NAME: PRERNA SUNIL JADHAV

SAP ID: 60004220127

BATCH: C2-2

BRANCH: COMPUTER ENGINEERING

COURSE: INFORMATION SECURITY LABORATORY

COURSE CODE: DJ19CEL603

EXPERIMENT 09

AIM: Perform Information Gathering / Footprinting

THEORY: Information gathering also known as reconnaissance, is a crucial initial phase in cybersecurity, it involves collecting as much relevant data as possible about a target system or network to identify potential vulnerabilities and attack vectors

1) Passive Information Gathering: This involves gathering information without directly interacting with the target. which includes. Searching online public sources such as social media.

2) Active Information Gathering: It involves more direct interaction with the target system techniques may include port scanning network mapping & service enumeration. etc

3) Footprinting: This is the process of collecting information about the target organization networks, system and infrastructure involves

Sundaram

identifying IP addresses, domain names, network blocks etc

4) Social Engineering: This technique involves manipulating individuals within the target organization to divulge confidential information or perform actions that compromise security.

CONCLUSION: Thus we have learnt how important information gathering is in cybersecurity & how to perform it using various tools.

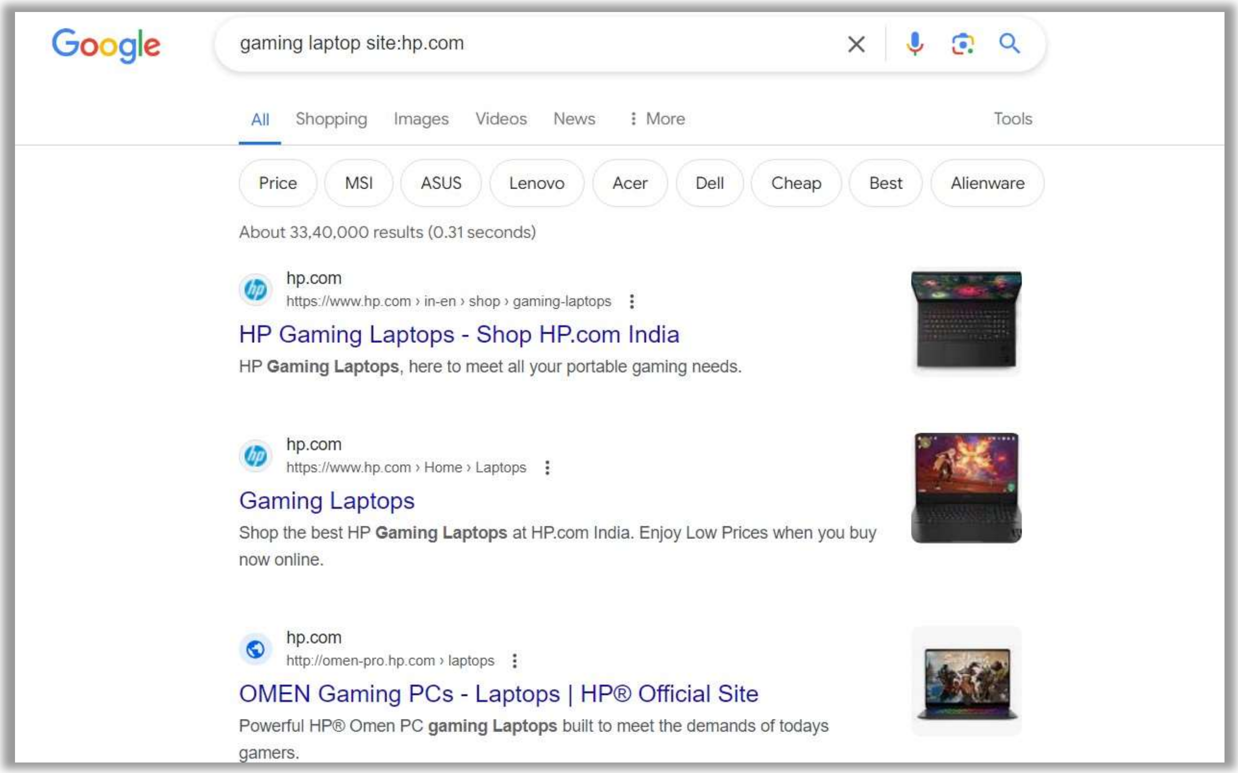
Shri Vile Parle Kelavani Mandal's
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING
(Autonomous College Affiliated to the University of Mumbai)
NAAC Accredited with "A" Grade (CGPA : 3.18)

Academic Year: 2022-2023

Name:	Prerna Sunil Jadhav
Sap Id:	60004220127
Class:	T. Y. B. Tech (Computer Engineering)
Course:	Information Security Laboratory
Course Code:	DJ19CEL603
Experiment No.:	09

AIM: Perform Information Gathering/ Footprinting.

