

Sri Lanka Institute of Information Technology



Specialized in Cyber Security

Year 2, Semester 2

IE2062 – Web Security

Bug Bounty – Report 01

Student ID No.	Name
IT23136106	D.M.M. Pasindu Supushmika

Table of Contents

- 01. [Website Overview](#)
- 02. [Step 01: Gather Information](#)
 - a. [Subdomain Discovery](#)
 - i. [Sublist3r](#)
 - ii. [Subfinder](#)
 - b. [Live Subdomains](#)
 - c. [IP Discovery](#)
 - d. [Open Ports](#)
 - e. [Used Technologies](#)
- 03. [Step 02: Scanning and Vulnerability Identification](#)
 - a. [Identify Potential Vulnerabilities](#)
 - b. [PII Disclosure](#)
- 04. [Step 03: Exploitation and Validation](#)
- 05. [Step 04: Mitigation / Fix](#)

1. Website Overview

Flipkart.com – Indian Online Shopping website

HackerOne Link: [Flipkart](#) | [Bug Bounty Program Policy](#) | [HackerOne](#)

«

▼ Security page

Program guidelines

Scope

Hackactivity

Thanks

Updates

Collaborators

Overview

Last updated on April 7, 2025. [View changes](#)

At Flipkart, we take the security of our systems very seriously, and it is our constant endeavour to make our products secure for our customers. However, in the rare case when some security researcher or member of the general public identifies a vulnerability in our systems, and responsibly shares the details of it with us, we appreciate their contribution, work closely with them to address such issues, and ensure that they are rewarded fairly for their contribution.

Instructions for signing up Flipkart accounts


- Researchers having Indian phone number can sign up/login using OTP. Please make a note to not open multiple accounts creating spam.
- Only our Android application supports sign-up via international phone numbers.

Scope Rules and Policy - Including Out of Scope assets

We would advice to stick strictly to the scope defined for this program. Submissions on assets that are not within scope are not entertained however based on Severity and Business impact, may be considered for acceptance on a case by case basis.

Report Eligibility

- Be the first to report a vulnerability.
- Submit one vulnerability per report, unless you need to chain vulnerabilities to provide impact.
- Multiple vulnerabilities caused by one underlying issue will be awarded one bounty. If the root cause is the same and endpoints are different within the same application , it will be treated as a duplicate. Sometimes exceptions are made upon discreteness of Flipkart security team.
- Provide [high quality reports](#) with clear and comprehensive reproducible steps. High quality submissions allow our team to better understand the issue and relay the bug to the internal teams to fix it quickly.

 **Flipkart**

<https://flipkart.com>

[@Flipkart](#)

India's Biggest Online Store

Bug Bounty Program launched in Apr 2025

● Response efficiency: 96%

[Submit report](#)

Rewards

Severity	Rewards
<div>Low</div> <div>Avg. bounty \$250</div> <div>39.22% submissions</div>	\$200–\$350
<div>Medium</div> <div>Avg. bounty \$550</div> <div>33.33% submissions</div>	\$550–\$800
<div>High</div>	\$1,250–\$2,500

Activate Windows
Go to Settings to activate Windows.

Step 01: Gather Information.

a. Sub-domain Discovery

i. Sublist3r: [Sublist3r Result.txt](#)

Tool : Sublist3r

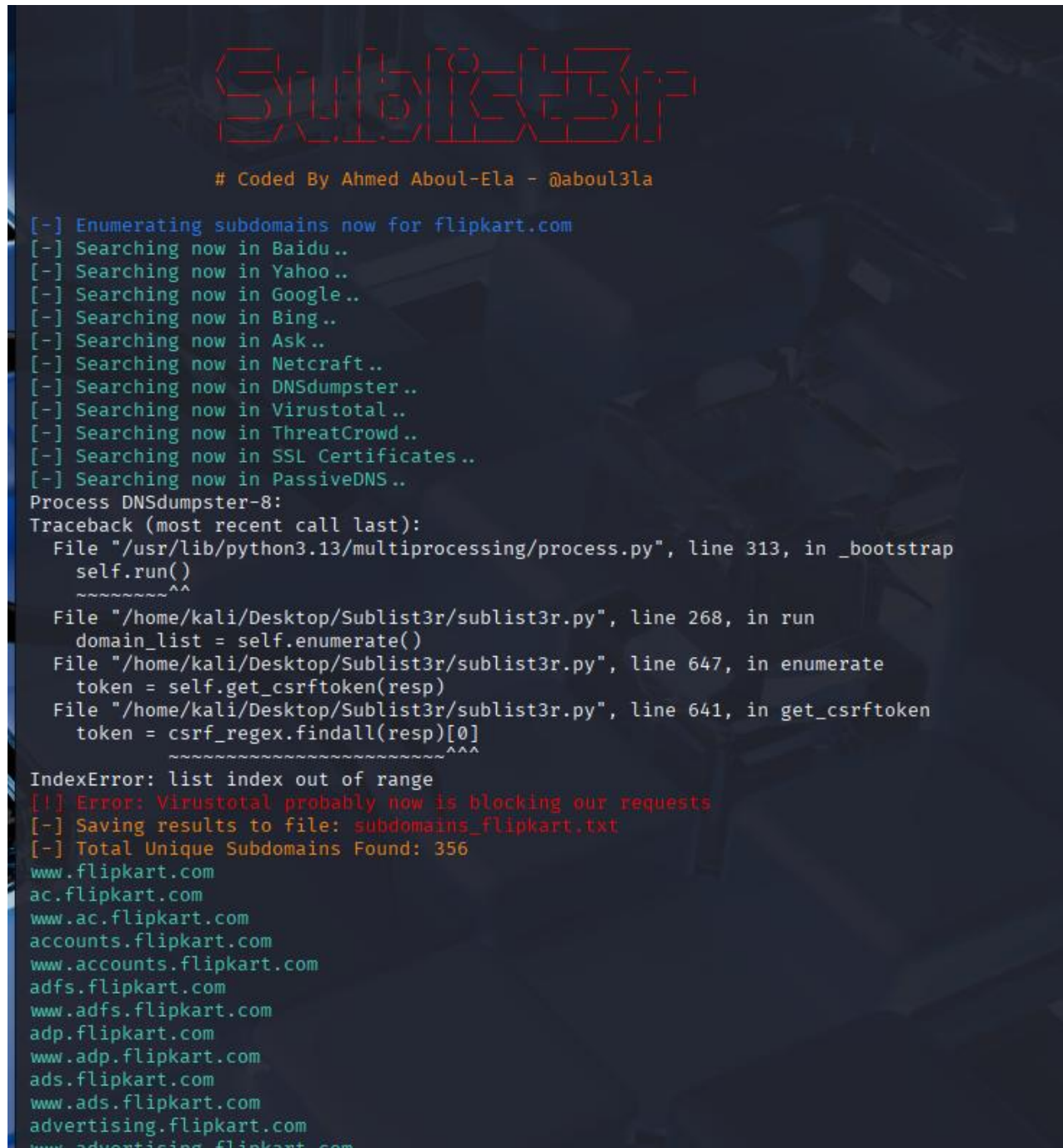
Code : python3 sublist3r.py -d flipkart.com -o subdomains_flipkart.txt

