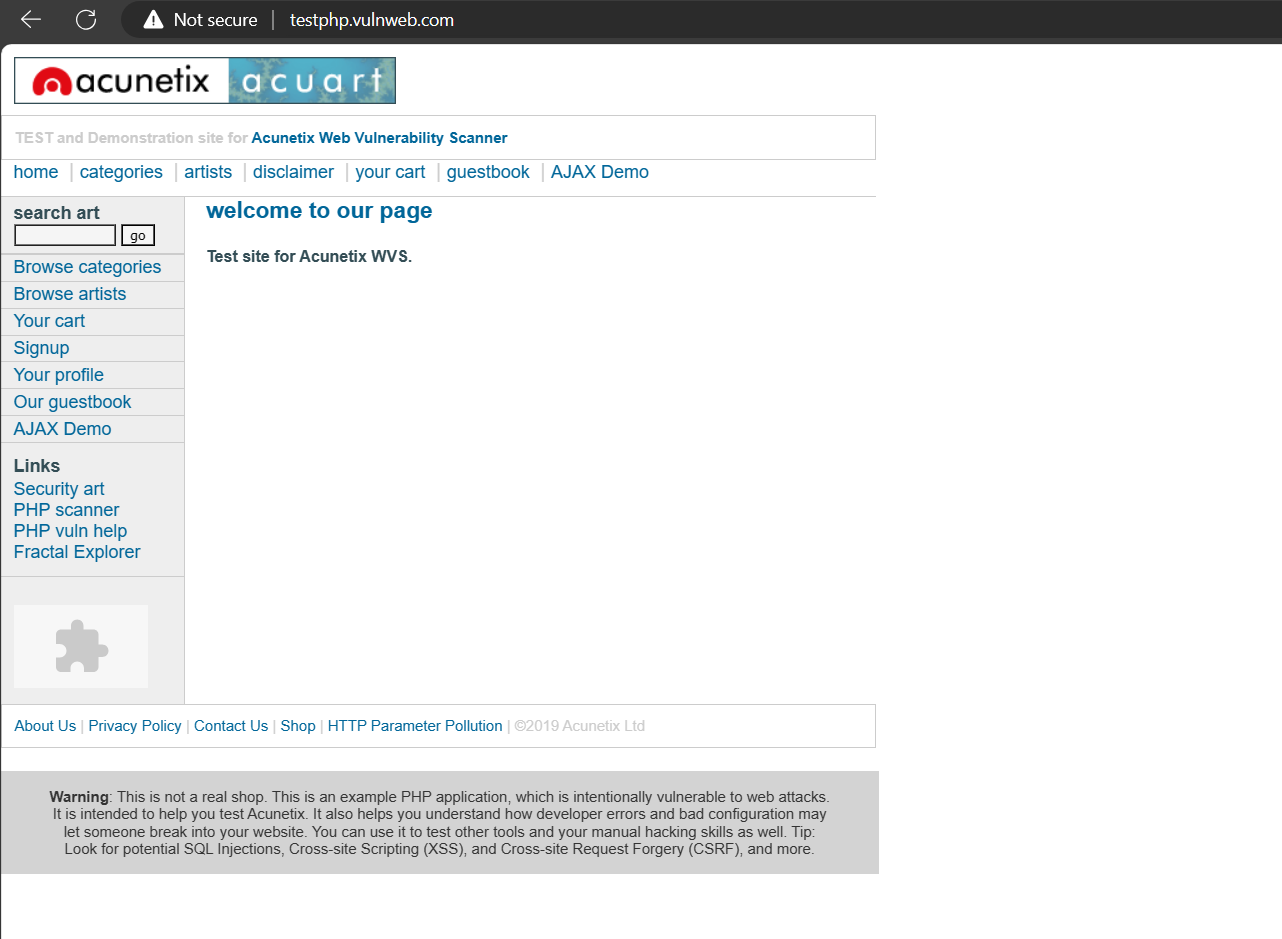
Name**: Prasanth Kumar Malleboina**

Roll No: **20A41A0531**

College: **Loyola Institute Of Technology and Management**

**STEP 1:**



**Foot Printing: & Reconnaissance :**

**STEP 2:**

**Whois Record for VulnWeb.com**

[How does this work?](https://whois.domaintools.com/vulnweb.com)

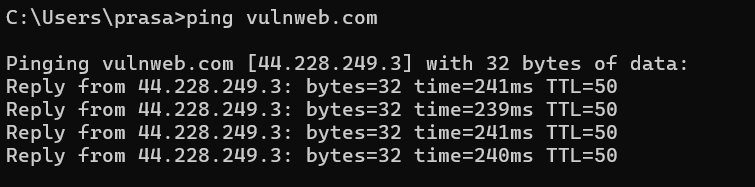
https://whois.domaintools.com/buffer.pgif?r=1896956521