1. **GOOGLE DORK:**



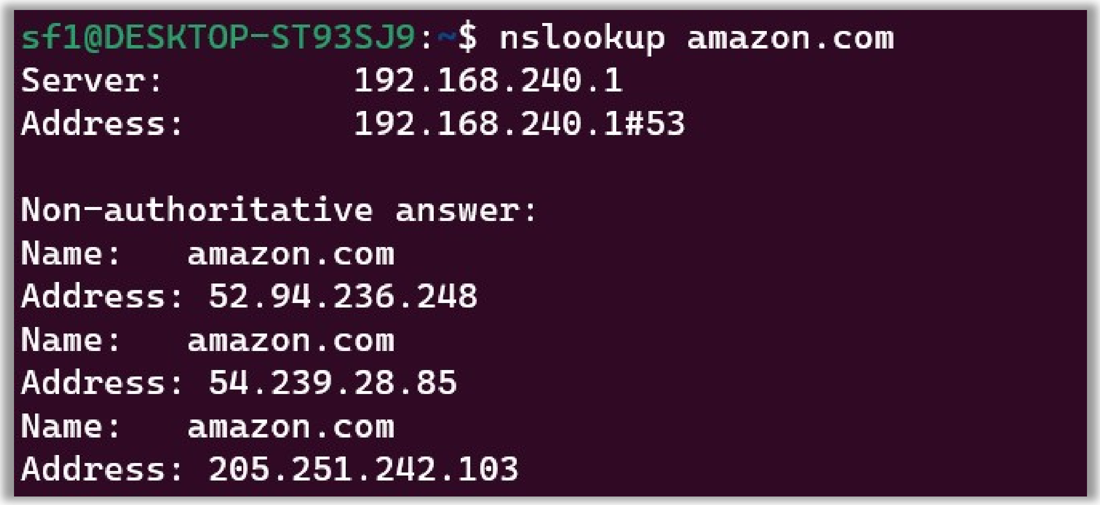
About 33,40,000 results (0.31 seconds)

hp.com
https://www.hp.com › in-en › shop › gaming-laptops
HP Gaming Laptops - Shop HP.com India
HP **Gaming Laptops**, here to meet all your portable gaming needs.

hp.com
https://www.hp.com › Home › Laptops
Gaming Laptops
Shop the best HP **Gaming Laptops** at HP.com India. Enjoy Low Prices when you buy now online.

hp.com
http://omen-pro.hp.com › laptops
OMEN Gaming PCs - Laptops | HP® Official Site
Powerful HP® Omen PC **gaming Laptops** built to meet the demands of todays gamers.

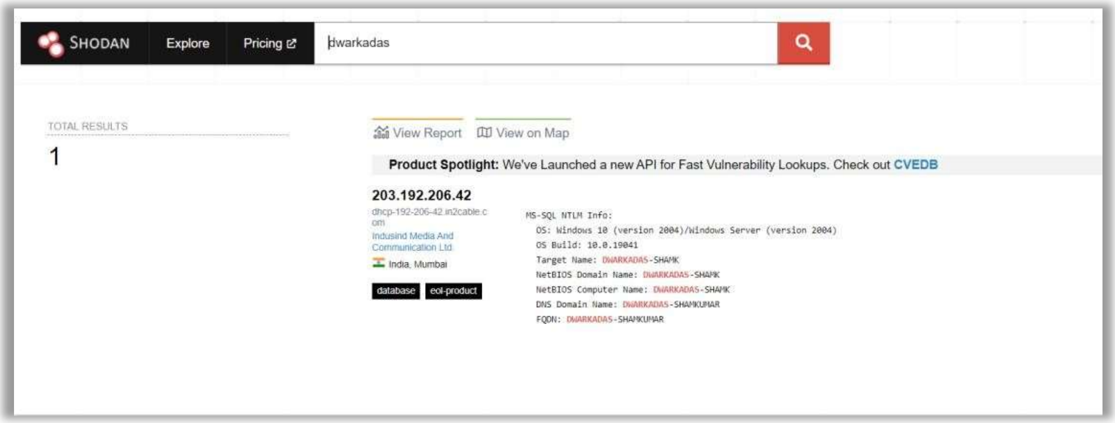
2. **NSLOOKUP**



```
sf1@DESKTOP-ST93SJ9:~$ nslookup amazon.com
Server:         192.168.240.1
Address:        192.168.240.1#53

Non-authoritative answer:
Name:   amazon.com
Address: 52.94.236.248
Name:   amazon.com
Address: 54.239.28.85
Name:   amazon.com
Address: 205.251.242.103
```