Explanation:

python3 sublist3r.py - Run the script using python

-d flipkart.com - Target domain

-o subdomains_flipkart.txt – Output file where the result is saved



```
Sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for flipkart.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..
Process DNSdumpster-8:
Traceback (most recent call last):
  File "/usr/lib/python3.13/multiprocessing/process.py", line 313, in _bootstrap
    self.run()
    ~~~~~^^
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 268, in run
    domain_list = self.enumerate()
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 647, in enumerate
    token = self.get_csrf_token(resp)
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 641, in get_csrf_token
    token = csrf_regex.findall(resp)[0]
    ~~~~~^
IndexError: list index out of range
[!] Error: Virustotal probably now is blocking our requests
[-] Saving results to file: subdomains_flipkart.txt
[-] Total Unique Subdomains Found: 356
www.flipkart.com
ac.flipkart.com
www.ac.flipkart.com
accounts.flipkart.com
www.accounts.flipkart.com
adfs.flipkart.com
www.adfs.flipkart.com
adp.flipkart.com
www.adp.flipkart.com
ads.flipkart.com
www.ads.flipkart.com
advertising.flipkart.com
www.advertising.flipkart.com
```

www.flipkart.com
 ac.flipkart.com
www.ac.flipkart.com
 accounts.flipkart.com
www.accounts.flipkart.com
 adfs.flipkart.com
www.adfs.flipkart.com
 adp.flipkart.com
www.adp.flipkart.com
 ads.flipkart.com
www.ads.flipkart.com
 advertising.flipkart.com
www.advertising.flipkart.com
 affiliate.flipkart.com
www.affiliate.flipkart.com
 1.bifrost.api.flipkart.com
www.1.bifrost.api.flipkart.com
 comms.api.flipkart.com
www.comms.api.flipkart.com
 edigateway-prod.api.flipkart.com
www.edigateway-prod.api.flipkart.com
 edigateway-uat.api.flipkart.com
www.edigateway-uat.api.flipkart.com
 1.fdp.api.flipkart.com
www.1.fdp.api.flipkart.com
 2.fdp.api.flipkart.com
 blog.flipkart.com
www.blog.flipkart.com
 bot.flipkart.com
www.bot.flipkart.com
 brandhub.flipkart.com
www.brandhub.flipkart.com
 brandmanager.flipkart.com
www.brandmanager.flipkart.com
 brands.flipkart.com
www.brands.flipkart.com
 ch.flipkart.com
 authn.ch.flipkart.com
www.authn.ch.flipkart.com
www.cloud.flipkart.com
 ads.cloud.flipkart.com
www.ads.cloud.flipkart.com
 checkout.cloud.flipkart.com
www.checkout.cloud.flipkart.com
 console.cloud.flipkart.com
www.console.cloud.flipkart.com
 fm.cloud.flipkart.com
www.fm.cloud.flipkart.com
 pricing.cloud.flipkart.com
www.pricing.cloud.flipkart.com
 pricing2.cloud.flipkart.com
www.pricing2.cloud.flipkart.com
 superset.pricing2.cloud.flipkart.com
www.superset.pricing2.cloud.flipkart.com
 api.translation.cloud.flipkart.com
www.api.translation.cloud.flipkart.com
 credolen-preprod.flipkart.com

www.2.fdp.api.flipkart.com
 sonic.fdp.api.flipkart.com
www.sonic.fdp.api.flipkart.com
 1.sonic.fdp.api.flipkart.com
 2.sonic.fdp.api.flipkart.com
 ondc.api.flipkart.com
www.ondc.api.flipkart.com
 ondc-preprod.api.flipkart.com
www.ondc-preprod.api.flipkart.com
 rome.api.flipkart.com
 1.rome.api.flipkart.com
 2.rome.api.flipkart.com
 upi.pg.rome.api.flipkart.com
www.upi.pg.rome.api.flipkart.com
 upi.rome.api.flipkart.com
www.upi.rome.api.flipkart.com
 1.upi.rome.api.flipkart.com
www.1.upi.rome.api.flipkart.com
 2.upi.rome.api.flipkart.com
www.2.upi.rome.api.flipkart.com
 auth.flipkart.com
www.auth.flipkart.com
 beta-homeservice.flipkart.com
www.beta-homeservice.flipkart.com
 beta-seller.flipkart.com
www.beta-seller.flipkart.com

 authn-meta.ch.flipkart.com
www.authn-meta.ch.flipkart.com
 bastion-backend.ch.flipkart.com
www.bastion-backend.ch.flipkart.com
 ibot.ch.flipkart.com
www.ibot.ch.flipkart.com
 induna.ch.flipkart.com
www.induna.ch.flipkart.com
 chat.flipkart.com
www.chat.flipkart.com
 1.chat.flipkart.com
 2.chat.flipkart.com
 cloud.flipkart.com
www.credolen-preprod.flipkart.com
 credolen-preprod-1.flipkart.com
 credolen-preprod-2.flipkart.com
 cri-playground.flipkart.com
www.cri-playground.flipkart.com
 cri-trino.flipkart.com
www.cri-trino.flipkart.com
 delivery.flipkart.com
 partners.digital.flipkart.com
www.partners.digital.flipkart.com
 dl.flipkart.com
 dummy.flipkart.com
www.dummy.flipkart.com
 uat.edigateway.flipkart.com
www.uat.edigateway.flipkart.com
 ekl-argo.flipkart.com
www.ekl-argo.flipkart.com
 ekl-fm-during.flipkart.com

www.ekl-fm-during.flipkart.com
www.ekl-port-app.flipkart.com
 enrich.flipkart.com
www.enrich.flipkart.com
 enterprise.flipkart.com
www.enterprise.flipkart.com
 fact-extractor.flipkart.com
www.fact-extractor.flipkart.com
 fact-extractor-preprod.flipkart.com
www.fact-extractor-preprod.flipkart.com
 stage.farmtohome.flipkart.com
www.stage.farmtohome.flipkart.com
 fddkim.flipkart.com
 finapi.flipkart.com
 1.finapi.flipkart.com
 2.finapi.flipkart.com
 preprod.finapi.flipkart.com
www.preprod.finapi.flipkart.com
 1.preprod.finapi.flipkart.com
 2.preprod.finapi.flipkart.com
 3.preprod.finapi.flipkart.com
 4.preprod.finapi.flipkart.com
 sm.finapi.flipkart.com
www.sm.finapi.flipkart.com
 firedrops.flipkart.com
 healthplus.flipkart.com
www.healthplus.flipkart.com
 homeservice.flipkart.com
www.homeservice.flipkart.com
 hubsystem.flipkart.com
www.hubsystem.flipkart.com
 ibot.hyd.flipkart.com
www.ibot.hyd.flipkart.com
 induna.hyd.flipkart.com
www.induna.hyd.flipkart.com
 icap.flipkart.com
www.icap.flipkart.com
 icapch.flipkart.com
www.icapch.flipkart.com
 icapws.flipkart.com
www.icapws.flipkart.com
 img.flipkart.com
www.img.flipkart.com
 edge-hyd.fkcloud.inpartners.flipkart.com
 insights.flipkart.com
www.insights.flipkart.com
 insights-preprod.flipkart.com
www.insights-preprod.flipkart.com
 insurance.flipkart.com
www.insurance.flipkart.com
 insurance-preprod.flipkart.com
 jcs.flipkart.com
www.jcs.flipkart.com
 jeeves.flipkart.com
www.jeeves.flipkart.com
 l.flipkart.com
www.l.flipkart.com
 listings.flipkart.com

