe/cdir: The presence of sensepost.exe indicates the system was vulnerable to a Unicode flaw and was compromised with a test script from SensePost. The sensepost.exe allows command execution if it is run in cdir mode (see http://www.cert.org/advisories/CA-2000-02.html).
OSVDB-4360: /acm2/2/acm2_0.mbs: Microsoft Word 2000 2.0 allows remote user to read customer database file which may contain usernames, passwords, credit cards and more.
OSVDB-3689: /vti_namazu.cgi: Numazu search engine found. Vulnerable to XSS attacks (fixed 2001-11-25). Attacker could write arbitrary files outside docroot (fixed 2000-01-20). http://www.cert.org/advisories/CA-2000-02.html
OSVDB-3709: /cgi-bin/nscconfig: Contains authorization information
OSVDB-6666: /cgi-bin/hpnst.exe?sp=1&sr=SystemInfo.html: HP Instant TopTools GoAhead WebServer hpnst.exe may be vulnerable to a DoS.
OSVDB-6695: /cgi-bin/rwrcg160: 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/rwrcg160/shownew: 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/myclassified/
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.../windows/repair/sam: BadBlue server is vulnerable to multiple remote exploits. See http://www.securitem.com/exploits/SHPOM2A600.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.securitem.com/exploits/SHPOM2A600.html for more information.
OSVDB-721: /...%255c.%2525c.%2525c.%2525c...%2525c.../windows/repair/sam: BadBlue server is vulnerable to multiple remote exploits. See http://www.securitem.com/exploits/SHPOM2A600.html for more information.
OSVDB-721: /...%255c.%2525c.%2525c.%2525c...%2525c.../winnt/repair/sam: BadBlue server is vulnerable to multiple remote exploits. See http://www.securitem.com/exploits/SHPOM2A600.html for more information.
OSVDB-38580: /cgi-bin/c2web.exe/GetImageName?CustomerEmail=txtC2980.pdf: C2982 contains a null byte directory traversal in the ImageName variable.
STATUS: Completed 4750 requests (-69% complete, 9.4 minute left): currently in plugin 'Nikto Tests'
STATUS: Running average: 100 requests/s
STATUS: 2249 set, 10 requests: 0.250 sec.
```

Below are some screenshots of sample attempts at scanning ...

Activities com-sittinglittleduck-DirBuster-Start • May 16 20:43 • OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://47.254.177.101:80/cgi-bin/

Scan Information \ Results - List View: Dirs: 0 Files: 0 \ Results - Tree View \ Errors: 0 \

Testing for dirs in /cgi-bin/

Request	Error Message
Testing for files in /cgi-bin/ with extention .php	0%
Testing for files in /cgi-bin/ with extention .asp	0%
Testing for files in /cgi-bin/ with extention .php3	0%
Testing for files in /cgi-bin/ with extention .exe	0%
Testing for files in /cgi-bin/ with extention .dll	0%
Testing for files in /cgi-bin/ with extention .cgi	0%
Testing for files in /cgi-bin/ with extention .pl.mdb	0%

Current speed: 448 requests/sec  
Average speed: (T) 214, (C) 214 requests/sec  
Parse Queue Size: 0  