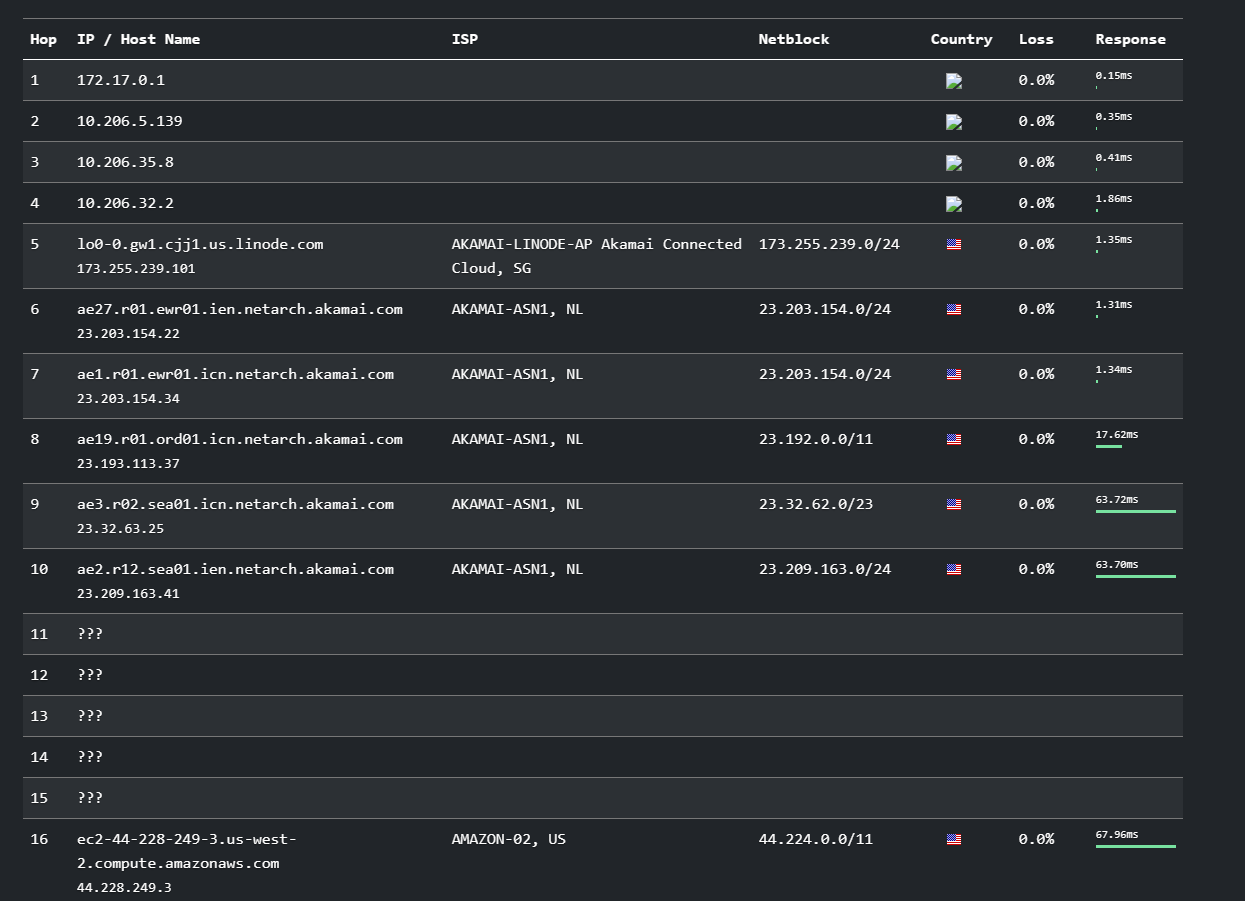
**Domain Profile**

|  |  |  |
| --- | --- | --- |
| **Registrar** | Eurodns S.A. EuroDNS S.A. IANA ID: 1052 URL: http://www.eurodns.com,http://www.EuroDNS.com Whois Server: whois.eurodns.com https://source.domaintools.com/email.pgif?md5=14d63d2299f8b53886e25cf0c3ce87f5&face=arial&size=9&color=000000&bgcolor=FFFFFF&face=Lato-Regular&size=10&color=5a5a5a&bgcolor=FFFFFF&format%5b%5d=transparent&format%5b%5d=transparent (p)https://source.domaintools.com/phone.pgif?hash=G%2F5Le5Dp69qngtd2GOjh1N7ct9PAKT7R&face=Lato-Regular&size=10&color=5a5a5a&bgcolor=FFFFFF&format%5b%5d=transparent&face=Lato-Regular&size=10&color=5a5a5a&bgcolor=FFFFFF&format%5b%5d=transparent | |
| **Registrar Status** | clientTransferProhibited | |