ekl-port-app.flipkart.com
 fkipl.flipkart.com
www.fkipl.flipkart.com
 ctrlw-rpaocapp.fkipl.flipkart.com
www.ctrlw-rpaocapp.fkipl.flipkart.com
 fk-prisma-panorama-1.fkipl.flipkart.com
www.fk-prisma-panorama-1.fkipl.flipkart.com
 fpay.flipkart.com
www.fpay.flipkart.com
 1.fpay.flipkart.com
 2.fpay.flipkart.com
www.2.fpay.flipkart.com
 uat.fpg.flipkart.com
www.uat.fpg.flipkart.com
 friedrops.flipkart.com
 ftcollections.flipkart.com
www.ftcollections.flipkart.com
 accounting.prod.gateway.flipkart.com
www.accounting.prod.gateway.flipkart.com
 accounting.uat.gateway.flipkart.com
www.accounting.uat.gateway.flipkart.com
 looster1r.flipkart.com
www.gibraltar.flipkart.com
 looster1r-preprod.flipkart.com
www.gibraltar-preprod.flipkart.com
www.listings.flipkart.com
 location.flipkart.com
 preprod.location.flipkart.com
www.preprod.location.flipkart.com
 m.flipkart.com
www.m.flipkart.com
 maps.flipkart.com
www.maps.flipkart.com
 msite-stage1.flipkart.com
 msite-stage10.flipkart.com
 msite-stage2.flipkart.com
 msite-stage3.flipkart.com
 msite-stage4.flipkart.com
 msite-stage5.flipkart.com
 msite-stage6.flipkart.com
 msite-stage7.flipkart.com
 msite-stage8.flipkart.com
 msite-stage9.flipkart.com
 mx.flipkart.com
 delivery.ncb.flipkart.com
 delivery.ncp.flipkart.com
 delivery.nct.flipkart.com
 neo.flipkart.com
www.neo.flipkart.com
 nm.flipkart.com
 console.nm.flipkart.com
 ctrls-ldap-slave.nm.flipkart.com
www.ctrls-ldap-slave.nm.flipkart.com
 ekl-fm-ui.nm.flipkart.com
www.ekl-fm-ui.nm.flipkart.com
 nm-ldap.nm.flipkart.com
www.nm-ldap.nm.flipkart.com
 nm-ldap-slave.nm.flipkart.com

www.nm-ldap-slave.nm.flipkart.com
suv-ui.nm.flipkart.com
www.suv-ui.nm.flipkart.com
toph.nm.flipkart.com
www.toph.nm.flipkart.com
zuko.nm.flipkart.com
www.zuko.nm.flipkart.com
pandora.flipkart.com
www.pandora.flipkart.com
partner.flipkart.com
www.partner.flipkart.com
partners.flipkart.com
www.partners.flipkart.com
pay.flipkart.com
payments.flipkart.com
www.payments.flipkart.com
1.payments.flipkart.com
2.payments.flipkart.com
phantom.flipkart.com
www.phantom.flipkart.com
desktop.phantom.flipkart.com
msite.phantom.flipkart.com
preprod.flipkart.com
www.preprod.flipkart.com
pandora.preprod.flipkart.com
www.pandora.preprod.flipkart.com
preprod-adp.flipkart.com
www.preprod-adp.flipkart.com
reset.flipkart.com
www.reset.flipkart.com
rv-next1.flipkart.com
rv-next2.flipkart.com
stream-hyd.flipkart.com
www.stream-hyd.flipkart.com
tech.flipkart.com
www.tech.flipkart.com
travel.flipkart.com
www.travel.flipkart.com
travelqa.flipkart.com
www.travelqa.flipkart.com
upi-gateway-pg.flipkart.com
www.upi-gateway-pg.flipkart.com
1.upi-gateway-pg.flipkart.com
upi-gateway-preprod.flipkart.com
www.upi-gateway-preprod.flipkart.com
upi-gateway-prod.flipkart.com
www.upi-gateway-prod.flipkart.com
1.upi-gateway-prod.flipkart.com
2.upi-gateway-prod.flipkart.com
www.2.upi-gateway-prod.flipkart.com
upi-pg.flipkart.com
www.upi-pg.flipkart.com
1.upi-pg.flipkart.com
2.upi-pg.flipkart.com
upi-pg-cs.flipkart.com
www.upi-pg-cs.flipkart.com
upi-preprod.flipkart.com
www.upi-preprod.flipkart.com

secure.flipkart.com
securechat.flipkart.com
www.securechat.flipkart.com
seller.flipkart.com
www.seller.flipkart.com
delivery.seller.flipkart.com
sellers.flipkart.com
www.sellers.flipkart.com
sentry.flipkart.com
www.sentry.flipkart.com
slashn.flipkart.com
sm-aapi-preprod.flipkart.com
www.sm-aapi-preprod.flipkart.com
sm-pandora.flipkart.com
www.sm-pandora.flipkart.com
sm-pl-aapi.flipkart.com
www.sm-pl-aapi.flipkart.com
sm-pl-aapi-preprod.flipkart.com
www.sm-pl-aapi-preprod.flipkart.com
stage.flipkart.com
store.flipkart.com
airtel.store.flipkart.com
axis.store.flipkart.com
looster.store.flipkart.com
indusind.store.flipkart.com
itzcash.store.flipkart.com
offers.store.flipkart.com
yahoo.store.flipkart.com
yono.store.flipkart.com
stories.flipkart.com
www.stories.flipkart.com
stream.flipkart.com
www.stream.flipkart.com
1.upi-preprod.flipkart.com
upi-prod.flipkart.com
www.upi-prod.flipkart.com
upi-prod-cs.flipkart.com
www.upi-prod-cs.flipkart.com
vendorhub.flipkart.com
www.vendorhub.flipkart.com
vendorportal.flipkart.com
www.vendorportal.flipkart.com
vendorsupport.flipkart.com
ventures.flipkart.com
www.ventures.flipkart.com
looster.flipkart.com
www.wooster.flipkart.com
zion-stage1.flipkart.com
www.zion-stage1.flipkart.com
zion-stage10.flipkart.com
zion-stage11.flipkart.com
zion-stage12.flipkart.com
zion-stage13.flipkart.com
zion-stage14.flipkart.com
zion-stage15.flipkart.com
zion-stage16.flipkart.com
zion-stage17.flipkart.com
zion-stage18.flipkart.com
zion-stage19.flipkart.com

zion-stage2.flipkart.com
zion-stage20.flipkart.com
zion-stage3.flipkart.com
zion-stage4.flipkart.com
zion-stage5.flipkart.com

zion-stage6.flipkart.com
zion-stage7.flipkart.com
zion-stage8.flipkart.com
zion-stage9.flipkart.com

ii. Subfinder: [Subfinder_Result.txt](#)**Tool** : Subfinder**Code** : subfinder -d flipkart.com -o subfinder_result.txt**Explanation:***Subfinder* - run subfinder tool*-d flipkart.com* - Mention the target website*-o subfinder_result.txt* - Mention the output file

```

projectdiscovery.io

[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for flipkart.com
1.upi.rome.api.flipkart.com
checkout.cloud.flipkart.com
ncmail129.ncb.flipkart.com
pepimail133.nct.flipkart.com
2.upi-gateway-prod.flipkart.com
zion-stage11.flipkart.com
ncmail121.ncb.flipkart.com
ncmail73.ncb.flipkart.com
ac.flipkart.com
1.rome.api.flipkart.com
location.flipkart.com
dl.flipkart.com
pepi70.in.ncb.flipkart.com
hubsystem.flipkart.com
induna.hyd.flipkart.com
maps.flipkart.com
axis.store.flipkart.com
2.upi-pg.flipkart.com
2.chat.flipkart.com
pepimail149.nct.flipkart.com
2.payments.flipkart.com
test2.flipkart.com
chat.flipkart.com
api.translation.cloud.flipkart.com
partners.digital.flipkart.com
pepimail145.nct.flipkart.com
pricing.cloud.flipkart.com
zion-stage14.flipkart.com
cloud.flipkart.com
zion-stage2.flipkart.com
enterprise.flipkart.com
stream-hyd.flipkart.com
zion-stage16.flipkart.com
ncmail128.ncb.flipkart.com
nmplay-ekl-port-app.flipkart.com
2.rome.api.flipkart.com
ekl-fm-during.flipkart.com
o17.email.flipkart.com
pepimail62.ncp.flipkart.com