Total Requests: 1719/0764385  
Time To Finish: 02:17:16

Starting dirfile list based brute forcing

(Select and right click for more options)

Report /cgi-bin/9.php3

Activities com-sittinglittleduck-DirBuster-Start • May 8 10:05 • OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

https://47.254.177.101:443/alibaba/aliexpress/

Scan Information \ Results - List View: Dirs: 0 Files: 0 \ Results - Tree View \ Errors: 121 \

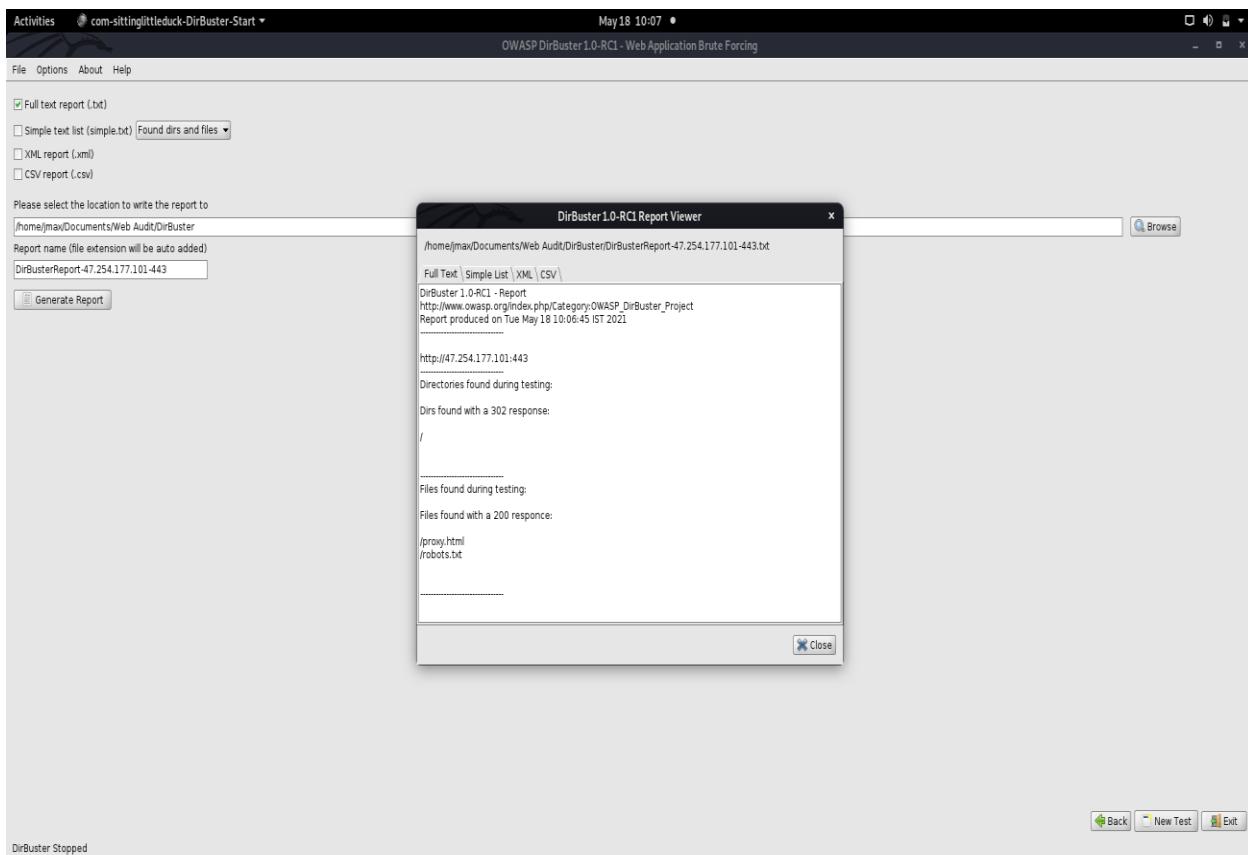
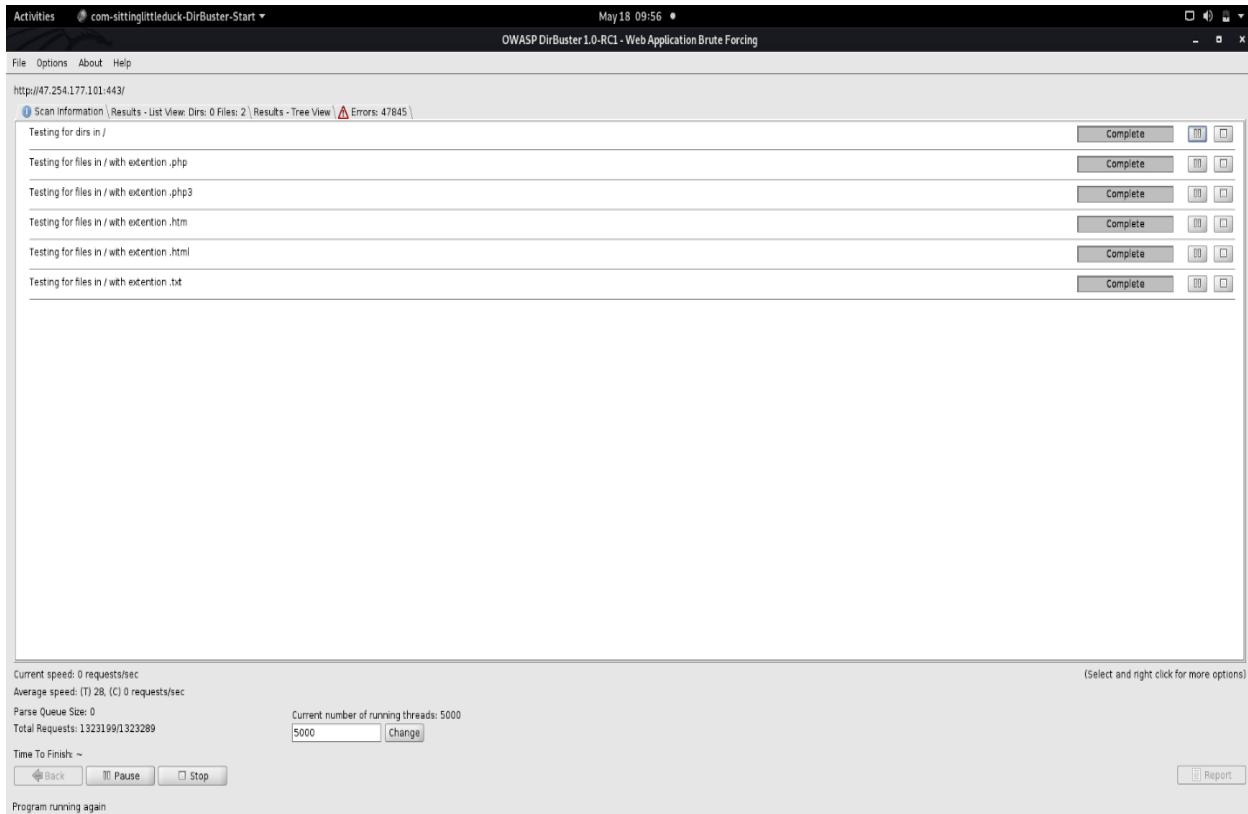
Request	Error Message
https://47.254.177.101:443/alibaba/aliexpress/9000/	IOException Connection reset
https://47.254.177.101:443/alibaba/aliexpress/7494/	IOException Connection reset
https://47.254.177.101:443/alibaba/aliexpress/9317/	IOException Connection reset
https://47.254.177.101:443/alibaba/aliexpress/search-marketing.php	IOException Connection reset
https://47.254.177.101:443/alibaba/aliexpress/our-services.php	IOException Connection reset
https://47.254.177.101:443/alibaba/aliexpress/rudolph.php	IOException Connection reset
https://47.254.177.101:443/alibaba/aliexpress/4359/	IOException Connection reset
https://47.254.177.101:443/alibaba/aliexpress/5258/	IOException Connection reset
https://47.254.177.101:443/alibaba/aliexpress/Pix.php	IOException Connection reset
https://47.254.177.101:443/alibaba/aliexpress/5426/	IOException Connection reset
https://47.254.177.101:443/alibaba/aliexpress/blackjack-1/	IOException connect timed out
https://47.254.177.101:443/alibaba/aliexpress/adfree.php	IOException Connection reset
https://47.254.177.101:443/alibaba/aliexpress/hdrs/	IOException Connection reset
https://47.254.177.101:443/alibaba/aliexpress/comptroller.php	IOException Connection reset

Current speed: 0 requests/sec  
Average speed: (T) 9, (C) 0 requests/sec  
Parse Queue Size: 0  
Total Requests: 441007/441097  
Time To Finish: ~

Program running again

(Select and right click for more options)

Report /cgi-bin/9.php3



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	/proxy.html	302	597
File	/robots.txt	200	305
File		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 Current number of running threads: 5000  
Total Requests: 1323199/1323289 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 |

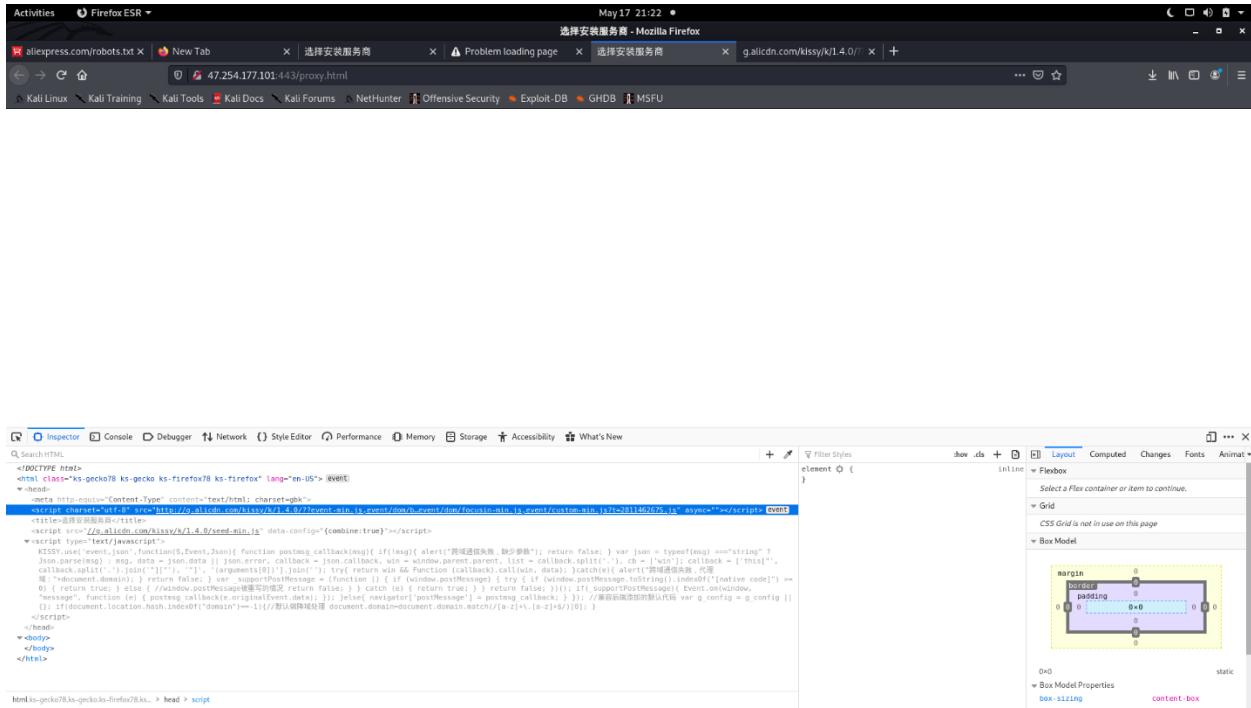
Directory Structure	Response Code	Response Size
/ proxy.html	302	597
/ robots.txt	200	305
	200	309

Current speed: 0 requests/sec (Select and right click for more options)  
Average speed: (T) 28, (C) 0 requests/sec  
Parse Queue Size: 0 Current number of running threads: 5000  
Total Requests: 1323199/1323289 5000 Change  
Time To Finish: ~

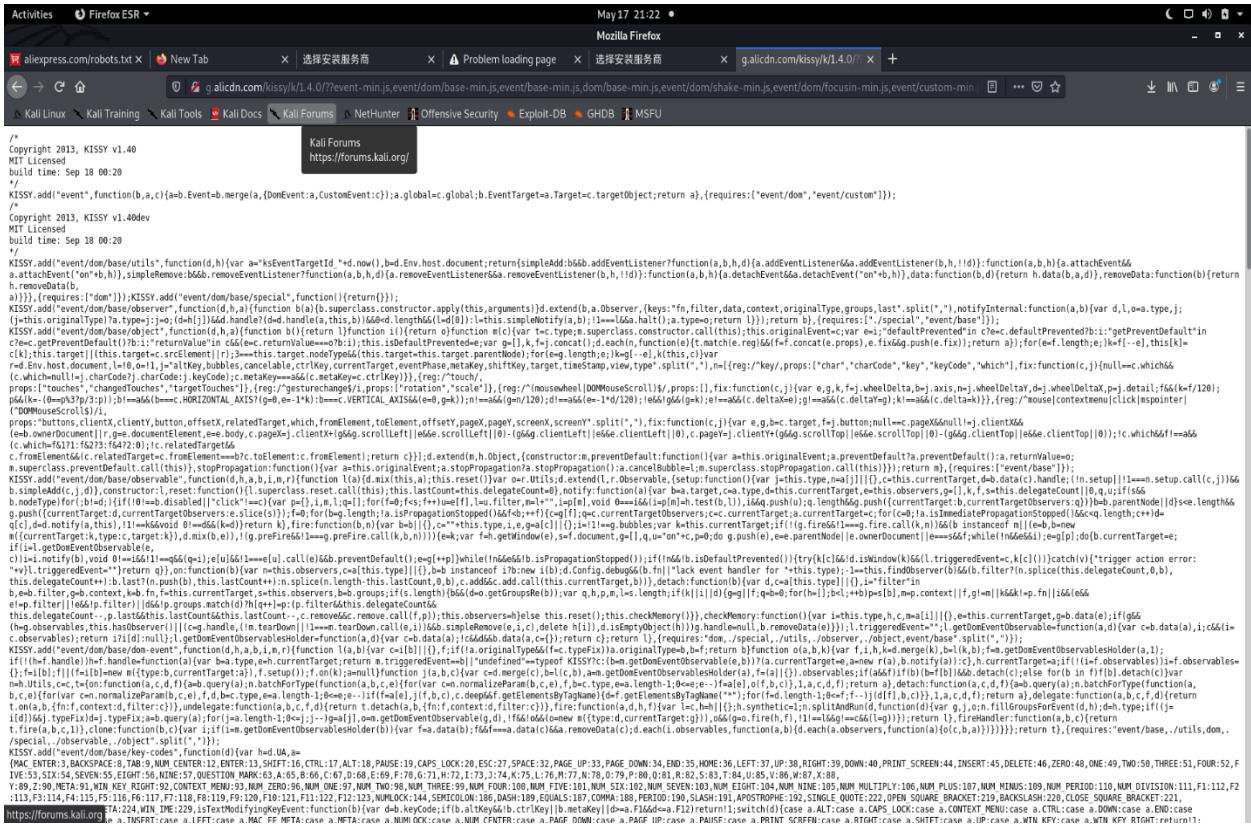
Back Pause Stop Report

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.







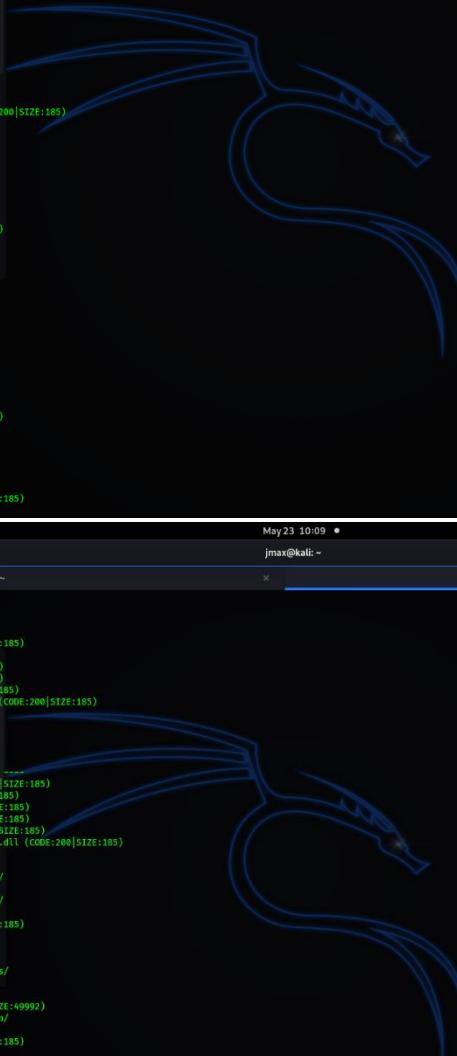
Then I opened the robots.txt file, which contains AliExpress's user-agents and several sub-directories that are unique to them.

