



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.EUODNS.COM
Name Server: NS2.EUODNS.COM
Name Server: NS3.EUODNS.COM
Name Server: NS4.EUODNS.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: legal.services@eurodns.com
Registrar Abuse Contact Phone: +352.27220150
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

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

acunetix

Vulnerable test websites for Acunetix Web Vulnerability Scanner.

Name	URL	Technologies	Resources
Acunetix	http://www.acunetix.com	Apache, Python, Flask, CouchDB	Review Acunetix HTML5 scanner or learn more on the blog
Acunetix	http://test.vulnweb.com	Apache, PHP, MySQL	Review Acunetix PHP scanner or learn more on the blog
Acunetix	http://test.vulnweb.com	JS, ASP, Microsoft SQL Server	Review Acunetix SQL scanner or learn more on the blog
Acunetix	http://test.vulnweb.com	JS, ASP.NET, Microsoft SQL Server	Review Acunetix network scanner or learn more on the blog
Acunetix	http://test.vulnweb.com	Apache, PHP, MySQL	Review Acunetix scanner or learn more on the blog

Warning: This site hosts intentionally vulnerable web applications. You can use these applications to understand how programming and configuration errors lead to security breaches. We created the site to help you test Acunetix but you may also use it for manual penetration testing or for educational purposes. It will help you learn about vulnerabilities such as SQL Injection, Cross-site Scripting (XSS), Cross-site Request Forgery (CSRF), and many more.

Shodan.io:

New Tab x Acunetix Web Vulnerability x Flipkart.com - Shodan Se: x +

https://www.shodan.io/search?query=flipkart.com

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

TOTAL RESULTS: 18

TOP COUNTRIES

India 18
United Kingdom 2

TOP PORTS

443 10
80 5
25 1
53 1
1234 1

More...

TOP ORGANIZATIONS

Flipkart Internet Pvt Ltd 15
BG-NETWORK 2
Internet Service Provider 1

Product Spotlight: We've launched a new API for Fast Vulnerability Lookups. Check out CVEDB

163.53.76.13

www.ads.cloud.flipkart.com
ads.cloud.flipkart.com
Flipkart Internet Pvt Ltd
India, Mumbai

SSL Certificate

Issued By: GlobalSign RSA OV SSL CA 2018
Common Name: www.ads.cloud.flipkart.com
Organization: Flipkart Internet Private Limited
Issued To: www.ads.cloud.flipkart.com

HTTP/1.1 302 Found
server: nginx
date: Wed, 08 Oct 2025 04:38:36 GMT
content-type: text/html; charset=utf-8
content-length: 372
Set-Cookie: nonce=166389226; Max-Age=1343424; Path=/; Expires=Thu, 12 Mar 2026 16:22:39 GMT; HttpOnly
Set-Cookie: _csrfa2e6-v4Eagp2SLEuG0WjR0u; Path=/
Set-...

Sell Online on Flipkart | Grow your business with the leader in Indian e-commerce

163.53.76.11

www.seller.flipkart.com
seller.flipkart.com
seller.flipkart.com
www.seller.flipkart.com
Flipkart Internet Pvt Ltd
India, Hyderabad

SSL Certificate

Issued By: GlobalSign RSA OV SSL CA 2018
Common Name: www.seller.flipkart.com
Organization: Flipkart Internet Private Limited
Issued To: www.seller.flipkart.com

HTTP/1.1 200 OK
server: nginx
date: Wed, 08 Oct 2025 04:34:14 GMT
content-type: text/html; charset=utf-8
content-length: 4873
x-frame-options: SAMEORIGIN
cache-control: private, no-cache, no-store, must-revalidate
expires: -1
pragmas: no-cache
Set-Cookie: T=ID_413c3a31-2ac5-4687-baff-b964...



The screenshot shows a web browser window with the Shodan search engine interface. The search results for the IP address 163.53.76.13 are displayed. The main section shows a map of Navi Mumbai, India, with a red pin indicating the location. Below the map, the IP address 163.53.76.13 is highlighted. The search results are categorized into 'General Information' and 'Open Ports'.