3. SHODAN



dwarkadas

TOTAL RESULTS

1

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

203.192.206.42

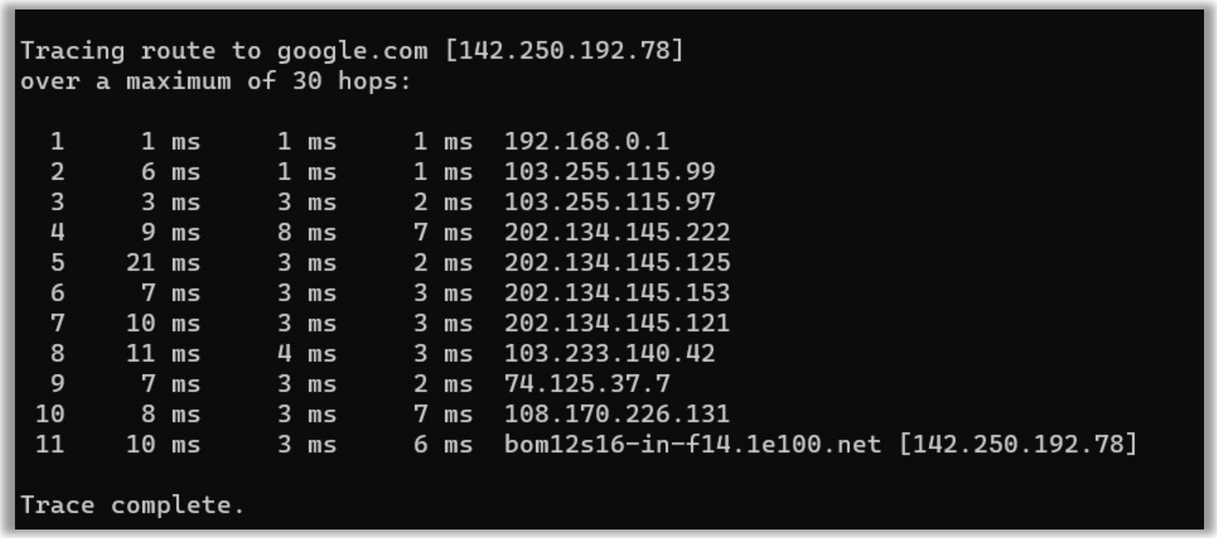
dhcp-192-206-42.in2cable.com

Indusind Media And Communication Ltd.

India, Mumbai

```
MS-SQL NTLM Info:
  OS: Windows 10 (version 2004)/Windows Server (version 2004)
  OS Build: 10.0.19041
  Target Name: DWARKADAS-SHAMK
  NetBIOS Domain Name: DWARKADAS-SHAMK
  NetBIOS Computer Name: DWARKADAS-SHAMK
  DNS Domain Name: DWARKADAS-SHAMKUMAR
  FQDN: DWARKADAS-SHAMKUMAR
```