```
User-agent: *
Disallow: /items/*
Disallow: /bin/*
Disallow: /search/*
Disallow: /wholesale/*
Disallow: /productdetail/*
Disallow: /api/*
Disallow: /api*.do
Disallow: /apps/*
Disallow: /downloads/*
Disallow: /category/*
Disallow: /shopcart/*
Disallow: /brands/*
Disallow: /cp/*
Disallow: /item-img/*
Disallow: /product/*
Disallow: /p4p*list.html
Disallow: /orderList.html
Disallow: /ws/api-server.html$*
Disallow: /mmend.html$*
Disallow: /mmend/*
Disallow: /ajax.htm$*
Disallow: /store/*ajax.htm$*
Disallow: /detail/*Ajax.do$*
Disallow: /ajax*.do$*
Disallow: /_ncf/*
Disallow: /_mobile/*
Disallow: /seo/*
Disallow: /cross-domain/*
Disallow: /store/group/*
Disallow: /store/all-wholesale-items/*
Disallow: /store/all-wholesale-products/*
Disallow: /store/top-rated-products/*
Disallow: /i/api/*

User-agent: YandexBot
Crawl-delay: 0.5
Disallow: /bin/*
Disallow: /category/*
Disallow: /wholesale/*
Disallow: /productdetail/*
Disallow: /api/*
Disallow: /api*.do
Disallow: /apps/*
Disallow: /downloads/*
Disallow: /wishlist/*
Disallow: /shopcart/*
Disallow: /brands/*
Disallow: /cp/*
Disallow: /item-img/*
Disallow: /product/*
Disallow: /p4p*list.html
Disallow: /orderList.html
Disallow: /ws/api-server.html$*
Disallow: /mmend.html$*
Disallow: /mmend/*
Disallow: /ajax.htm$*
Disallow: /store/*ajax.htm$*
Disallow: /detail/*Ajax.do$*
Disallow: /ajax*.do$*
Disallow: /_ncf/*
```

## 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.



