02
Reconnaissance Practice

Summary

Performed passive and active reconnaissance on vulnweb.com and flipkart. Focused on WHOIS, reverse-DNS and Shodan checks for asset discovery. WHOIS not applicable for private IPs; reverse-DNS returned none. Shodan queries yielded no public records (lab IP). Maltego mapped assets; results exported for documentation and verify externally when authorised.

Checklist (completed / recommended)

1. Check WHOIS (not applicable — private IP).
2. Shodan.io – Provide ip address of domain.
3. Wappalyzer - Capture frameworks, server, CMS, JS lib.
4. Subfinder – To identify the subdomains.
5. Maltego graph — Nodes added and saved.

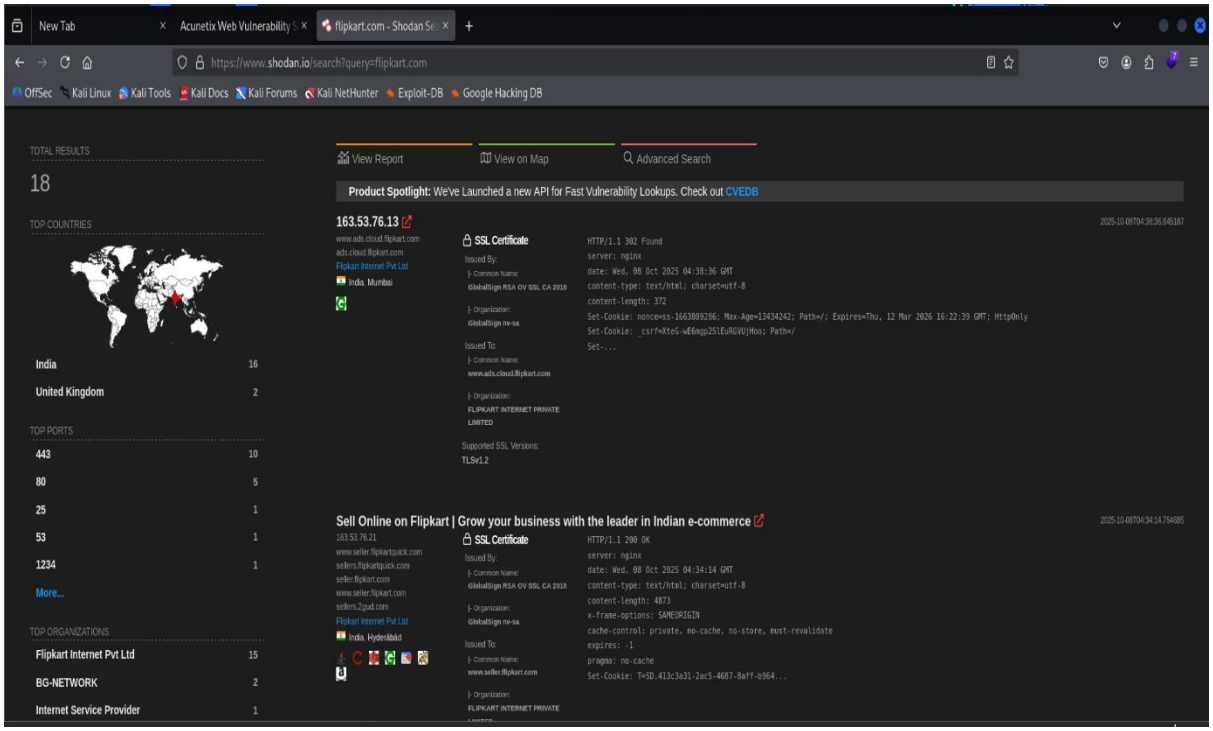
Result

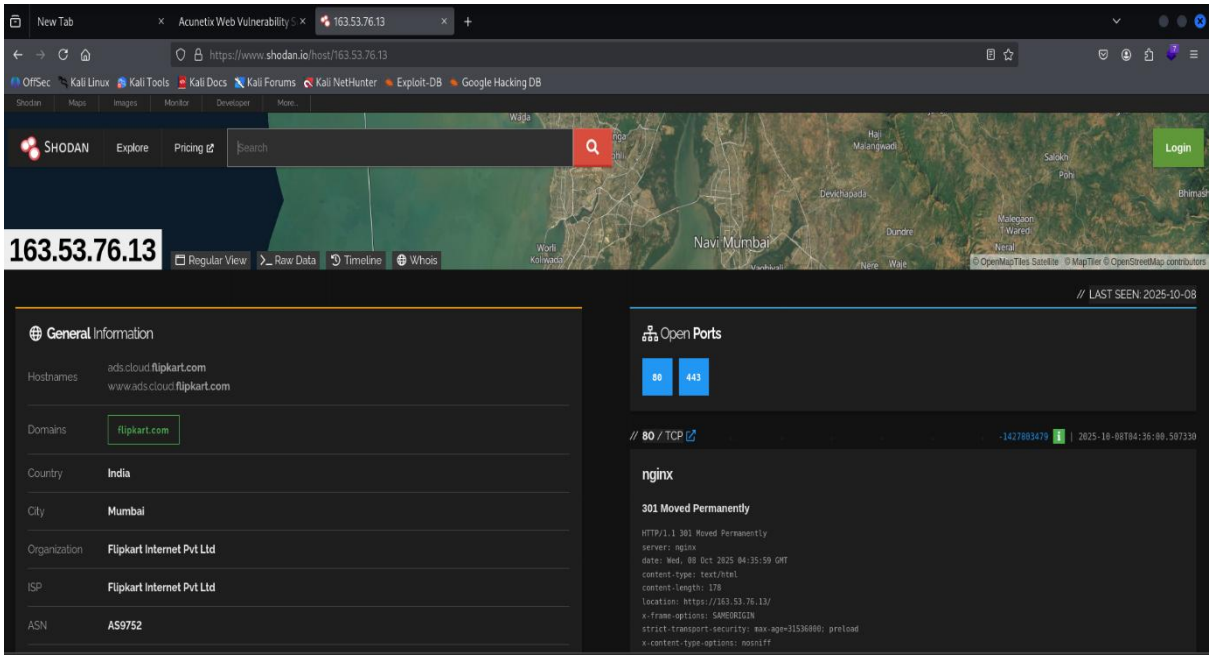
WHOIS:

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ whois vulnweb.com
   Domain Name: VULNWEB.COM
   Registry Domain ID: 1602006391_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.eurodns.com
   Registrar URL: http://www.EuroDNS.com
   Updated Date: 2025-05-20T08:14:02Z
   Creation Date: 2010-06-14T07:50:29Z
   Registry Expiry Date: 2026-06-14T07:50:29Z
   Registrar: EuroDNS S.A.
   Registrar IANA ID: 1052
   Registrar Abuse Contact Email: legalservices@eurodns.com
   Registrar Abuse Contact Phone: +352.27220150
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransf
erProhibited
   Name Server: NS1.EURODNS.COM
   Name Server: NS2.EURODNS.COM
   Name Server: NS3.EURODNS.COM
   Name Server: NS4.EURODNS.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wi
cf/
>>> Last update of whois database: 2025-10-08T15:03:21Z <<<