4. TRACERT

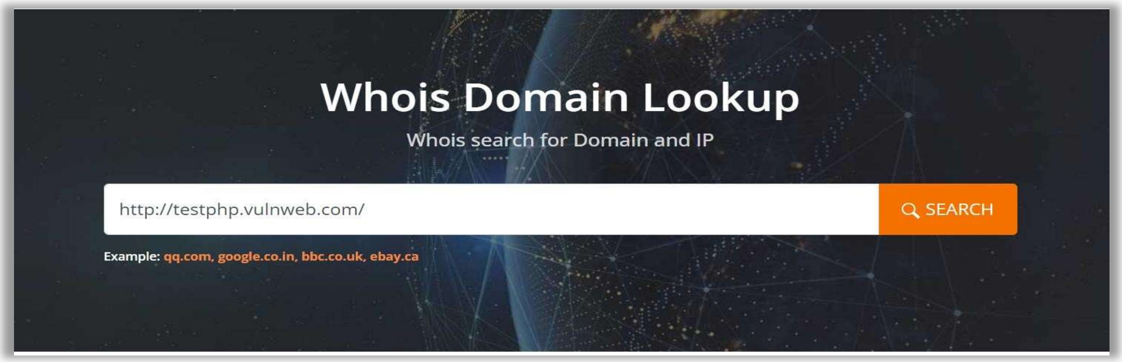


```
Tracing route to google.com [142.250.192.78]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.0.1
  2     6 ms     1 ms     1 ms  103.255.115.99
  3     3 ms     3 ms     2 ms  103.255.115.97
  4     9 ms     8 ms     7 ms  202.134.145.222
  5    21 ms     3 ms     2 ms  202.134.145.125
  6     7 ms     3 ms     3 ms  202.134.145.153
  7    10 ms     3 ms     3 ms  202.134.145.121
  8    11 ms     4 ms     3 ms  103.233.140.42
  9     7 ms     3 ms     2 ms  74.125.37.7
 10     8 ms     3 ms     7 ms  108.170.226.131
 11    10 ms     3 ms     6 ms  bom12s16-in-f14.1e100.net [142.250.192.78]

Trace complete.
```