```
Activities Terminal • May 23 10:08 • jmax@kali: ~
jmax@kali:~$ dirb https://www.aliexpress.com
DIRB v2.22
By The Dark Raver
https://www.aliexpress.com/2023/05/22-18-35-49.png
START TIME: Sun May 23 04:15:00 2021
URL BASE: https://www.aliexpress.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----
GENERATED WORDS: 4612
---- Scanning URL: https://www.aliexpress.com/ ----
+ http://www.aliexpress.com/.hashrc (CODE:200|SIZE:185)
+ http://www.aliexpress.com/.htaccess (CODE:200|SIZE:185)
+ http://www.aliexpress.com/.htpasswd (CODE:200|SIZE:185)
+ http://www.aliexpress.com/.vt1_bin/.vt1_admin.dll (CODE:200|SIZE:185)
=>> DIRECTORY: https://www.aliexpress.com/about/
+ http://www.aliexpress.com/.action (CODE:102|SIZE:258)
=>> DIRECTORY: https://www.aliexpress.com/activities/
=>> DIRECTORY: https://www.aliexpress.com/activity/
+ http://www.aliexpress.com/.category (CODE:200|SIZE:185)
+ http://www.aliexpress.com/.categoryaction (CODE:200|SIZE:185)
+ http://www.aliexpress.com/.cg-bin/ (CODE:200|SIZE:185)
=>> DIRECTORY: https://www.aliexpress.com/core/
=>> DIRECTORY: https://www.aliexpress.com/coupon/
+ http://www.aliexpress.com/.crossdomain.xml (CODE:200|SIZE:618)
=>> DIRECTORY: https://www.aliexpress.com/.express/
=>> DIRECTORY: https://www.aliexpress.com/electronics/
+ http://www.aliexpress.com/.fission.ice (CODE:200|SIZE:159)
=>> DIRECTORY: https://www.aliexpress.com/help/
=>> DIRECTORY: https://www.aliexpress.com/icons/
+ http://www.aliexpress.com/.index.html (CODE:200|SIZE:37386)
+ http://www.aliexpress.com/.indexdef.html (CODE:200|SIZE:258)
+ http://www.aliexpress.com/.index.jsp (CODE:201|SIZE:258)
+ http://www.aliexpress.com/.main.ndn (CODE:200|SIZE:185)
+ http://www.aliexpress.com/.obiz (CODE:402|SIZE:258)
=>> DIRECTORY: https://www.aliexpress.com/plugins/
+ http://www.aliexpress.com/.robots.txt (CODE:200|SIZE:2468)
+ http://www.aliexpress.com/.script (CODE:200|SIZE:185)
+ http://www.aliexpress.com/.search (CODE:301|SIZE:278)
+ http://www.aliexpress.com/.shops_buynation (CODE:402|SIZE:258)
=>> DIRECTORY: https://www.aliexpress.com/style/
+ http://www.aliexpress.com/.transaction (CODE:303|SIZE:256)
+ http://www.aliexpress.com/.wholesale (CODE:200|SIZE:39144)
=>> DIRECTORY: https://www.aliexpress.com/wireless/
---- Entering directory: https://www.aliexpress.com/about/ ----
+ http://www.aliexpress.com/about/.hash_history (CODE:200|SIZE:185)
+ http://www.aliexpress.com/about/.hashrc (CODE:200|SIZE:185)