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 (TCP)
- 443 (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: 179

location: https://163.53.76.13/

x-frame-options: SAMEORIGIN

strict-transport-security: max-age=31536000; preload

x-content-type-options: nosniff

Wappalyzer:

The screenshot shows the Wappalyzer application interface. The main section displays the search results for the IP address 163.53.76.13. The search results are categorized into 'General Information' and 'Open Ports'.

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 (TCP)
- 443 (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: 179

location: https://163.53.76.13/

x-frame-options: SAMEORIGIN

strict-transport-security: max-age=31536000; preload

x-content-type-options: nosniff

Wappalyzer Technologies

- 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

Generate sales leads

Find new prospects by the technologies they use. Search now



Subfinder:

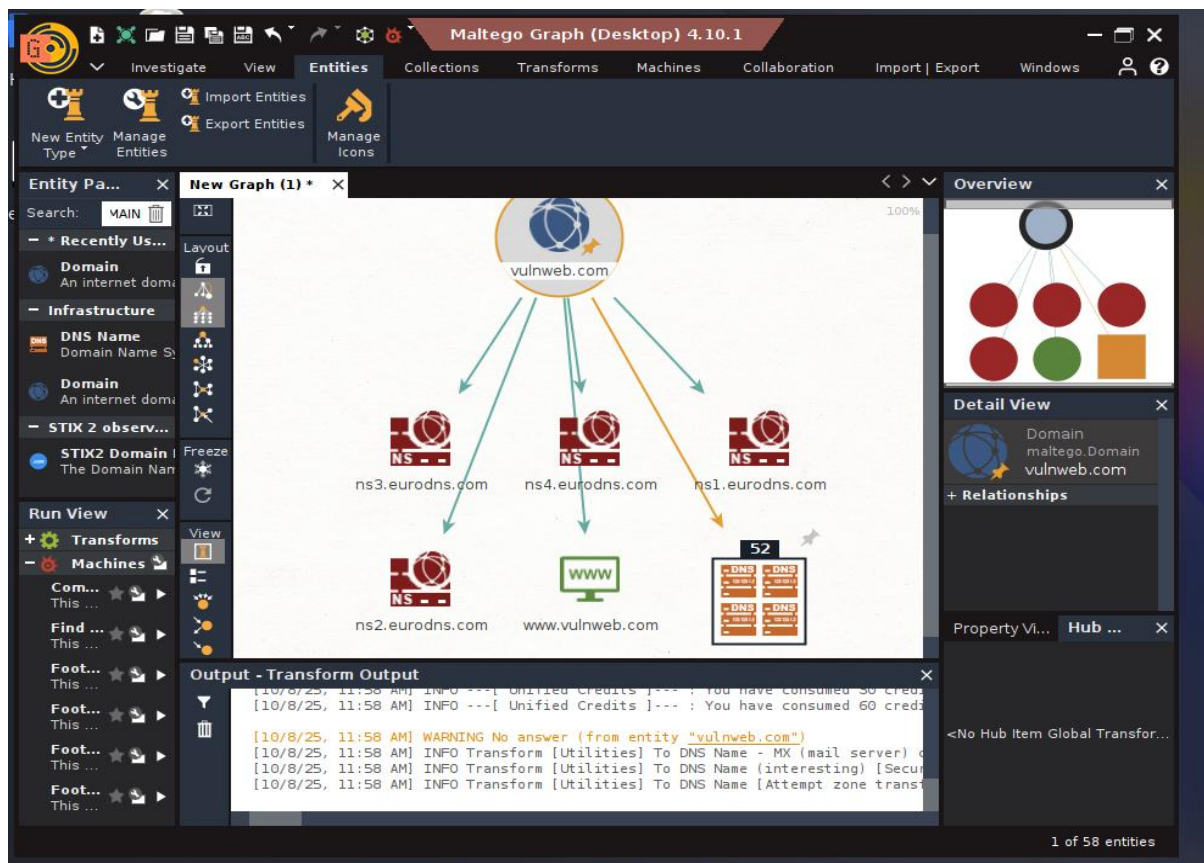
```
(kali㉿kali)-[~]
$ subfinder -d vulnweb.com -o subfinderweb.txt

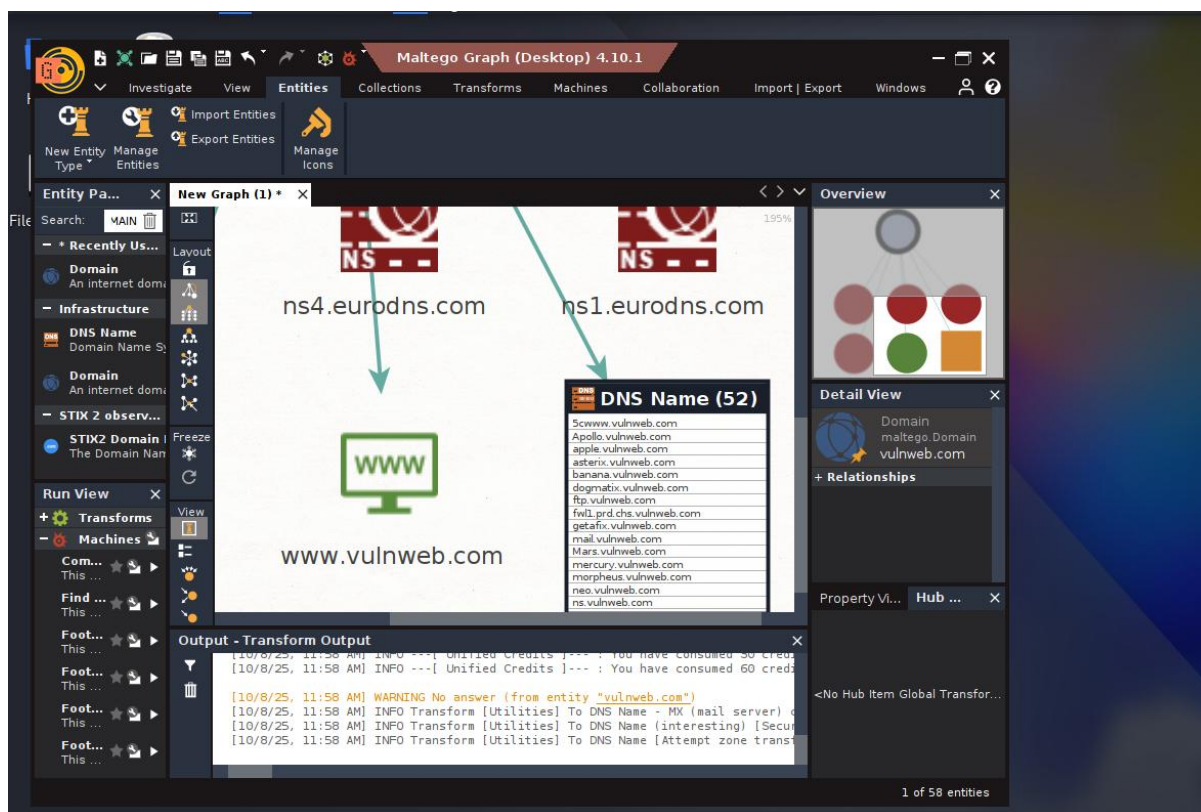
subfinder

projectdiscovery.io

[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for vulnweb.com
testaps.vulnweb.com
testphp.vulnweb.com
www.testasp.vulnweb.com
testphp.vulnweb.com
sieb-web1.testphp.vulnweb.com
testaspnet.vulnweb.com
testphp.vulnweb.com
testasp.vulnweb.com
test.php.vulnweb.com
www.test.php.vulnweb.com
www.vulnweb.com
rest.vulnweb.com
testasp.vulnweb.com
httpstestaspnet.vulnweb.com
plogger.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