5. WHOIS

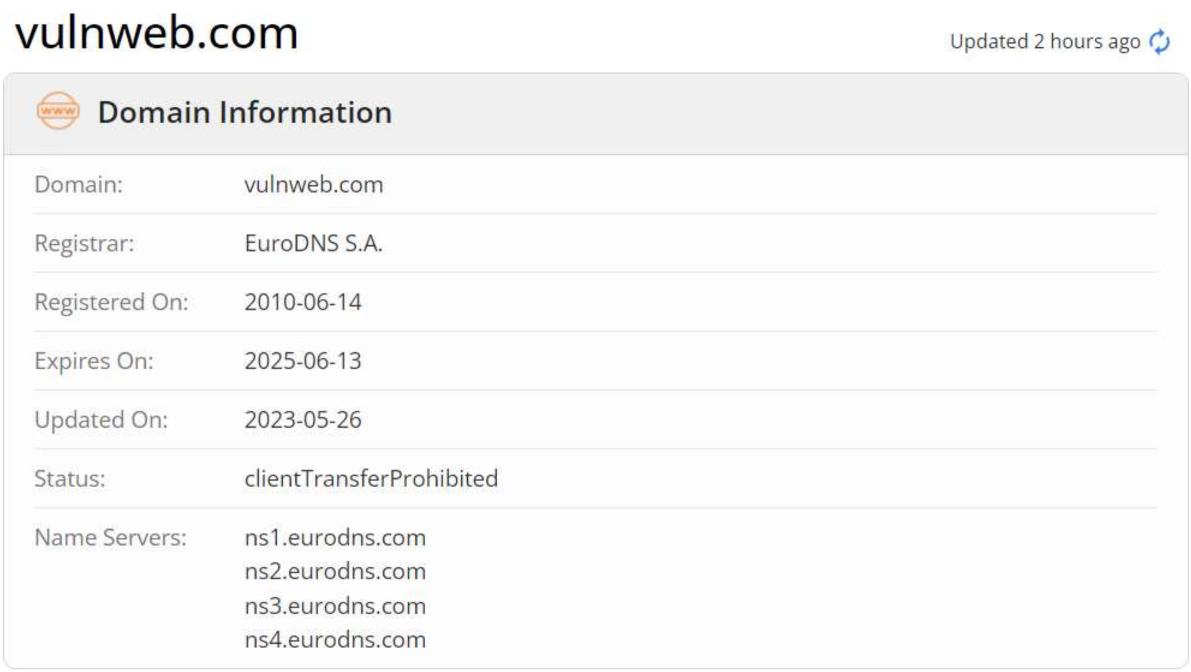


Whois Domain Lookup

Whois search for Domain and IP

http://testphp.vulnweb.com/

Example: qq.com, google.co.in, bbc.co.uk, ebay.ca

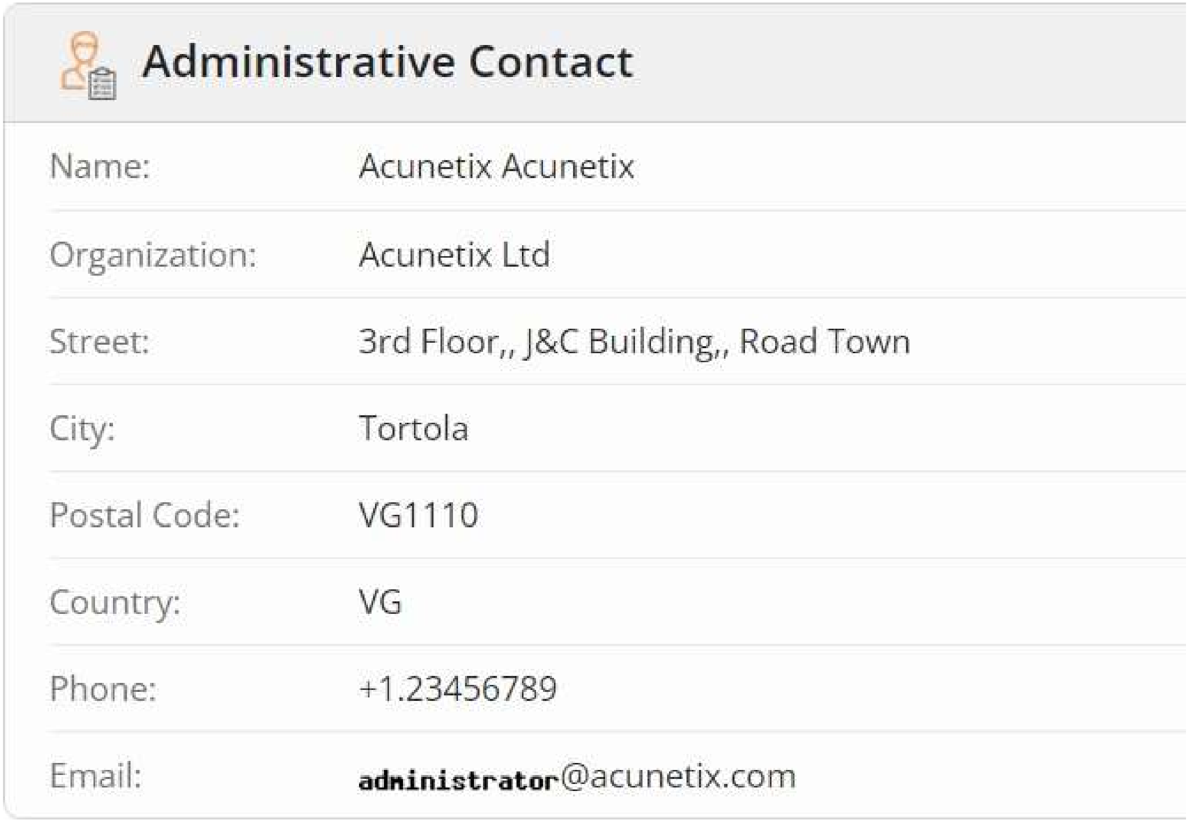


vulnweb.com

Updated 2 hours ago

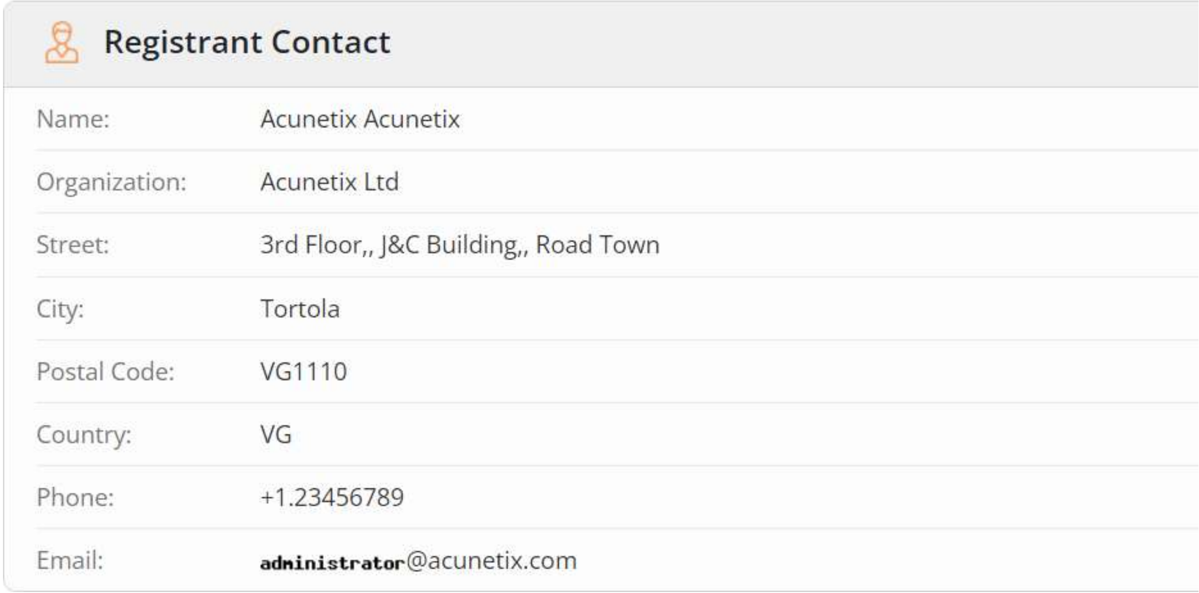
Domain Information

Domain:	vulnweb.com
Registrar:	EuroDNS S.A.
Registered On:	2010-06-14
Expires On:	2025-06-13