Activities Terminal • May 23 10:09 • jmax@kali: ~
jmax@kali: ~
jmax@kali:~$ dirb https://www.aliexpress.com/wireless
DIRB v2.22
By The Dark Raver
https://www.aliexpress.com/2023/05/22-18-35-49.png
START TIME: Sun May 23 04:15:00 2021
URL BASE: https://www.aliexpress.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----
+ https://www.aliexpress.com/.wholesale (CODE:200|SIZE:9144)
=>> DIRECTORY: https://www.aliexpress.com/wireless/
---- Entering directory: https://www.aliexpress.com/about/ ----
+ http://www.aliexpress.com/.about/.base_history (CODE:200|SIZE:185)
+ https://www.aliexpress.com/.about/.hashrc (CODE:200|SIZE:185)
+ https://www.aliexpress.com/.about/.htaccess (CODE:200|SIZE:185)
+ https://www.aliexpress.com/.about/.htpasswd (CODE:200|SIZE:185)
+ http://www.aliexpress.com/.about/.index (CODE:200|SIZE:185)
+ https://www.aliexpress.com/.about/.vt1_bin/.vt1_admin.dll (CODE:200|SIZE:185)
+ https://www.aliexpress.com/.about/.cgi-bin/ (CODE:200|SIZE:185)
+ http://www.aliexpress.com/.about/.html (CODE:301|SIZE:278)
+ https://www.aliexpress.com/.about/.main.ndn (CODE:200|SIZE:185)
+ http://www.aliexpress.com/.about/.script (CODE:200|SIZE:185)
+ ...
---- Entering directory: https://www.aliexpress.com/activities/ ----
+ http://www.aliexpress.com/.activities/.hash_history (CODE:200|SIZE:185)
+ https://www.aliexpress.com/.activities/.hashrc (CODE:200|SIZE:185)
+ https://www.aliexpress.com/.activities/.htaccess (CODE:200|SIZE:185)
+ https://www.aliexpress.com/.activities/.htpasswd (CODE:200|SIZE:185)
+ http://www.aliexpress.com/.activities/.index (CODE:200|SIZE:49992)
+ https://www.aliexpress.com/.activities/.information/
+ https://www.aliexpress.com/.activities/.logistics/
+ https://www.aliexpress.com/.activities/.main.ndn (CODE:200|SIZE:185)
=>> DIRECTORY: https://www.aliexpress.com/.activities/.module/
+ https://www.aliexpress.com/.activities/.performance/
=>> DIRECTORY: https://www.aliexpress.com/.activities/.pp/
=>> DIRECTORY: https://www.aliexpress.com/.activities/.preview/
=>> DIRECTORY: https://www.aliexpress.com/.activities/.product/
=>> DIRECTORY: https://www.aliexpress.com/.activities/.promotion/
=>> DIRECTORY: https://www.aliexpress.com/.activities/.promotions/
=>> DIRECTORY: https://www.aliexpress.com/.activities/.purchase/
=>> DIRECTORY: https://www.aliexpress.com/.activities/.ru/
+ https://www.aliexpress.com/.activities/.script (CODE:200|SIZE:185)
+ https://www.aliexpress.com/.activities/.subject/
=>> DIRECTORY: https://www.aliexpress.com/.activities/.test/
=>> DIRECTORY: https://www.aliexpress.com/.activities/.text/
=>> DIRECTORY: https://www.aliexpress.com/.activities/.toys/
```

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

#### **Vulnerabilities**

1.1. [https://www.aliexpress.com/api/data\\_homepage.do?featuresWhitelist=1](https://www.aliexpress.com/api/data_homepage.do?featuresWhitelist=1)

**CONFIRMED**

Method	Parameter	Value
GET	featuresWhitelist	1

#### **Identified Cookie(s)**

- JSESSIONID

#### **Cookie Source**

- HTTP Header

## **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=917BE72D4BAD219A494AC9CFA292E7EA; 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=oSYJitXde7oguPgpCi1D7ecq5BPUuQ7bIuVCzGIX7gfb17Utun+pPQ==; intl_locale=en_US; xman_f=GjpqAmnoj6VaT/arm8AbM31YV7S11uFEv53hFSJR/sbmH/QgxZHU+6dRGrwhfafw2vYih2vhakvlF9eprBNd19F75w1T7Td0F4m1HTJ2gpSnL3Bhn4jp+w==; xman_t=D3HVjjZG5uKe253JVPv6goHmuTwT7VsAV10u3kKX2vPCexh+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: 0b0a556816221085713145513e4959
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%22cookieCacheEffectTime%22%3A1622108861517%2C%22isCookieCache%22%3A%22Y%22%2C%22ms%22%3A%220%22%7D&acs_rt=2c8c5a0aa91644e88951b7ca4fa13571; 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: 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: pJeLZyn5QivxAPPh0DfvVJJcqwzFQrdxlza7Ivl4cN5XObnU3wJDFHZXI4roXSGNGZ0tBpYw1VB/H18850BM9R25WsGeIk1+Ib1ctX8PPBk=
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=2c8c5a0aa91644e88951b7ca4fa13571; 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-age must be at least 31536000 seconds (1 year)
  - The includeSubDomains directive must be specified
  - The preload directive 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.

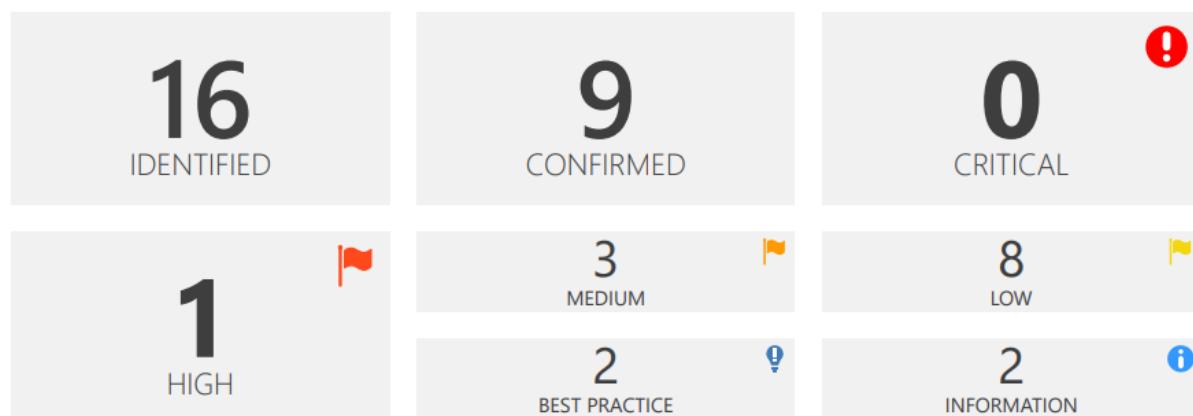
## Overview Summary:

 <a href="https://www.aliexpress.com/">https://www.aliexpress.com/</a>	Scan Time : 5/27/2021 3:12:38 PM (UTC+05:30)	Risk Level: <b>HIGH</b>
Scan Duration : 00:04:16:32	Total Requests : 95,854	
Average Speed : 6.2r/s		

## Explanation

This report is generated based on OWASP Top Ten 2017 classification.

There are 8 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.



### Identified Vulnerabilities



Critical	0
High	1
Medium	3
Low	8
Best Practice	2
Information	2
<b>TOTAL</b>	<b>16</b>

### Confirmed Vulnerabilities



Critical	0
High	1
Medium	1
Low	5
Best Practice	1
Information	1
<b>TOTAL</b>	<b>9</b>

<https://www.2014.aliexpress.com>

## Vulnerabilities By OWASP 2017

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

### 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/>

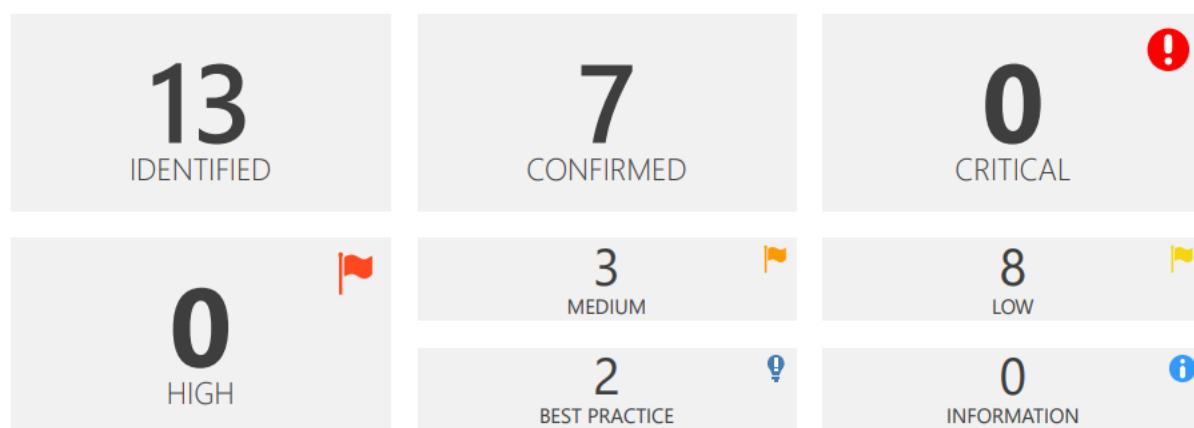
Scan Time : 5/26/2021 6:48:58 PM (UTC+05:30)  
Scan Duration : 00:00:40:36  
Total Requests : 41,885  
Average Speed : 17.2r/s

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.



### Identified Vulnerabilities



Critical	0
High	0
Medium	3
Low	8
Best Practice	2
Information	0
<b>TOTAL</b>	<b>13</b>

### Confirmed Vulnerabilities



Critical	0
High	0
Medium	1
Low	5
Best Practice	1
Information	0
<b>TOTAL</b>	<b>7</b>

<https://www.activities.aliexpress.com>

## Vulnerabilities By OWASP 2017

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

### 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.

### 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
```

#### Response

Response Time (ms) : 724.3485 Total Bytes Received : 547 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
EagleEye-TraceId: 0b0a555916221040180661980e55c6
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Date: Thu, 27 May 2021 08:26:58 GMT
Vary: Accept-Encoding
Cache-Control: no-store
```

```
<a id="a-link" href="https://www.taobao.com/markets/bx/deny_pc?uuid=6de6e707ba930a71a3fd7e075c9eec83&action=deny"></a> <script>document.getElementById("a-link").click();</script>
```

## 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/>

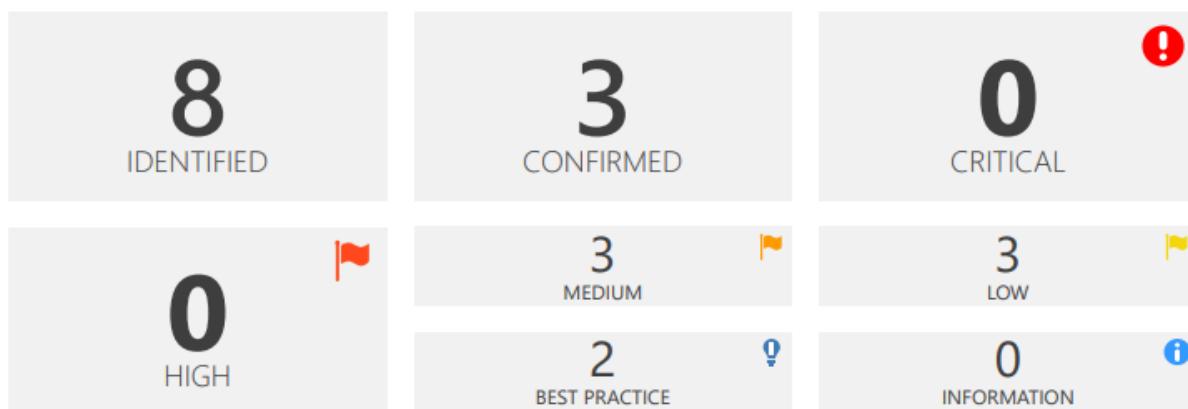
Scan Time : 5/27/2021 1:56:45 PM (UTC+05:30)  
Scan Duration : 00:00:02:47  
Total Requests : 701  
Average Speed : 4.2r/s

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
<b>TOTAL</b>	<b>8</b>

### Confirmed Vulnerabilities



Critical	0
High	0
Medium	1
Low	1
Best Practice	1
Information	0
<b>TOTAL</b>	<b>3</b>

## <https://www.ajax.aliexpress.com>

### A6 - SECURITY MISCONFIGURATION

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

### 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
```