```

upi-prod.flipkart.com
 accounting.uat.gateway.flipkart.com
 preprod-adp.flipkart.com
 www.sentry.flipkart.com
 o13.email.flipkart.com
 www.2.upi-gateway-prod.flipkart.com
 msite-stage7.flipkart.com
 affiliate.flipkart.com
 o6.email.flipkart.com
 comms.api.flipkart.com
 www.upi.pg.rome.api.flipkart.com

img.flipkart.com
 www.2.fdp.api.flipkart.com
 uat.fpg.flipkart.com
 o40.ptr2142.sgp.flipkart.com
 zion-stage19.flipkart.com
 store.flipkart.com
 enrich.flipkart.com
 pepi54.in.nct.flipkart.com
 pepi58.in.nct.flipkart.com
 www.affiliate.flipkart.com
 new.flipkart.com

ctrls-ldap-slave.nm.flipkart.com
desktop.phantom.flipkart.com
www.l.flipkart.com
www.brands.flipkart.com
webreader.flipkart.com
2.upi.rome.api.flipkart.com
www.cri-trino.flipkart.com
deliver.ncp.flipkart.com
upi.pg.rome.api.flipkart.com
phantom.flipkart.com
1.fpay.flipkart.com
www.induna.ch.flipkart.com
dummy.flipkart.com
fpay.flipkart.com
ekl-port-app.flipkart.com
ncmail73.ncb.flipkart.com
fk-prisma-panorama-1.fkipl.flipkart.com
fm.cloud.flipkart.com
bot.flipkart.com
www.neo.flipkart.com
beta.flipkart.com
www.ekl-fm-during.flipkart.com
sendgrid.flipkart.com
edge-hyd.fkcloud.inpartners.flipkart.com
www.partners.flipkart.com
static03.digital.flipkart.com
ads.flipkart.com
www.preprod.finapi.flipkart.com
pepi57.in.nct.flipkart.com
www.l.upi.rome.api.flipkart.com
upi-gateway-prod.flipkart.com
firedrops.flipkart.com
pepimail130.nct.flipkart.com
cri-playground.flipkart.com
pepimail138.ncp.flipkart.com
www.uat.edigateway.flipkart.com
www.upi-preprod.flipkart.com
www.authn-meta.ch.flipkart.com
airtel.store.flipkart.com
www.advertising.flipkart.com
flap-tk.ads.flipkart.com
beta-seller.flipkart.com
o17.email.flipkart.com
www.credolen-preprod.flipkart.com
1.sonic.fdp.api.flipkart.com
www.sm-pl-aapi.flipkart.com
www.upi-gateway-preprod.flipkart.com
pay.flipkart.com
maps.flipkart.com
pepi70.in.ncb.flipkart.com
ncmail85.ncb.flipkart.com
www.sonic.fdp.api.flipkart.com
www.sm-pandora.flipkart.com
flipkart.com
chat.flipkart.com
www.brandmanager.flipkart.com
www.pandora.preprod.flipkart.com
api.flipkart.com
upi.rome.api.flipkart.com
securechat.flipkart.com
www.ekl-argo.flipkart.com
www.fact-extractor-preprod.flipkart.com
ibot.ch.flipkart.com
misc1-vm1.store.flipkart.com

stories.flipkart.com
zion-stage7.flipkart.com
o5.email.flipkart.com
ncmail129.ncb.flipkart.com
rv-next1.flipkart.com
m.flipkart.com
hackday.flipkart.com
www.edigateway-uat.api.flipkart.com
www.nm-ldap.nm.flipkart.com
www.console.cloud.flipkart.com
pepi53.in.nct.flipkart.com
www.m.flipkart.com
yahoo.store.flipkart.com
static01.digital.flipkart.com
pepi69.in.ncb.flipkart.com
3.preprod.finapi.flipkart.com
test.flipkart.com
zion-stage4.flipkart.com
www.upi-prod-cs.flipkart.com
offers.store.flipkart.com
www-sp.flipkart.com
o7.email.flipkart.com
www.adfs.flipkart.com
www.wooster.flipkart.com
www.adp.flipkart.com
www.hubsystem.flipkart.com
pepimail145.nct.flipkart.com
homeservice.flipkart.com
authn.ch.flipkart.com
axis.store.flipkart.com
edigateway-uat.api.flipkart.com
o14.email.flipkart.com
1.upi-preprod.flipkart.com
www.insights.flipkart.com
o19.email.flipkart.com
o21.email.flipkart.com
o3.email.flipkart.com
insights-preprod.flipkart.com
306fc.store.flipkart.com
o38.ptr4558.sgp.flipkart.com
zion-stage16.flipkart.com
www.partners.digital.flipkart.com
ch.flipkart.com
beta-homeservice.flipkart.com
www.insights-preprod.flipkart.com
2.rome.api.flipkart.com
pepimail62.ncp.flipkart.com
www.homeservice.flipkart.com
www.ctrlw-rpaocapp.fkipl.flipkart.com
www.ads.cloud.flipkart.com
zion-stage12.flipkart.com
cri-trino.flipkart.com
upi-pg-cs.flipkart.com
zion-stage20.flipkart.com
www.cri-playground.flipkart.com
www.seller.flipkart.com
msite-stage9.flipkart.com
pepi55.in.nct.flipkart.com
www.stories.flipkart.com
upi-pg.flipkart.com
www.accounts.flipkart.com
vendorhub.flipkart.com
zion-stage18.flipkart.com
ads.cloud.flipkart.com