| **Dates** | 5,037 days old Created on 2010-06-14 Expires on 2025-06-13 Updated on 2023-05-26 |  |
| **Name Servers** | NS1.EURODNS.COM (has 305,149 domains) NS2.EURODNS.COM (has 305,149 domains) NS3.EURODNS.COM (has 305,149 domains) NS4.EURODNS.COM (has 305,149 domains) |  |
| **IP Address** | 44.228.249.3 is hosted on a dedicated server |  |
| **IP Location** | United States - Oregon - Boardman - Amazon.com Inc. | |
| **ASN** | United States AS16509 AMAZON-02, US (registered May 04, 2000) | |
| **Domain Status** | Registered And No Website | |
| **IP History** | 4 changes on 4 unique IP addresses over 10 years |  |
| **Registrar History** | 2 registrars |  |
| **Hosting History** | 1 change on 2 unique name servers over 14 years |  |

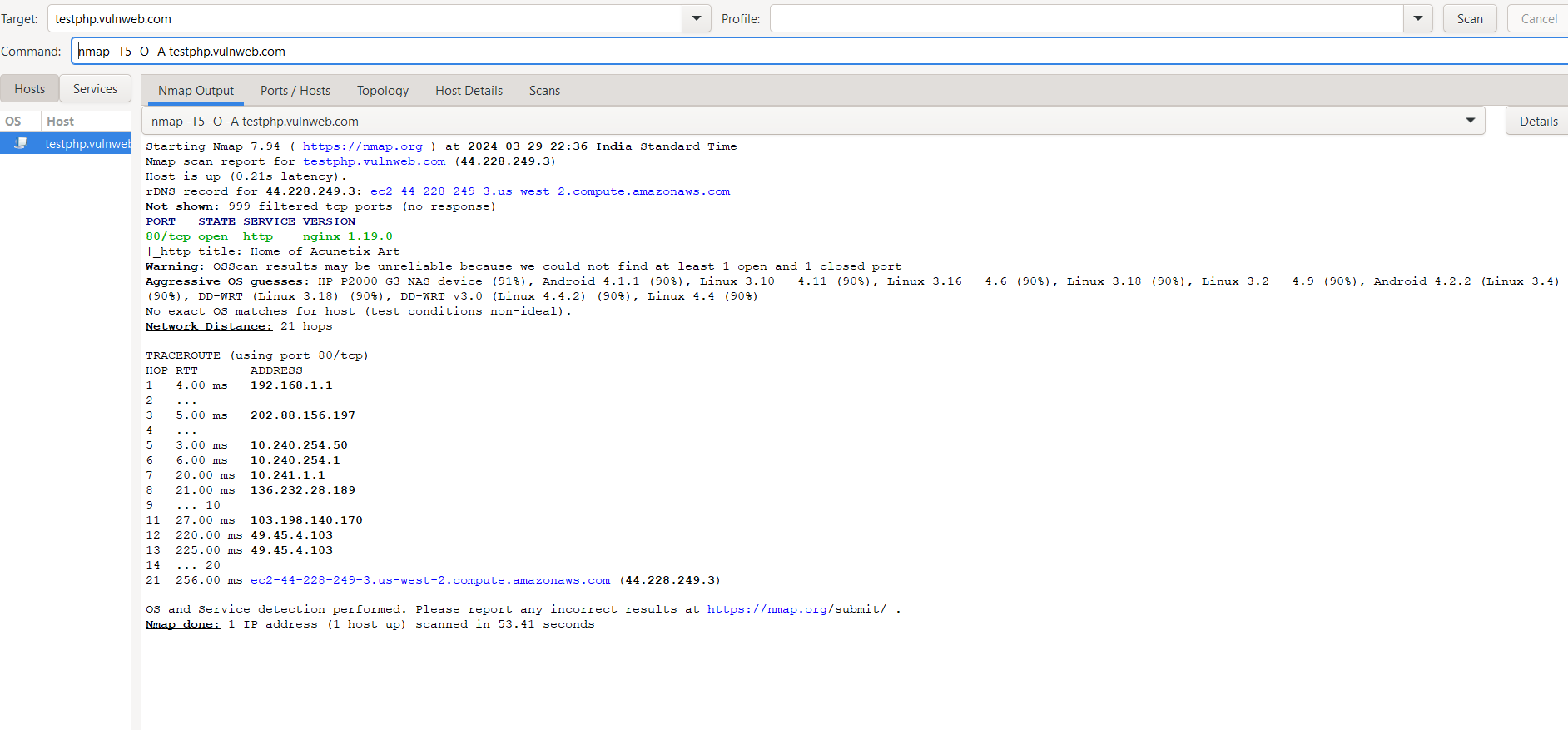
**Whois Record ( last updated on 2024-03-29 )**