## Response

Response Time (ms) : 280.2748 Total Bytes Received : 585 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=0
EagleEye-TraceId: 0ab6f82116221042692082757e5184
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Thu, 27 May 2021 08:31:09 GMT
Vary: Accept-Encoding
Cache-Control: no-store
```

```
<a id="a-link" href="https://www.taobao.com/markets/bx/deny_pc?uuid=5f7b147a355f04aa87bcf5924a88d007&action=deny"></a> <script>document.getElementById("a-link").click();</script>
```

## 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

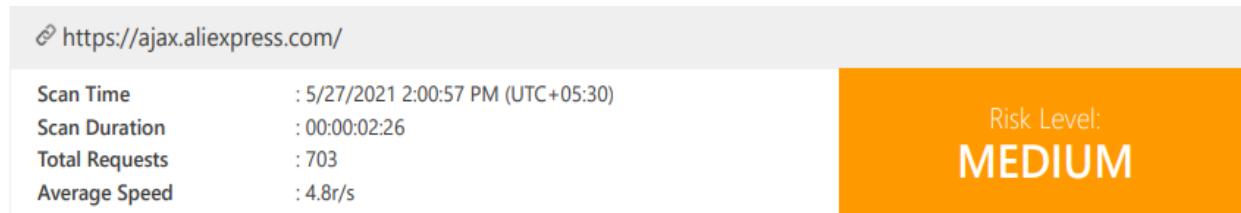
On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the

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

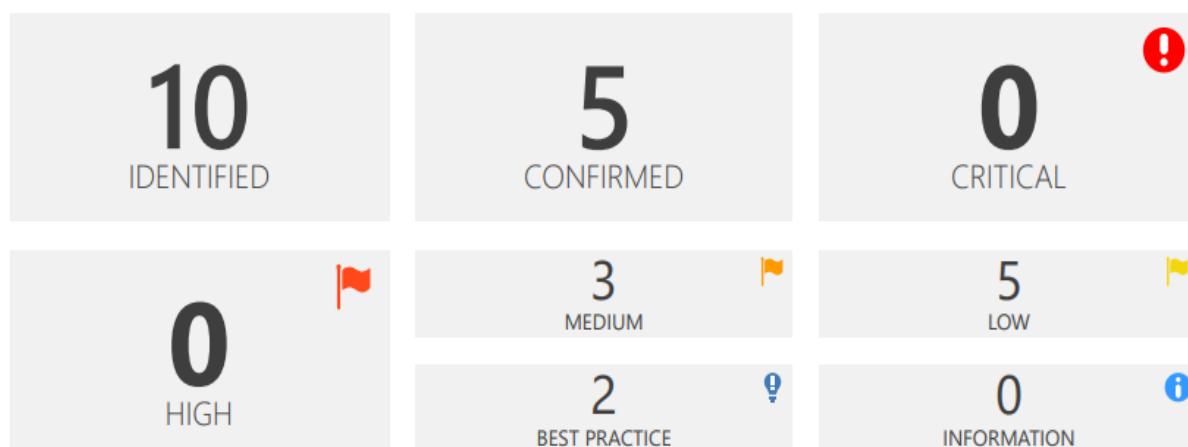
- Serve an HSTS header on the base domain for HTTPS requests:
  - The max-age must be at least 31536000 seconds (1 year)
  - The includeSubDomains directive must be specified
  - The preload directive must be specified
  - 
  - If you are serving an additional redirect from your HTTPS site, that redirect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



## Explanation

This report is generated based on OWASP Top Ten 2017 classification.

There are 2 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.



### Identified Vulnerabilities



### Confirmed Vulnerabilities



<https://www.amacc.aliexpress.com>

A6 - SECURITY MISCONFIGURATION

	<a href="#">Misconfigured Access-Control-Allow-Origin Header</a>	GET	https://amacc.aliexpress.com/cgi-bin/	<span>LOW</span>
	<a href="#">Missing X-Frame-Options Header</a>	GET	https://amacc.aliexpress.com/	<span>LOW</span>

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.

Vulnerabilities

5.1. https://amacc.aliexpress.com/

Certainty



Request