o8.email.flipkart.com
nm.flipkart.com
pepimail135.ncp.flipkart.com
sm-pl-aapi.flipkart.com
www.2.upi.rome.api.flipkart.com
www.upi-pg-cs.flipkart.com
www.ads.flipkart.com
pricing2.cloud.flipkart.com
sellers.flipkart.com
pandora.preprod.flipkart.com
www.sm-pl-aapi-preprod.flipkart.com
o43.ptr9872.sgp.flipkart.com
zion-stage11.flipkart.com
credolen-preprod-1.flipkart.com
delivery.nct.flipkart.com
pepi66.in.ncp.flipkart.com
gibraltar-preprod.flipkart.com
static02.digital.flipkart.com
o10.email.flipkart.com
pepi52.in.nct.flipkart.com
old-console.nm.flipkart.com
fact-extractor.flipkart.com
www.fkipl.flipkart.com
www.induna.hyd.flipkart.com
comms.flipkart.com
ondc.api.flipkart.com
www.nm-ldap-slave.nm.flipkart.com
ekl-fm-ui.nm.flipkart.com
zion-stage2.flipkart.com
www.upi.rome.api.flipkart.com
upi-gateway-preprod.flipkart.com
accounts.flipkart.com
pepi59.in.ncp.flipkart.com
test2.flipkart.com
zion-stage5.flipkart.com
www.upi-prod.flipkart.com
itzcash.store.flipkart.com
insurance.flipkart.com
digital.flipkart.com
pepi64.in.ncp.flipkart.com
www.ibot.ch.flipkart.com
www.blog.flipkart.com
pepi62.in.ncp.flipkart.com
www.travelqa.flipkart.com
uat.edigateway.flipkart.com
yono.store.flipkart.com
www.stage.farmtohome.flipkart.com
msite-stage2.flipkart.com
o9.email.flipkart.com
www.reset.flipkart.com
www.checkout.cloud.flipkart.com
v.flipkart.com
console.cloud.flipkart.com
o23.email.flipkart.com
pepimail137.ncp.flipkart.com
friedrops.flipkart.com
www.upi-gateway-prod.flipkart.com
o15.email.flipkart.com
pepimail136.ncp.flipkart.com
www.superset.pricing2.cloud.flipkart.com
vendorsupport.flipkart.com
pepi74.in.ncb.flipkart.com
ncmail128.ncb.flipkart.com
www.uat.fpg.flipkart.com
icapch.flipkart.com
preprod.finapi.flipkart.com
2.upi-gateway-prod.flipkart.com
location.flipkart.com
o25.email.flipkart.com
partner.flipkart.com
brands.flipkart.com
ncmail74.ncb.flipkart.com
www.beta-homeservice.flipkart.com
msite-stage8.flipkart.com
pepi56.in.nct.flipkart.com
2.chat.flipkart.com
www.icap.flipkart.com
www.stream-hyd.flipkart.com
wooster.flipkart.com
partners.flipkart.com
ncb.flipkart.com
pepi73.in.ncb.flipkart.com
pepimail150.ncp.flipkart.com
pepimail71.ncp.flipkart.com
credolen-preprod-2.flipkart.com
www.sm.finapi.flipkart.com
induna.hyd.flipkart.com
gj0225gj.store.flipkart.com
insurance-preprod.flipkart.com
upi-preprod.flipkart.com
secure.flipkart.com
zuko.nm.flipkart.com
www.sb.flipkart.com
www.ekl-port-app.flipkart.com
www.phantom.flipkart.com
jcs.flipkart.com
zion-stage10.flipkart.com
pepimail149.nct.flipkart.com
travel.flipkart.com
credolen-preprod.flipkart.com
www.fm.cloud.flipkart.com
www.suv-ui.nm.flipkart.com
zion-stage3.flipkart.com
o22.email.flipkart.com
www.zion-stage1.flipkart.com
sm-pandora.flipkart.com
fkipl.flipkart.com
o24.email.flipkart.com
www.sm-aapi-preprod.flipkart.com
www.jcs.flipkart.com
enterprise.flipkart.com
pepimail147.nct.flipkart.com
rv-next2.flipkart.com
www.gibraltar.flipkart.com
upi-prod-cs.flipkart.com
auth.flipkart.com
1.rome.api.flipkart.com
1.flipkart.com
2.sonic.fdp.api.flipkart.com
edigateway-prod.api.flipkart.com
www.ibot.hyd.flipkart.com
www.pricing.cloud.flipkart.com
zion-stage9.flipkart.com
www.edigateway-prod.api.flipkart.com
www.ac.flipkart.com
www.accounting.prod.gateway.flipkart.com
www.1.bifrost.api.flipkart.com
delivery.ncp.flipkart.com

zion-stage13.flipkart.com
www.stream.flipkart.com
o20.email.flipkart.com
www.healthplus.flipkart.com
advertising.flipkart.com
k8s-prd.store.flipkart.com
blog.flipkart.com
zion-stage8.flipkart.com
icapws.flipkart.com
sm.finapi.flipkart.com
www.pricing2.cloud.flipkart.com
msite-stage6.flipkart.com
www.authn.ch.flipkart.com
ekl-argo.flipkart.com
www.enrich.flipkart.com
pepi67.in.ncb.flipkart.com
o11.email.flipkart.com
gibraltar.flipkart.com
1.finapi.flipkart.com
2.fdp.api.flipkart.com
o1.email.flipkart.com
pepi68.in.ncb.flipkart.com
www.preprod-adp.flipkart.com
www.gibraltar-preprod.flipkart.com
2.fpay.flipkart.com
o16.email.flipkart.com
1.upi-gateway-pg.flipkart.com
upi-gateway-pg.flipkart.com
4.preprod.finapi.flipkart.com
sonic.fdp.api.flipkart.com
hubsystem.flipkart.com
pepi51.in.nct.flipkart.com
zion-stage1.flipkart.com
www.comms.api.flipkart.com
pepi72.in.ncb.flipkart.com
www.enterprise.flipkart.com
www.auth.flipkart.com
stream-hyd.flipkart.com
www.partner.flipkart.com
1.upi.rome.api.flipkart.com
www.fk-prisma-panorama-1.fkipl.flipkart.com
pepi71.in.ncb.flipkart.com
pepi60.in.ncp.flipkart.com
zion-stage14.flipkart.com
zion-stage17.flipkart.com
delivery.seller.flipkart.com
pepimail131.nct.flipkart.com
pepimail133.nct.flipkart.com
console.nm.flipkart.com
insights.flipkart.com
api.translation.cloud.flipkart.com
ibot.hyd.flipkart.com
pepi65.in.ncp.flipkart.com
pepimail61.ncp.flipkart.com
www.ctrls-ldap-slave.nm.flipkart.com
www.icapws.flipkart.com
www.vendorhub.flipkart.com
downloadi.flipkart.com
pepi63.in.ncp.flipkart.com
finapi.flipkart.com
www.ventures.flipkart.com
www.img.flipkart.com
ekl-fm-during.flipkart.com
sip.flipkart.com

ondc-preprod.api.flipkart.com
superset.pricing2.cloud.flipkart.com
zion-stage15.flipkart.com
ventures.flipkart.com
adfs.flipkart.com
1.payments.flipkart.com
ctrlw-rpaocapp.fkipl.flipkart.com
www.bastion-backend.ch.flipkart.com
neo.flipkart.com
www.fact-extractor.flipkart.com
bastion-backend.ch.flipkart.com
www.bot.flipkart.com
jeeves.flipkart.com
ww.flipkart.com
2.upi-pg.flipkart.com
www.brandhub.flipkart.com
toph.nm.flipkart.com
preprod.location.flipkart.com
pepi61.in.ncp.flipkart.com
stage.flipkart.com
vendorportal.flipkart.com
payments.flipkart.com
ncmail86.ncb.flipkart.com
www.dummy.flipkart.com
o42.ptr6005.sgp.flipkart.com
www.2.fpay.flipkart.com
indusind.store.flipkart.com
claimfreegiftcard.flipkart.com
healthplus.flipkart.com
2.finapi.flipkart.com
www.pandora.flipkart.com
www.chat.flipkart.com
www.preprod.location.flipkart.com
www.maps.flipkart.com
brandmanager.flipkart.com
www3.flipkart.com
www.cloud.flipkart.com
adp.flipkart.com
suv-ui.nm.flipkart.com
www.upi-gateway-pg.flipkart.com
www.beta-seller.flipkart.com
seller.flipkart.com
o18.email.flipkart.com
sentry.flipkart.com
sentry.flipkart.com
www.insurance.flipkart.com
www.ekl-fm-ui.nm.flipkart.com
1.preprod.finapi.flipkart.com
bhaskar.store.flipkart.com
1.fdp.api.flipkart.com
pandora.flipkart.com
nm-ldap.nm.flipkart.com
delivery.flipkart.com
slashn.flipkart.com
www.sellers.flipkart.com
www.preprod.flipkart.com
fddkim.flipkart.com
pepimail132.nct.flipkart.com
www.ftcollections.flipkart.com
pepimail70.ncp.flipkart.com
nmplay-ekl-port-app.flipkart.com
o36.ptr9478.sgp.flipkart.com
www.payments.flipkart.com
www.vendorportal.flipkart.com
sdlchook.flipkart.com