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

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiratio
n
```

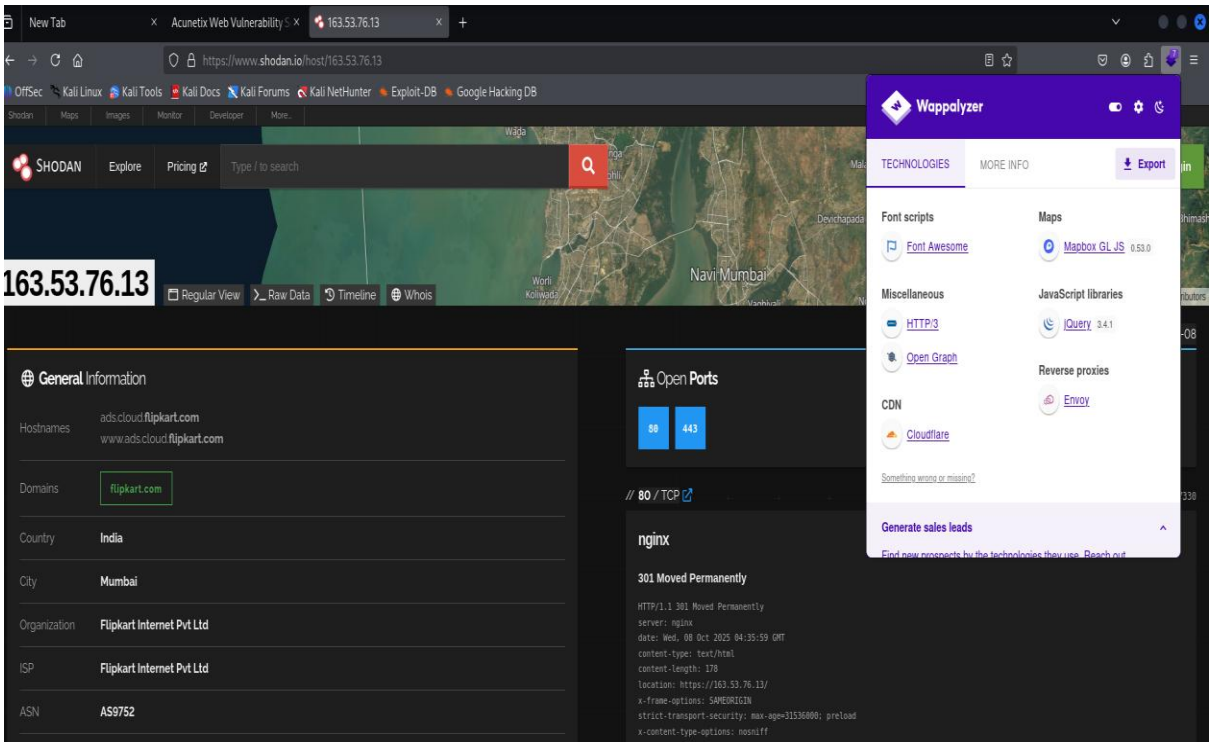
```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: vulnweb.com
Registry Domain ID: D22051771-COM
Registrar WHOIS Server: whois.eurodns.com
Registrar URL: http://www.eurodns.com
Updated Date: 2025-05-21T15:16:31Z
Creation Date: 2010-06-14T00:00:00Z
Registrar Registration Expiration Date: 2026-06-13T00:00:00Z
Registrar: Eurodns S.A.
Registrar IANA ID: 1052
Registrar Abuse Contact Email: legalservices@eurodns.com
Registrar Abuse Contact Phone: +352.27220150
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransf
erProhibited
Registry Registrant ID:
Registrant Name: Antevski Gjorgji
Registrant Organization: Acunetix Limited
Registrant Street: Mirabilis Building Level 2, Triq L-Intornjatur
Registrant City: Mriehel
Registrant State/Province:
Registrant Postal Code: CBD 3050
Registrant Country: MT
Registrant Phone: +356.79204709
Registrant Fax:
Registrant Email: administrator@invicti.com