```
GET / HTTP/1.1
Host: amacc.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) : 1606.2008 Total Bytes Received : 1444 Body Length : 1097 Is Compressed : No

```
HTTP/1.1 403 Forbidden
Server: Tengine
x-alicdn-da-ups-status: end0s,0,403
Connection: keep-alive
Via: cache34.12cm10-9[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: a3b50b9916221030040616279e

<!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**

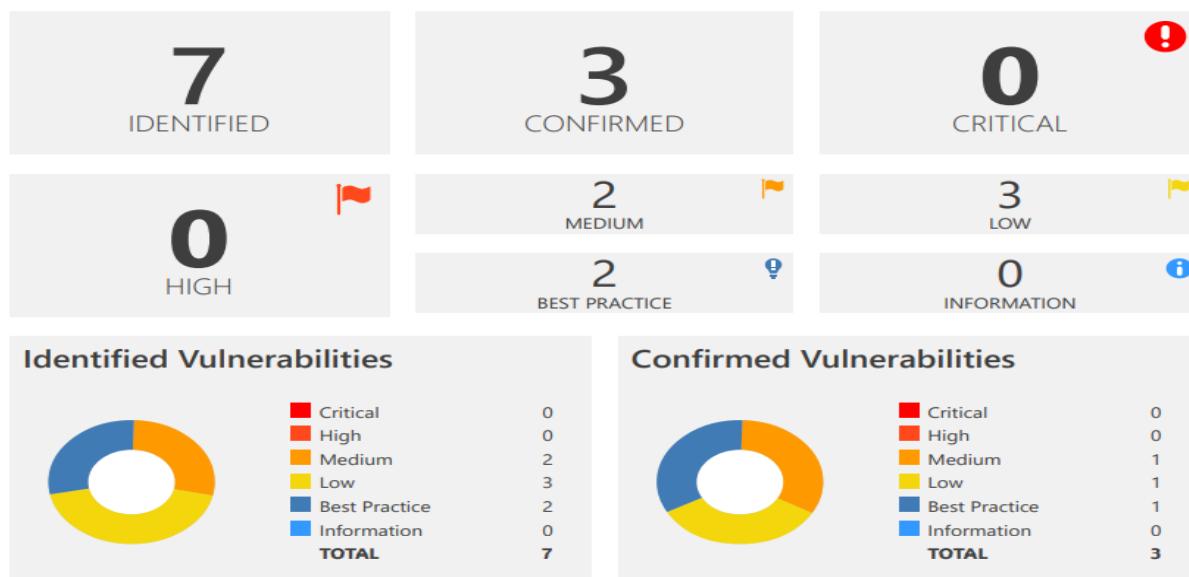
- ✓ Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
  - ✓ X-Frame-Options: DENYIt completely denies to be loaded in frame/iframe.
  - ✓ X-Frame-Options: SAMEORIGINIt allows only if the site which wants to load has a same origin.
  - ✓ 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

 <a href="https://amacc.aliexpress.com/">https://amacc.aliexpress.com/</a>	Scan Time : 5/27/2021 1:40:01 PM (UTC+05:30)	Scan Duration : 00:00:02:47	Total Requests : 993	Average Speed : 5.9r/s	Risk Level: <b>MEDIUM</b>
---	--	-----------------------------	----------------------	------------------------	---------------------------

### Explanation

This report is generated based on OWASP Top Ten 2017 classification.  
There are 4 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.



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

## Vulnerabilities By OWASP 2017

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
<b>A3 - SENSITIVE DATA EXPOSURE</b>				
	<a href="#">Weak Ciphers Enabled</a>	GET	<a href="https://api.dos.aliexpress.com/">https://api.dos.aliexpress.com/</a>	<span>MEDIUM</span>
	<a href="#">Insecure HTTP Usage</a>	GET	<a href="http://api.dos.aliexpress.com/">http://api.dos.aliexpress.com/</a>	<span>MEDIUM</span>
	<a href="#">Insecure Transportation Security Protocol Supported (TLS 1.0).</a>	GET	<a href="https://api.dos.aliexpress.com/">https://api.dos.aliexpress.com/</a>	<span>LOW</span>
	<a href="#">Insecure Transportation Security Protocol Supported (TLS 1.1).</a>	GET	<a href="https://api.dos.aliexpress.com/">https://api.dos.aliexpress.com/</a>	<span>BEST PRACTICE</span>
	<a href="#">Referrer-Policy Not Implemented</a>	GET	<a href="https://api.dos.aliexpress.com/">https://api.dos.aliexpress.com/</a>	<span>BEST PRACTICE</span>

## SENSITIVE DATA EXPOSURE

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

### Vulnerabilities

6.1. <https://api.dos.aliexpress.com/>

**CONFIRMED**

#### Request

[NETSPARKER] SSL Connection

#### Response

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

[NETSPARKER] SSL Connection

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.conf file 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 regedit32 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

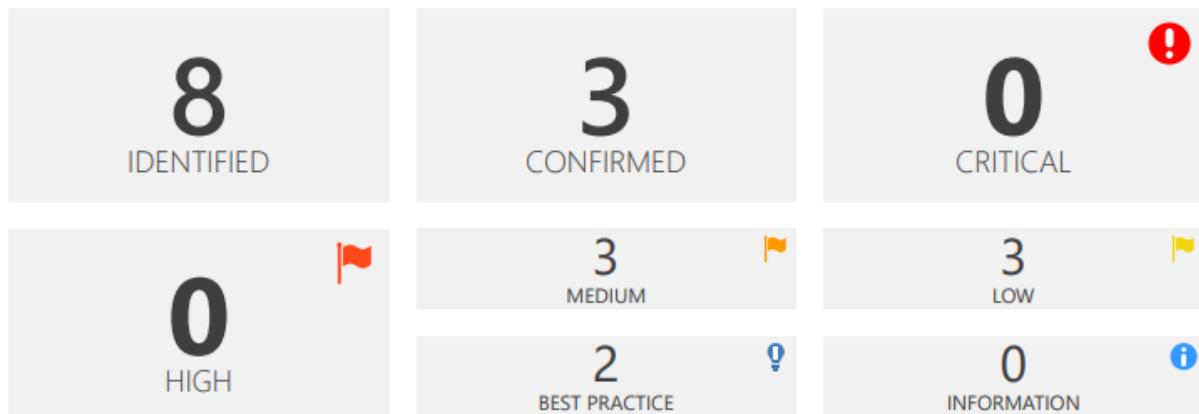
🔗 <https://api.dos.aliexpress.com/>

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.



### Identified Vulnerabilities



Critical	0
High	0
Medium	3
Low	3
Best Practice	2
Information	0
<b>TOTAL</b>	<b>8</b>

### Confirmed Vulnerabilities



Critical	0
High	0
Medium	1
Low	1
Best Practice	1
Information	0
<b>TOTAL</b>	<b>3</b>

<https://www.best.aliexpress.com>

## Vulnerabilities By OWASP 2017

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
<b>A3 - SENSITIVE DATA EXPOSURE</b>				
	<a href="#">Session Cookie Not Marked as Secure</a>	GET	https://best.aliexpress.com/ali/ae-traffic-kn-best-report/0.0.3/index.umd.js	HIGH
	<a href="#">Weak Ciphers Enabled</a>	GET	https://best.aliexpress.com/	MEDIUM
	<a href="#">Cookie Not Marked as Secure</a>	GET	https://best.aliexpress.com/	LOW
	<a href="#">Insecure Transportation Security Protocol Supported (TLS 1.0)</a>	GET	https://best.aliexpress.com/	LOW
	<a href="#">Insecure Transportation Security Protocol Supported (TLS 1.1)</a>	GET	https://best.aliexpress.com/	BEST PRACTICE
	<a href="#">Referrer-Policy Not Implemented</a>	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=Ckkntpzu6k7o899pmi0eeehfyhL8; acs_usuc_t=acs_rt=0d731d9abe6448d7aed516ca76af1e5a&x_csrf=10zvh6wfbwoe; ali_apache_id=10.182.248.30.1622106421106.449475.2; ali_apache_track=; ali_apache_tracktmp=; xman_f=PR51w7fvYhs0V6iaC8VvV1KFCRNLhSNj9nkTYG3CLArH3BFBBefTGJnvfaFj0LKI4588AVf6u7yZAHHzrs/YYvnblYTJD13zoHkC8Biis8fUILnflmQPoOHA==; xman_t=o9s07l4XN9E4YuwpXWmNbDAJBGWhLM851XnmdM+Bpx+SqJqAt+I5ys6p509YIjyf; xman_us_f=x_l=0&acs_rt=0d731d9abe6448d7aed516ca76af1e5a; isg=B0_vsmeI08msQtfk1Lk0zF3ufgP51E02xtZ65gF8i951UA9SCWTTBu0C1ljuMxsu; tfstk=c4khBuM3pXPCFyFiGpwIvFxoArvAwIQuW4uxQY-44uxhciCc715-HjdgdzhvGN; l=eBTjmKaRjkv39ugtBOfanurza770SIRYYuPzaNbMi0CP0B1B5uNPB6sHTLY6C3MNhs_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=.aliexpress.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=Fx0tZCYzx/0Bx7BMUV0+7DRKFFHfqfAiB8tp1Fzbywpo0zDZPX13Ug==; Domain=.aliexpress.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.

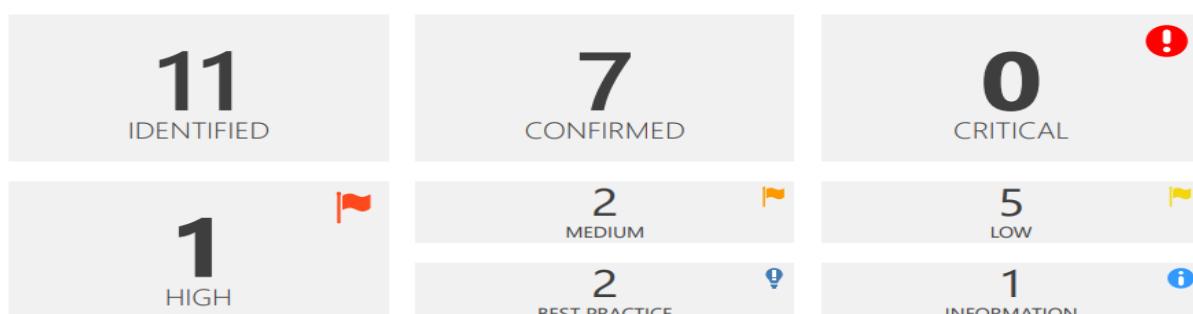
## Overview Summary



### Explanation

This report is generated based on OWASP Top Ten 2017 classification.

There are 4 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.



### Identified Vulnerabilities



Critical	0
High	1
Medium	2
Low	5
Best Practice	2
Information	1
<b>TOTAL</b>	<b>11</b>

### Confirmed Vulnerabilities



Critical	0
High	1
Medium	1
Low	4
Best Practice	1
Information	0
<b>TOTAL</b>	<b>7</b>

## <https://www.brands.aliexpress.com>

### A6 - SECURITY MISCONFIGURATION

	<a href="#">HTTP Strict Transport Security (HSTS) Errors and Warnings</a>	GET	<a href="https://brands.aliexpress.com/">https://brands.aliexpress.com/</a>	<span>MEDIUM</span>
	<a href="#">Misconfigured Access-Control-Allow-Origin Header</a>	GET	<a href="https://brands.aliexpress.com/.well-known/">https://brands.aliexpress.com/.well-known/</a>	<span>LOW</span>
	<a href="#">Missing X-Frame-Options Header</a>	GET	<a href="https://brands.aliexpress.com/">https://brands.aliexpress.com/</a>	<span>LOW</span>

### 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: 0b0a555816221036836112167e62b4
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=0e39e0fa1340796f99cf8b8ac587a9c&action=deny"></a> <script>document.getElementById("a-link").click();</script>
```