www.toph.nm.flipkart.com
stage.farntohome.flipkart.com
rome.api.flipkart.com
pricing.cloud.flipkart.com
www.securechat.flipkart.com
zion-stage6.flipkart.com
brandhub.flipkart.com
msite-stage5.flipkart.com
authn-meta.ch.flipkart.com
preprod.flipkart.com
10.72.180.60sentry.flipkart.com
checkout.cloud.flipkart.com
ctl.weread.flipkart.com
travelqa.flipkart.com
nm-ldap-slave.nm.flipkart.com
pepimail139.ncp.flipkart.com
pepimail134.nct.flipkart.com
stream.flipkart.com
delivery.ncb.flipkart.com
ncmail127.ncb.flipkart.com
www.listings.flipkart.com
www.travel.flipkart.com
msite-stage10.flipkart.com
axiszion-stage11.store.flipkart.com
o4.email.flipkart.com
www.ondc.api.flipkart.com
o39.ptr2597.sgp.flipkart.com
cloud.flipkart.com
pepimail146.nct.flipkart.com
pepimail148.nct.flipkart.com
www.upi-pg.flipkart.com
www.fpay.flipkart.com
msite-stage3.flipkart.com
email.flipkart.com
partners.digital.flipkart.com
1.upi-gateway-prod.flipkart.com
sm-pl-aapi-preprod.flipkart.com
2.preprod.finapi.flipkart.com

www.ondc-preprod.api.flipkart.com
www.accounting.uat.gateway.flipkart.com
accounting.prod.gateway.flipkart.com
tech.flipkart.com
o2.email.flipkart.com
ncmail126.ncb.flipkart.com
ac.flipkart.com
1.upi-pg.flipkart.com
www.api.translation.cloud.flipkart.com
www.1.fdp.api.flipkart.com
induna.ch.flipkart.com
www.jeeves.flipkart.com
ebook.digital.flipkart.com
ncmail121.ncb.flipkart.com
mx.flipkart.com
www.zuko.nm.flipkart.com
fact-extractor-preprod.flipkart.com
icap.flipkart.com
2.payments.flipkart.com
ncmail72.ncb.flipkart.com
dl.flipkart.com
www.icapch.flipkart.com
www.flipkart.com
reset.flipkart.com
1.bifrost.api.flipkart.com
ftcollections.flipkart.com
msite.phantom.flipkart.com
o41.ptr6943.sgp.flipkart.com
o12.email.flipkart.com
o37.ptr9297.sgp.flipkart.com
msite-stage4.flipkart.com
www.tech.flipkart.com
sentry.flipkart.com
sm-aapi-preprod.flipkart.com
msite-stage1.flipkart.com
listings.flipkart.com
1.chat.flipkart.com

b. Live Subdomain Discovery

Tool : [httpx: Live Subdomain Results.txt](#)

Code : `httpx-toolkit -l subfinder_result.txt -o livesub_results.txt`

Explanation:

`httpx-toolkit` - run the httpx tool

`-l subfinder_result.txt` – mention the file containing input

`-o livesub_results.txt` – mention the file which should write the output

```
(kali㉿kali)-[~/Desktop/Sublist3r/flipkart]
$ httpx-toolkit -l subfinder_result.txt -o livesub_results.txt

Example:
$ httpx-toolkit -l subfinder_result.txt -o livesub_results.txt
v1.1.5

reprod.flipkart.com
specified, so projectdiscovery.io

Use with caution. You are responsible for your actions.
Developers assume no liability and are not responsible for any misuse or damage.
https://2.sonic.fdp.api.flipkart.com
https://1.sonic.fdp.api.flipkart.com
https://auth.flipkart.com
https://1.fdp.api.flipkart.com
https://1.finapi.flipkart.com
https://advertising.flipkart.com
https://accounts.flipkart.com
https://2.upi.rome.api.flipkart.com
https://1.fpay.flipkart.com
https://1.upi-pg.flipkart.com
https://airtel.store.flipkart.com
https://1.chat.flipkart.com
https://api.translation.cloud.flipkart.com
https://1.upi-gateway-prod.flipkart.com
https://2.chat.flipkart.com
https://1.upi-gateway-pg.flipkart.com
https://ac.flipkart.com
https://2.fpay.flipkart.com
https://affiliate.flipkart.com
https://adp.flipkart.com
https://2.finapi.flipkart.com
https://beta-seller.flipkart.com
https://bhaskar.store.flipkart.com
https://ads.cloud.flipkart.com
https://2.upi-pg.flipkart.com
https://delivery.ncp.flipkart.com
https://delivery.seller.flipkart.com
https://brandhub.flipkart.com
https://brandmanager.flipkart.com
https://chat.flipkart.com
https://console.cloud.flipkart.com
https://checkout.cloud.flipkart.com
https://delivery.nct.flipkart.com
https://edigateway-uat.api.flipkart.com
https://delivery.ncb.flipkart.com
```

Activate Windows
Go to Settings to activate Windows.

c. IP Discovery

Tool: nslookup: [nslookup Results.txt](#)

Code: since we have a file with subdomains, to find IP addresses using “nslookup” we need to make a loop until all the IPs of all the subdomains are found.

```
while read sub; do
    echo "Looking up: $sub" >> ips.txt
    nslookup "$sub" | awk '/^Name:/^Address:/' >> ips.txt
    echo "-----" >> ips.txt
done < subdomains.txt
```

Explanation:

While read sub; do - start of the loop

Echo “Looking up: \$sub”>>ips.txt - print message “Looking up: subdomain” into the file “ips.txt”

nslookup “\$sub” | awk ‘/^Name:/^Address:/' >> ips.txt - run the nslookup command

echo “-----” >> ips.txt - separate one subdomain details from another

done < subdomains_flipkart.txt - End the loop and continue until the lines in the livesub_results.txt

```
(kali@kali)-[~/Desktop/Sublist3r]
$ ./nslookup.sh
Looking up IP for: www.flipkart.com
Address: 192.168.0.1#53
Name: flipkart.com
Address: 163.53.76.86
Looking up IP for: ac.flipkart.com
Address: 192.168.0.1#53
Name: ac.flipkart.com
Address: 163.53.76.191
Looking up IP for: www.ac.flipkart.com
Address: 192.168.0.1#53
Looking up IP for: accounts.flipkart.com
Address: 192.168.0.1#53
Name: accounts.flipkart.com
Address: 163.53.76.86
Looking up IP for: www.accounts.flipkart.com
Address: 192.168.0.1#53
Looking up IP for: adfs.flipkart.com
Address: 192.168.0.1#53
Name: adfs.flipkart.com
Address: 115.114.191.195
Looking up IP for: www.adfs.flipkart.com
Address: 192.168.0.1#53
Looking up IP for: adp.flipkart.com
Address: 192.168.0.1#53
Name: adp.flipkart.com
Address: 103.243.32.24
Looking up IP for: www.adp.flipkart.com
Address: 192.168.0.1#53
Looking up IP for: ads.flipkart.com
Address: 192.168.0.1#53
Name: ads.flipkart.com
Address: 52.172.39.71
Looking up IP for: www.ads.flipkart.com
Address: 192.168.0.1#53
Looking up IP for: advertising.flipkart.com
Address: 192.168.0.1#53
Name: advertising.flipkart.com
Address: 103.243.32.111
Looking up IP for: www.advertising.flipkart.com
Address: 192.168.0.1#53
Looking up IP for: affiliate.flipkart.com
Address: 192.168.0.1#53
Name: affiliate.flipkart.com
Address: 103.243.32.94
```