Updated On:	2023-05-26
Status:	clientTransferProhibited
Name Servers:	ns1.eurodns.com ns2.eurodns.com ns3.eurodns.com ns4.eurodns.com



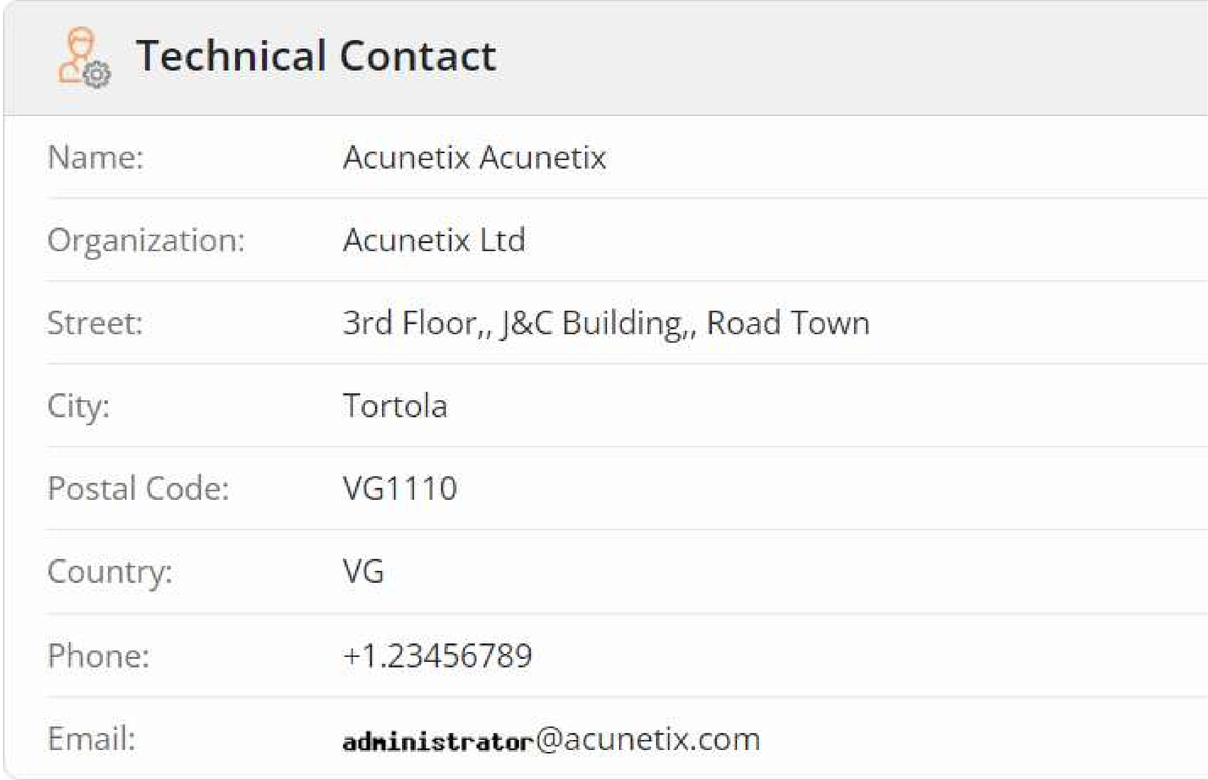
Administrative Contact

Name:	Acunetix Acunetix
Organization:	Acunetix Ltd
Street:	3rd Floor,, J&C Building,, Road Town
City:	Tortola
Postal Code:	VG1110
Country:	VG
Phone:	+1.23456789
Email:	administrator@acunetix.com