Registry Admin ID:
Admin Name: Antevski Gjorgji
Admin Organization: Acunetix Limited
Admin Street: Mirabilis Building Level 2, Triq L-Intornjatur
Admin City: Mriehel
```

Shodan.io:




New Tab
Acunetix Web Vulnerability
163.53.76.13
https://www.shodan.io/host/163.53.76.13
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
SHODAN Explore Pricing Search Login
163.53.76.13
Regular View Raw Data Timeline Whois
Navi Mumbai
// LAST SEEN: 2025-10-08
General Information
Hostnames ads.cloud.flipkart.com www.ads.cloud.flipkart.com
Domains flipkart.com
Country India
City Mumbai
Organization Flipkart Internet Pvt Ltd
ISP Flipkart Internet Pvt Ltd
ASN AS9752
Open Ports
80 443
// 80 / TCP
nginx
301 Moved Permanently
HTTP/1.1 301 Moved Permanently
server: nginx
date: Wed, 08 Oct 2025 04:35:59 GMT
content-type: text/html
content-length: 178
location: https://163.53.76.13/
x-frame-options: SAMEORIGIN
strict-transport-security: max-age=31536000; preload
x-content-type-options: nosniff

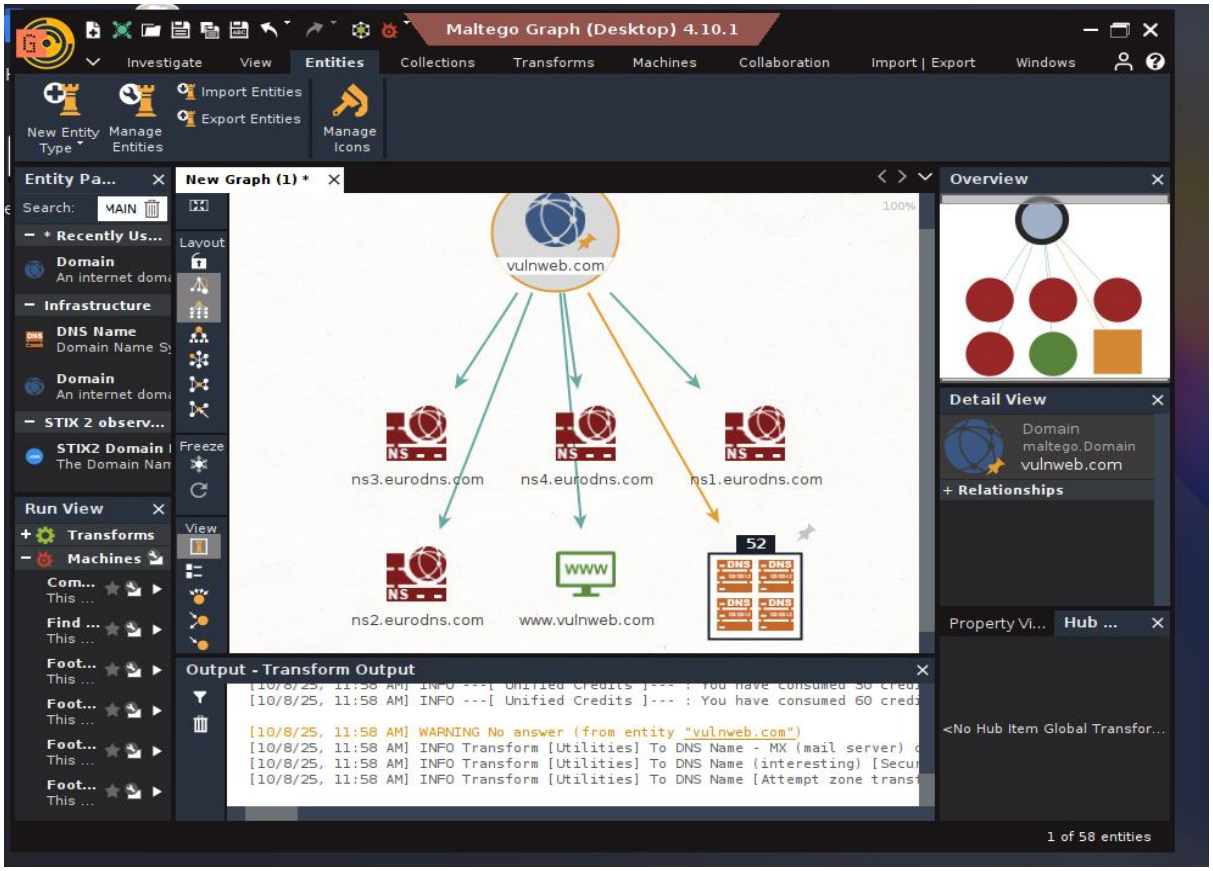
Wappalyzer:

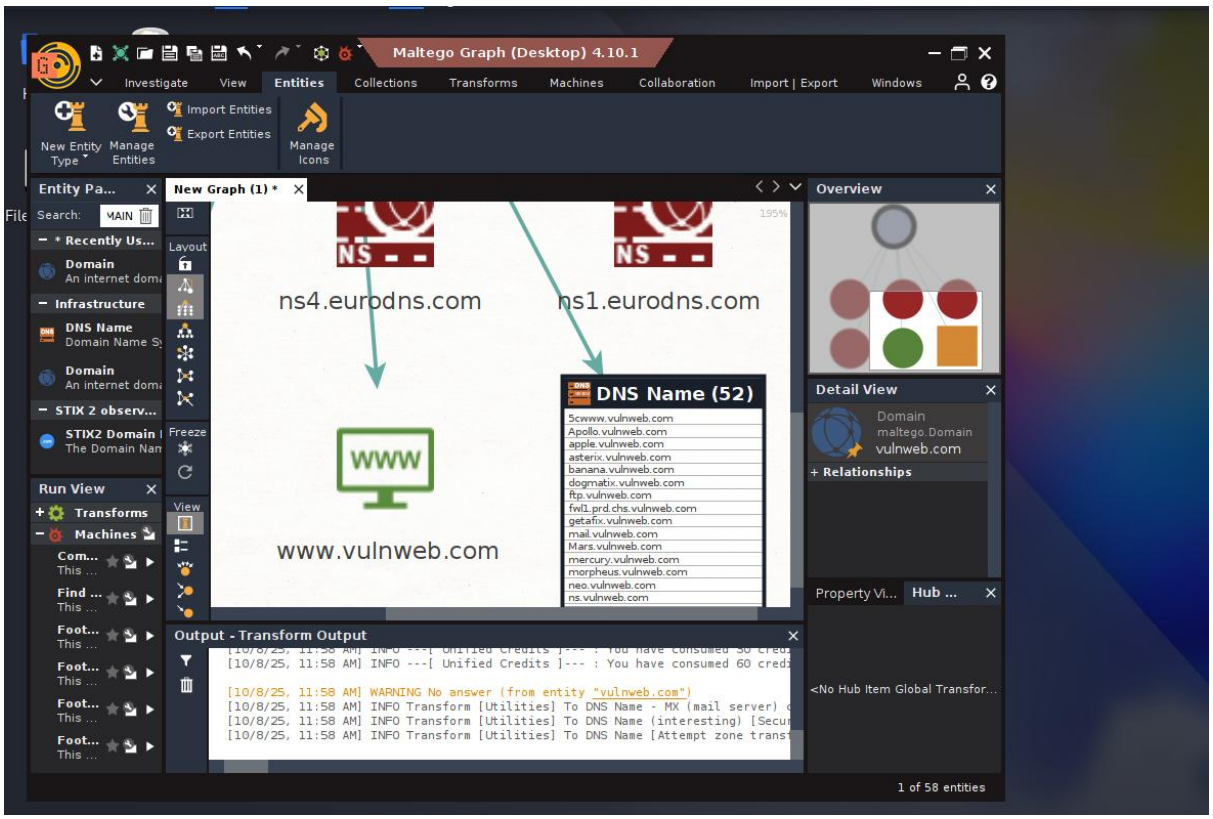

New Tab
Acunetix Web Vulnerability
163.53.76.13
https://www.shodan.io/host/163.53.76.13
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
SHODAN Explore Pricing Type / to search
163.53.76.13
Regular View Raw Data Timeline Whois
Navi Mumbai
Wappalyzer
TECHNOLOGIES MORE INFO Export
Font scripts
Font Awesome
Maps
Mapbox GL JS 0.53.0
Miscellaneous
HTTP/3
Open Graph
JavaScript libraries
jQuery 3.4.1
Reverse proxies
Envoy
CDN
Cloudflare
Something wrong or missing?
Generate sales leads
General Information
Hostnames ads.cloud.flipkart.com www.ads.cloud.flipkart.com
Domains flipkart.com
Country India
City Mumbai
Organization Flipkart Internet Pvt Ltd
ISP Flipkart Internet Pvt Ltd
ASN AS9752
Open Ports
80 443
// 80 / TCP
nginx
301 Moved Permanently
HTTP/1.1 301 Moved Permanently
server: nginx
date: Wed, 08 Oct 2025 04:35:59 GMT
content-type: text/html
content-length: 178
location: https://163.53.76.13/
x-frame-options: SAMEORIGIN
strict-transport-security: max-age=31536000; preload
x-content-type-options: nosniff

Subfinder:

```
┌──(kali㉿kali)-[~]
└─$ subfinder -d vulnweb.com -o subfinderweb.txt

                     __     _____
   _____  __  __  __/ /_   / ___/ ____ _ ____
  / ___/ / / / / / / __/   \__ \ / __ `/ / __ \
 (__  ) / /_/ / / / /_    ___/ / / /_/ / / / / /
/____/ /_,_/ /_/ /_/\__/ /____/  \__,_/ /_/ /_/

                projectdiscovery.io

[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-conf
ig.yaml
[INF] Enumerating subdomains for vulnweb.com
testaps.vulnweb.com
tesphp.vulnweb.com
www.testasp.vulnweb.com
estphp.vulnweb.com
sieb-web1.testphp.vulnweb.com
testaspnet.vulnweb.com
testphp.vulnweb.com
restasp.vulnweb.com
test.php.vulnweb.com
www.test.php.vulnweb.com
www.vulnweb.com
rest.vulnweb.com
testasp.vulnweb.com
httptestaspnet.vulnweb.com
blogger.com.vulnweb.com
viruswall.vulnweb.com
```

Maltego graph:





Asset Mapping (table):

Timestamp	Tool	Finding
2025-8-10 10:00:00	whois	Exposed email and contact info of vulnweb.com
2025-8-10 10:15:00	whois	Server name of vulnweb.com is NS1.EURODNS.COM
2025-08-10 10:20:00	Shodan.io	Identify the ip address, server, of Flipkart
2025-08-10 10:20:00	Shodan.io	Open ports 80 ,443 tcp ip 163.53.76.13
2025-08-10 10:21:00	Wappalyzer	Identify the miscellaneous-HTTP/3, opengrap,javabased libraries are used in flipkart page.
2025-08-10 10:25:00	Subfinder	Find the subdomains of vulnweb.com
2025-08-10 10:30:00	Maltego	Find the server's name of vulnweb.com
2025-08-10 10:31:00	Maltego	Find the DNS Name of the vulnweb.com