IP list:

```
Looking up: www.flipkart.com
Address: 192.168.0.1#53
Name: flipkart.com
Address: 103.243.32.90
-----
```

```
Looking up: ac.flipkart.com
Address: 192.168.0.1#53
Name: ac.flipkart.com
Address: 163.53.76.191
-----
```

Looking up: www.ac.flipkart.com

Address: 192.168.0.1#53

Looking up: accounts.flipkart.com

Address: 192.168.0.1#53

Name: accounts.flipkart.com

Address: 103.243.32.90

Looking up: www.accounts.flipkart.com

Address: 192.168.0.1#53

Looking up: adfs.flipkart.com

Address: 192.168.0.1#53

Name: adfs.flipkart.com

Address: 115.114.191.195

Looking up: www.adfs.flipkart.com

Address: 192.168.0.1#53

Looking up: adp.flipkart.com

Address: 192.168.0.1#53

Name: adp.flipkart.com

Address: 103.243.32.24

Looking up: www.adp.flipkart.com

Address: 192.168.0.1#53

Looking up: ads.flipkart.com

Address: 192.168.0.1#53

Name: ads.flipkart.com

Address: 52.172.39.71

Looking up: www.ads.flipkart.com

Address: 192.168.0.1#53

Looking up: advertising.flipkart.com

Address: 192.168.0.1#53

Name: advertising.flipkart.com

Address: 103.243.32.111

d. Open Ports

Tool: nmap: [nmap_Result.txt](#)

Code: nmap -sV -A -v -O flipkart.com -oN nmap_results.txt

Explanation:

nmap - start the tool
 -sV - Service and version detection
 -A - OS detection, version detection, script scanning
 -v - increase verbosity level
 -O - Os detection
 - flipkart.com - target website
 -oN nmap_results.txt - result in an output text file

```
(kali㉿kali)-[~/Desktop/Sublist3r/flipkart]
$ nmap -sV -A -v -O flipkart.com -oN nmap_result.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-22 14:51 +
0530
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:51
Completed NSE at 14:51, 0.00s elapsed
Initiating NSE at 14:51
Completed NSE at 14:51, 0.00s elapsed
Initiating NSE at 14:51
Completed NSE at 14:51, 0.00s elapsed
Initiating Ping Scan at 14:51
Scanning flipkart.com (163.53.76.86) [4 ports]
Completed Ping Scan at 14:51, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:51
Completed Parallel DNS resolution of 1 host. at 14:51, 6.57s
elapsed
Initiating SYN Stealth Scan at 14:51
Scanning flipkart.com (163.53.76.86) [1000 ports]
Discovered open port 25/tcp on 163.53.76.86
Discovered open port 80/tcp on 163.53.76.86
Discovered open port 443/tcp on 163.53.76.86
Completed SYN Stealth Scan at 14:52, 7.68s elapsed (1000 tota
l ports)
Initiating Service scan at 14:52
Scanning 3 services on flipkart.com (163.53.76.86)
Completed Service scan at 14:52, 5.00s elapsed (3 services on
1 host)
Initiating OS detection (try #1) against flipkart.com (163.53
.76.86)
Retrying OS detection (try #2) against flipkart.com (163.53.7
6.86)
Initiating Traceroute at 14:52
Completed Traceroute at 14:52, 0.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 14:52
Completed Parallel DNS resolution of 2 hosts. at 14:52, 6.54s elapsed
NSE: Script scanning 163.53.76.86.
Initiating NSE at 14:52
Completed NSE at 14:52, 30.08s elapsed
Initiating NSE at 14:52
Completed NSE at 14:53, 31.12s elapsed
Initiating NSE at 14:53
Completed NSE at 14:53, 0.00s elapsed
Nmap scan report for flipkart.com (163.53.76.86)
Host is up (0.0030s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE  VERSION
25/tcp    open  tcpwrapped
|_smtp-comands: Couldn't establish connection on port 25
80/tcp    open  tcpwrapped
```

e. Used Technologies

Tool: whatweb - [Whatweb Results.txt](#)

Code: whatweb -v flipkart.com --o whatweb_result.txt

Explanation:

whatweb - start whatweb tool

-v - verbose

flipkart.com - target website

--o whatweb_result.txt - file with the output

```
(kali㉿kali)~[~/Desktop/Sublist3r/flipkart]
$ whatweb -v flipkart.com --o whatweb_result.txt
WhatWeb report for http://flipkart.com
Status      : 301 Moved Permanently
Title       : 301 Moved Permanently
IP          : 103.243.32.90
Country     : INDIA, IN

Summary     : HTTPServer[nginx], nginx, RedirectLocation[https://www.flipkart.com/], UncommonHeaders[accept-ch]

Detected Plugins:
[ HTTPServer ]
  HTTP server header string. This plugin also attempts to identify the operating system from the server header.
  String      : nginx (from server string)

[ RedirectLocation ]
  HTTP Server string location. used with http-status 301 and 302
  String      : https://www.flipkart.com/ (from location)

[ UncommonHeaders ]
  Uncommon HTTP server headers. The blacklist includes all the standard headers and many non standard but common ones. Interesting but fairly common headers should have their own plugins, eg. x-powered-by, server and x-aspnet-version. Info about headers can be found at www.http-stats.com
  String      : accept-ch (from headers)

[ nginx ]
  Nginx (Engine-X) is a free, open-source, high-performance HTTP server and reverse proxy, as well as an IMAP/POP3 proxy server.
  Website     : http://nginx.net/

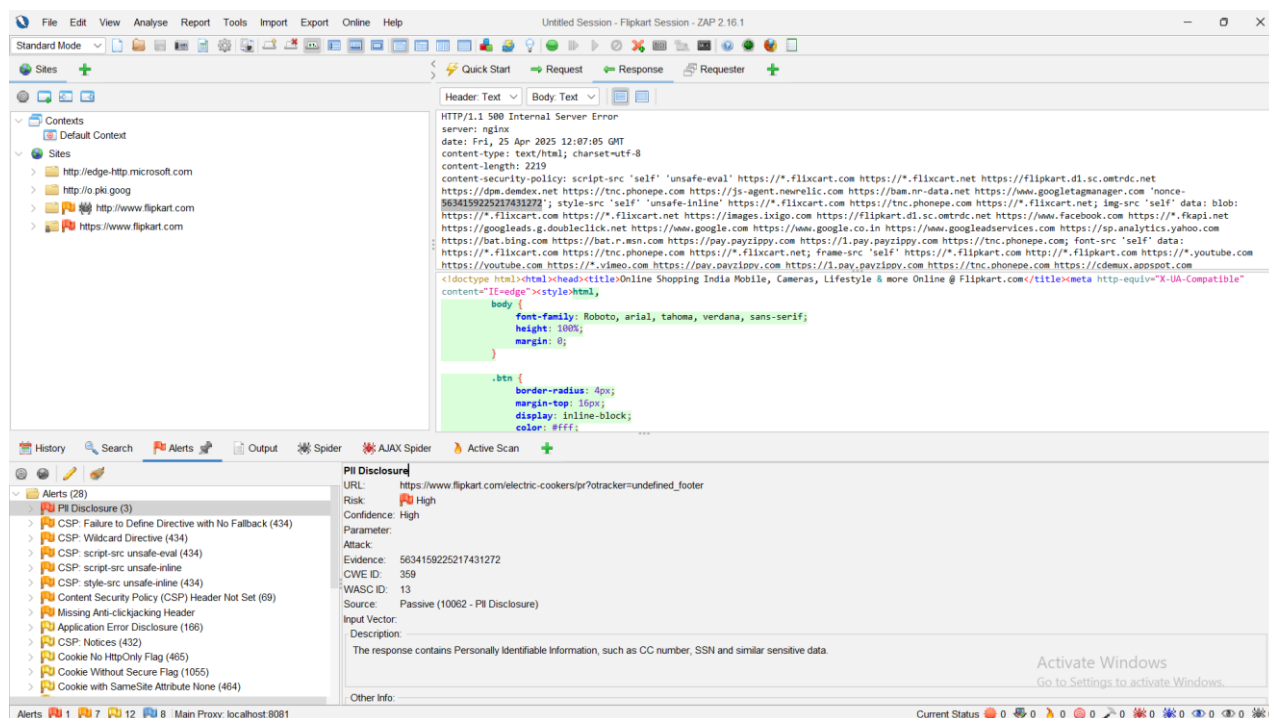
HTTP Headers:
HTTP/1.1 301 Moved Permanently
server: nginx
date: Tue, 22 Apr 2025 09:44:58 GMT
content-type: text/html
content-length: 162
location: https://www.flipkart.com/
accept-ch: Sec-CH-UA,Sec-CH-UA-Arch,Sec-CH-UA-Full-Version,Sec-CH-UA-Full-Version-List,Sec-CH-UA-Model,Sec-CH-UA-Platform,Sec-CH-UA-Platform-Version
connection: close
```