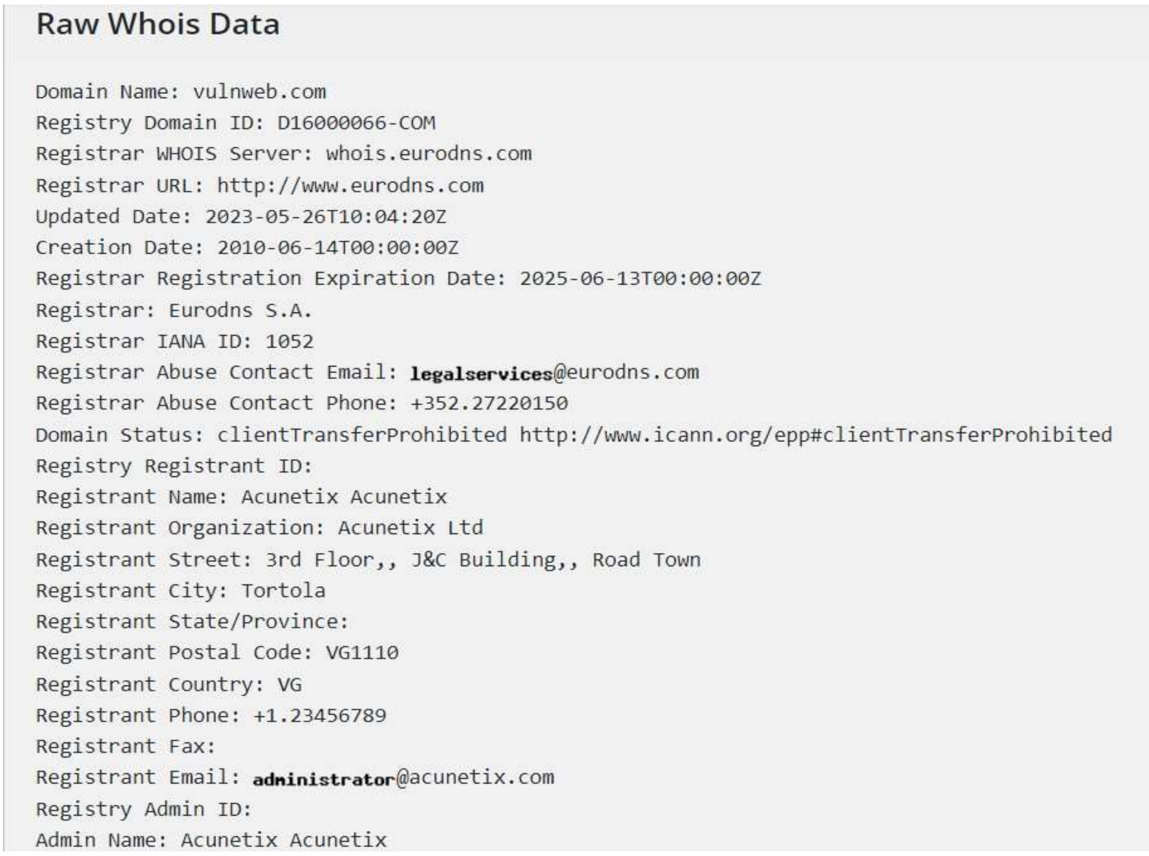
Registrant Contact

Name:	Acunetix Acunetix
Organization:	Acunetix Ltd
Street:	3rd Floor,, J&C Building,, Road Town
City:	Tortola
Postal Code:	VG1110
Country:	VG
Phone:	+1.23456789
Email:	administrator@acunetix.com