## Recommendations

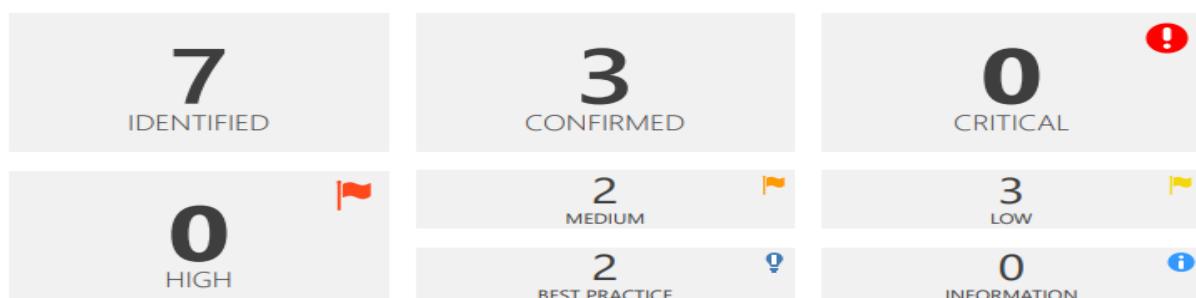
- ✓ Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
  - ✓ X-Frame-Options: DENYIt completely denies to be loaded in frame/iframe.
  - ✓ X-Frame-Options: SAMEORIGINIt allows only if the site which wants to load has a same origin.
  - ✓ 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



### 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	2
Low	3
Best Practice	2
Information	0
<b>TOTAL</b>	<b>7</b>

### Confirmed Vulnerabilities



Critical	0
High	0
Medium	1
Low	1
Best Practice	1
Information	0
<b>TOTAL</b>	<b>3</b>

<https://www.connectkeyword.aliexpress.com>

## SECURITY MISCONFIGURATION

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

### A6 - SECURITY MISCONFIGURATION

	<a href="#">HTTP Strict Transport Security (HSTS) Errors and Warnings</a>	GET	https://connectkeyword.aliexpress.com/	<span>MEDIUM</span>
	<a href="#">Misconfigured Access-Control-Allow-Origin Header</a>	GET	https://connectkeyword.aliexpress.com/.well-known/	<span>LOW</span>
	<a href="#">Missing X-Frame-Options Header</a>	GET	https://connectkeyword.aliexpress.com/	<span>LOW</span>

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

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

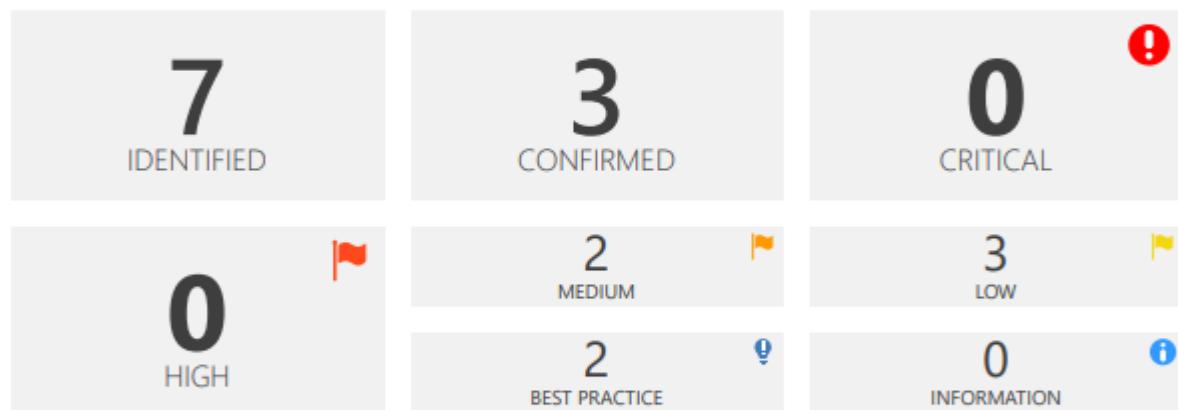
Risk Level:

**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.



### Identified Vulnerabilities



Critical	0
High	0
Medium	2
Low	3
Best Practice	2
Information	0
<b>TOTAL</b>	<b>7</b>

### Confirmed Vulnerabilities



Critical	0
High	0
Medium	1
Low	1
Best Practice	1
Information	0
<b>TOTAL</b>	<b>3</b>

<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

#### **Vulnerabilities**

8.1. <https://passport.aliexpress.com/>

#### **Certainty**



#### **Request**

```
GET / HTTP/1.1
Host: passport.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) : 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&action=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>
```

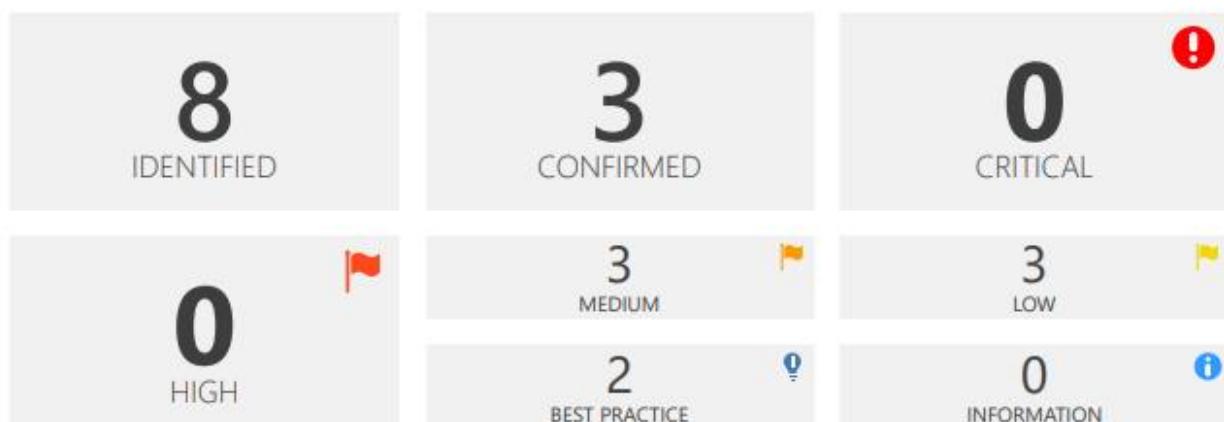
## Overview Summary

<a href="https://passport.aliexpress.com/">https://passport.aliexpress.com/</a>		Risk Level: <b>MEDIUM</b>
Scan Time	: 5/27/2021 12:49:59 PM (UTC+05:30)	
Scan Duration	: 00:00:04:10	
Total Requests	: 705	
Average Speed	: 2.8r/s	

## 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
<b>TOTAL</b>	<b>8</b>

### Confirmed Vulnerabilities



Critical	0
High	0
Medium	1
Low	1
Best Practice	1
Information	0
<b>TOTAL</b>	<b>3</b>

## Conclusion

This report has demonstrated the vulnerabilities and essential recommendations for the [www.aliexpress.com](http://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/](#)