3. Step 02: Scanning and vulnerability identification

a. Identify Potential Vulnerabilities

Tool : OWASP ZAP

Vulnerability : Personally Identifiable Information Disclosure



PII Disclosure:

URL: https://www.flipkart.com/electric-cookers/pr?otracker=undefined_footer

Risk: High

Confidential: High

Parameter:

Attack:

Evidence: 5634159225217431272

CWE ID: 359

WASC ID: 13

Source: Passive (10062 - PII Disclosure)

Input Vector:

- **Description:** The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.
- **Other Info:**
 - Credit Card Type detected: Maestro
 - Bank Identification Number: 563415
 - Brand: MAESTRO
 - Category:
 - Issuer:
- **Solution:** Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.
- **Reference:**
- **Alert Tags:**
 - CWE 359: <https://cwe.mitre.org/data/definitions/359.html>
 - OWASP_2021_A04: https://owasp.org/Top10/A04_2021-Insecure_Design/
 - OWASP_2017_A03: https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html

b. Personally Identifiable Information Disclosure

PII is unauthorized or unintentional exposure of sensitive data that can be used to identify an individual. This includes, but is not limited to, full names, email addresses, phone numbers, home addresses, Social Security numbers, financial information, and login credentials. PII disclosure can lead to identity theft, privacy violations, and legal consequences for both individuals and organizations.

Cause of PII in website:

- Insecure data storage or transmission (e.g., using HTTP instead of HTTPS)
- Misconfigured servers or APIs
- Inadequate access controls or broken authentication mechanisms
- Insufficient data encryption
- Logging sensitive data in server logs or client-side scripts
- Vulnerabilities such as Cross-Site Scripting (XSS), SQL Injection, or insecure file uploads

Propositions to Mitigation or Fix:

- Data Minimization
- Secure Data Transmission
- Access Control and Authentication
- Data Encryption
- Sanitize and Validate Inputs
- Secure Logging Practices
- Regular Security Assessments

[illegible]

```

HTTP/1.1 500 Internal Server Error
server: nginx
date: Fri, 25 Apr 2025 12:07:05 GMT
content-type: text/html; charset=utf-8
content-length: 2219
content-security-policy: script-src 'self' 'unsafe-eval' https://*.flipkart.com https://*.flipkart.net https://flipkart.d1.sc.omtrdc.net https://dpm.demdex.net https://tnc.phonepe.com https://js-agent.newrelic.com https://bam.nr-data.net https://www.googletagmanager.com 'nonce-5634159225217431272'; style-src 'self' 'unsafe-inline' https://*.flipkart.com https://tnc.phonepe.com https://*.flipkart.net; img-src 'self' data: blob: https://*.flipkart.com https://*.flipkart.net https://images.ixigo.com https://flipkart.d1.sc.omtrdc.net https://www.facebook.com https://*.fkapi.net https://googleads.g.doubleclick.net https://www.google.com https://www.google.co.in https://www.googleadservices.com https://sp.analytics.yahoo.com https://bat.bing.com https://bat.r.msn.com https://pay.payzippy.com https://1.pay.payzippy.com https://tnc.phonepe.com; font-src 'self' data: https://*.flipkart.com https://tnc.phonepe.com https://*.flipkart.net; frame-src 'self' https://*.flipkart.com http://*.flipkart.com https://*.youtube.com https://*.vimeo.com https://pay.payzippy.com https://1.pay.payzippy.com https://tnc.phonepe.com https://cdemux.appspot.com https://static-assets-web.flipkart.com/ https://raven-gam.shipsy.io 'nonce-5634159225217431272'; worker-src 'self' https://*.flipkart.com blob; child-src 'self' https://*.flipkart.com 'nonce-5634159225217431272'; connect-src 'self' *; object-src 'none'; base-uri 'self'; media-src https://static-assets-web.flipkart.com/; report-uri https://csp-flkt.domdog.io/report-uri/flipkart.com/3/1-1
content-security-policy-report-only: form-action 'self'; manifest-src 'self'; report-uri https://csp-flkt.domdog.io/report-uri/flipkart.com/3/2-1
x-xss-protection: 1; mode=block
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
Set-Cookie: T=1174558264536700142025104439671760570949522960866316704562333086250; Max-Age=31536000; Domain=flipkart.com; Path=/; Expires=Sat, 25 Apr 2026 12:07:05 GMT;

"Font-size: 20px; margin-top: 30px; font-weight: 600;">Just a quick repair needed</div><div style="font-size: 17px; margin-top: 10px; color: #666666;">Hang on, we're doing everything we can to fix this</div><div><button class="btn disable_btn" id="timer_text">Retry in 3 sec</button> <button class="btn" id="retry_btn" type="button">Try now</button></div><script nonce="5634159225217431272">let seconds = 3;
const timerText = document.getElementById("timer_text")
const retryBtn = document.getElementById("retry_btn")
// Update the count down every 1 second
var timerId = setInterval(function () {
    timerText.innerHTML = `Retry in ${seconds--} sec`;
    if (seconds < 0) {
        clearInterval(timerId);
        timerText.remove()
        retryBtn.style.display = "inline"
    }
}, 1000);
retryBtn.addEventListener('click', function () { window.location.reload() })</script></body></html>

```

5. Step 04: Mitigation / Fix

Immediate mitigation actions:

1. Block access to the leaky Endpoints – Temporarily disable the affected URL or API endpoints to prevent further exposure.
2. Mask or Remove Sensitive data – In this case replace credit card numbers with “*” in responses.
3. Sanitize Logs and Debug Data – Ensure no other pages are leaking similar data.

Secure the code by,

1. Tokenizing the credit card numbers.
2. Scan code for PII
3. Test payment flows

Long term Security:

1. Automate checks – Use tools like OWASP ZAP or Burp Suite to scan for leaks weekly.
2. Encrypt Everything – Ensure card data is encrypted in databases and during transmission (Use HTTPS)
3. Train the Team / Employees - Educate developers on secure coding.