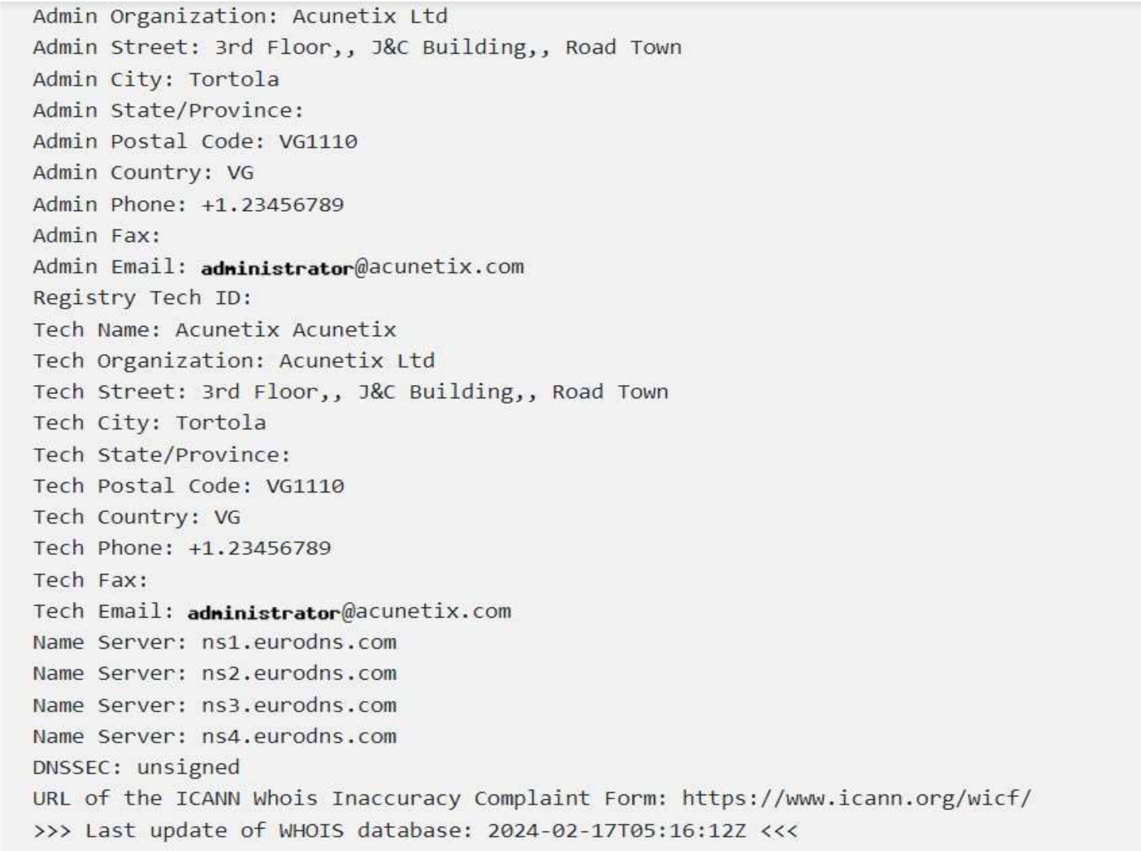
Technical Contact

Name:	Acunetix Acunetix
Organization:	Acunetix Ltd
Street:	3rd Floor,, J&C Building,, Road Town
City:	Tortola
Postal Code:	VG1110
Country:	VG
Phone:	+1.23456789
Email:	administrator@acunetix.com



Raw Whois Data

```
Domain Name: vulnweb.com
Registry Domain ID: D16000066-COM
Registrar WHOIS Server: whois.eurodns.com
Registrar URL: http://www.eurodns.com
Updated Date: 2023-05-26T10:04:20Z
Creation Date: 2010-06-14T00:00:00Z
Registrar Registration Expiration Date: 2025-06-13T00:00:00Z
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#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Acunetix Acunetix
Registrant Organization: Acunetix Ltd
Registrant Street: 3rd Floor,, J&C Building,, Road Town
Registrant City: Tortola
Registrant State/Province:
Registrant Postal Code: VG1110
Registrant Country: VG
Registrant Phone: +1.23456789
Registrant Fax:
Registrant Email: administrator@acunetix.com
Registry Admin ID:
Admin Name: Acunetix Acunetix
```



```
Admin Organization: Acunetix Ltd
Admin Street: 3rd Floor,, J&C Building,, Road Town
Admin City: Tortola
Admin State/Province:
Admin Postal Code: VG1110
Admin Country: VG
Admin Phone: +1.23456789
Admin Fax:
Admin Email: administrator@acunetix.com
Registry Tech ID:
Tech Name: Acunetix Acunetix
Tech Organization: Acunetix Ltd
Tech Street: 3rd Floor,, J&C Building,, Road Town
Tech City: Tortola
Tech State/Province:
Tech Postal Code: VG1110
Tech Country: VG
Tech Phone: +1.23456789
Tech Fax:
Tech Email: administrator@acunetix.com
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/wicf/
>>> Last update of WHOIS database: 2024-02-17T05:16:12Z <<<
```