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: [https://source.domaintools.com/email.pgif?md5=14d63d2299f8b53886e25cf0c3ce87f5&face=arial&size=9&color=000000&bgcolor=FFFFFF&face=arial&size=9&color=0000FF&bgcolor=FFFFFF&format%5b%5d=transparent&format%5b%5d=transparent](https://reversewhois.domaintools.com/?email=14d63d2299f8b53886e25cf0c3ce87f5)  
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: [https://source.domaintools.com/email.pgif?md5=eff823a2e8d72318ba26b26fdb1aa568&face=arial&size=9&color=000000&bgcolor=FFFFFF&face=arial&size=9&color=0000FF&bgcolor=FFFFFF&format%5b%5d=transparent&format%5b%5d=transparent](https://reversewhois.domaintools.com/?email=eff823a2e8d72318ba26b26fdb1aa568)  
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: [https://source.domaintools.com/email.pgif?md5=eff823a2e8d72318ba26b26fdb1aa568&face=arial&size=9&color=000000&bgcolor=FFFFFF&face=arial&size=9&color=0000FF&bgcolor=FFFFFF&format%5b%5d=transparent&format%5b%5d=transparent](https://reversewhois.domaintools.com/?email=eff823a2e8d72318ba26b26fdb1aa568)  
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: [https://source.domaintools.com/email.pgif?md5=eff823a2e8d72318ba26b26fdb1aa568&face=arial&size=9&color=000000&bgcolor=FFFFFF&face=arial&size=9&color=0000FF&bgcolor=FFFFFF&format%5b%5d=transparent&format%5b%5d=transparent](https://reversewhois.domaintools.com/?email=eff823a2e8d72318ba26b26fdb1aa568)  
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/  
  
Please email the listed admin email address if you wish to raise a legal issue.





**STEP 3:**



Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-29 22:36 India Standard Time

Nmap scan report for testphp.vulnweb.com (44.228.249.3)

Host is up (0.21s latency).

rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com

Not shown: 999 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

80/tcp open http nginx 1.19.0

|\_http-title: Home of Acunetix Art

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: HP P2000 G3 NAS device (91%), Android 4.1.1 (90%), Linux 3.10 - 4.11 (90%), Linux 3.16 - 4.6 (90%), Linux 3.18 (90%), Linux 3.2 - 4.9 (90%), Android 4.2.2 (Linux 3.4) (90%), DD-WRT (Linux 3.18) (90%), DD-WRT v3.0 (Linux 4.4.2) (90%), Linux 4.4 (90%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 21 hops

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

1 4.00 ms 192.168.1.1

2 ...

3 5.00 ms 202.88.156.197

4 ...

5 3.00 ms 10.240.254.50

6 6.00 ms 10.240.254.1

7 20.00 ms 10.241.1.1

8 21.00 ms 136.232.28.189

9 ... 10

11 27.00 ms 103.198.140.170

12 220.00 ms 49.45.4.103

13 225.00 ms 49.45.4.103

14 ... 20

21 256.00 ms ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)

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 53.41 seconds

**STEP 4:**

The scan results for **testphp.vulnweb.com** reveal some interesting details:

1. **Hostname and IP Address**:
   * Hostname: **ec2-44-228-249-3.us-west-2.compute.amazonaws.com**
   * [IP Address: **44.228.249.3** 1](https://www.ip-tracker.org/lookup.php?ip=Testphp.vulnweb.com)[2](https://whatismyip.live/ip/44.228.249.3)
2. **Web Server Information**:
   * The web server running on port 80 is **Nginx 1.19.0**.
   * [The title of the home page is **“Home of Acunetix Art”** 3](http://testphp.vulnweb.com/).
3. **Operating System and Service Detection**:
   * The aggressive OS guesses suggest possibilities like **HP P2000 G3 NAS device** and **Android 4.1.1**.
   * [However, no exact OS match was found due to non-ideal test conditions 3](http://testphp.vulnweb.com/).
4. **Network Traceroute**:
   * [The traceroute shows the network path with **21 hops** to reach the target server 3](http://testphp.vulnweb.com/).
5. **Security Implications**:
   * The website appears to be an intentionally vulnerable PHP application designed for testing purposes.
   * It helps users understand web vulnerabilities and how to secure their websites.