Information Gatherng

REPORT

2024 - 2025

IP Address Resolution

Resolved IP Address: 3.6.38.128

WHOIS Lookup

Domain Information

Domain Name: infopark.in

Registrar: Endurance Digital Domain Technology Private Limited

Registrar IANA ID: 1716

Creation Date: Not Available

Last Updated: Not Available

Expiration Date: Not Available

Domain Statuses: Not Available

Registrant Information

Name: Not Available

Organization: Not Available

Address: Not Available

City: Not Available

State: Not Available

Postal Code: Not Available

Country: Not Available

Phone: Not Available

Fax: Not Available

Email: Not Available

Administrative Contact

Name: Not Available

Organization: Not Available

State: Not Available

Country: Not Available

Technical Contact

Name: Not Available

Organization: Not Available

State: Not Available

Country: Not Available

Name Servers

Not Available

Additional Information

Domain Protection: The domain is safeguarded under multiple prohibitive statuses.

InternetDB Information

InternetDB Information for IP: 3.6.38.128

Open Ports:

-22

-80

-443

CPEs:

cpe:/a:php:php:7.3.15

cpe:/a:cloudflare:cloudflare

cpe:/a:getbootstrap:bootstrap

cpe:/a:jquery:jquery

cpe:/a:apache:http_server

cpe:/a:openbsd:openssh

Hostnames:

infopark.in

ec2-3-6-38-128.ap-south-1.compute.amazonaws.com

www.infopark.in

Tags:

cloud

Vulnerabilities:

CVE-2020-7068 CVE-2019-11048

CVE-2020-7071 CVE-2020-7066

CVE-2007-3205 CVE-2022-31628

CVE-2021-21707 CVE-2017-8923

CVE-2021-21703 CVE-2024-4577

CVE-2020-7065 CVE-2021-21702

CVE-2021-21704 CVE-2022-31629

CVE-2020-7070 CVE-2013-2220

CVE-2020-7064 CVE-2020-7069

CVE-2020-7067 CVE-2021-21705

CVE-2021-21706 CVE-2022-37454

Geolocation Lookup

IP Information

IP: 3.6.38.128

Hostname: ec2-3-6-38-128.ap-south-1.compute.amazonaws.com

City: Mumbai

Region: Maharashtra

Country: IN

Location: 19.0728,72.8826

Organization: AS16509 Amazon.com, Inc.

Postal: 400017

Timezone: Asia/Kolkata

Shodan Information

Shodan Information for IP: 3.6.38.128

Organization: Amazon Data Services India

Operating System: None

ISP: Amazon.com, Inc.

Country: India

City: Mumbai

Latitude: 19.07283

Longitude: 72.88261

Open Ports:

Port: 22

Service: OpenSSH

Version: 7.2p2 Ubuntu-4ubuntu2.8

Banner: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8

Key type: ssh-rsa

Key:

AAAAB3NzaC1yc2EAAAADAQABAAABAQDG1ea4WgOC9MeptF4RrlFotEixboNHTbshl
uMa7uUp4oV3
5hsZX5hdVL9K+kLR59Xw9Jma8pXIKt6UsWUiByskmS9NQRvBesXh7JH6isEuzCV1CIA
yL+eBnja2
fMM8itJQy7bnTA+CdaCdQh4io8XBgV0he8U8GrgdEn9AW3FDP3yfPvGDpsEUb84ljhTg
NoFYgxhz
sYocytboSYtqp9KNhallOYviu/FyYh/2Fr0aCtCzV8bK5WKPrih0Y++XCi80OMEbkAO+s3s
gUn+t
+lIltbR4cUy0L0BKNyp+00JRTJN9PreFtQRrYLUBvm/50B2CTNIBQ9Rqgs2IQA7Fm2ar

Fingerprint: fc:c4:14:1f:1f:b7:7c:f4:3d:6a:47:b7:f5:aa:42:a8

Kex Algorithms:

curve25519-sha256@libssh.org

ecdh-sha2-nistp256

ecdh-sha2-nistp384

ecdh-sha2-nistp521

diffie-hellman-group-exchange-sha256

diffie-hellman-group14-sha1

Server Host Key Algorithms:

ssh-rsa

rsa-sha2-512

rsa-sha2-256

ecdsa-sha2-nistp256

ssh-ed25519

Encryption Algorithms:

aes128-ctr

aes192-ctr

aes256-ctr

arcfour256

arcfour128

aes128-gcm@openssh.com

aes256-gcm@openssh.com

chacha20-poly1305@openssh.com

aes128-cbc

3des-cbc

blowfish-cbc

cast128-cbc

aes192-cbc

aes256-cbc

rijndael-cbc@lysator.liu.se

MAC Algorithms:

umac-64-etm@openssh.com

umac-128-etm@openssh.com

hmac-sha2-256-etm@openssh.com

hmac-sha2-512-etm@openssh.com

hmac-sha1-etm@openssh.com

umac-64@openssh.com

umac-128@openssh.com

hmac-sha2-256

hmac-sha2-512

hmac-sha1

Compression Algorithms:

none

zlib@openssh.com

Port: 80

Service: Apache httpd

Version: N/A

Banner: HTTP/1.1 200 OK

Date: Tue, 20 Aug 2024 18:51:23 GMT

Server: Apache

X-Powered-By: PHP/7.3.15

Cache-Control: no-cache

Set-Cookie:

XSRF-TOKEN=eyJpdiI6IlhFV1ZXQ0p3N083R2FvenZXXC9yWUpRPT0iLCJ2YWx1ZSI6InY5S01xbFwvejJzZ25EekhraVhLdkNzYmJ6VWEwQzVvOXgzZVNNcTdsV1RMY3I3RitQNWt5YVNuaEwrRlBnUmxzYTk3U202SlJrQ082TzllOUdTQ3RaQT09IiwibWFjIjoiYmU3ZTBlMzAwOWM2YjdkMWVjYTdjYjgwZmQyODAyZTJiNzhjNTM3NjNjMzFiNDM2Y2IzNGFhNDVmY2E1MDQzMyJ9; expires=Tue, 20-Aug-2024 20:51:23 GMT; Max-Age=7200; path=/

Set-Cookie:

laravel_session=eyJpdiI6ImNUcTMrUVh5TU94K0NyTU9kcjQxNEE9PSIsInZhbHVlIjoiMk1TdWc1OVVGeFF4ZHZ1TzA3TGVcL05FV3BhOERWUTkzWktrRkpQRUcyaklmQWg0ckw0WUFKWHNKUFd1dDJTQTdmU3Nla0FPTW5Ia21kc1BsUkRoQ2pnPT0iLCJtYWMiOiJiMzYwMWU3MTJmY2IzNTAyOWExZWNlMWE4OGYwN2NkODA0ZTQzM2QyODk3NWY0ODA4NTQzMDdkYWQ4ODBhYzc3In0%3D; expires=Tue, 20-Aug-2024 20:51:23 GMT; Max-Age=7200; path=/; HttpOnly

X-Frame-Options: SAMEORIGIN

X-Mod-Pagespeed: 1.13.35.2-0

Vary: Accept-Encoding

Cache-Control: max-age=0, no-cache, s-maxage=10

Content-Length: 70061

Content-Type: text/html; charset=UTF-8

Port: 443

Service: Apache httpd

Version: N/A

Banner: HTTP/1.1 200 OK

Date: Mon, 26 Aug 2024 07:36:14 GMT

Server: Apache

X-Powered-By: PHP/7.3.15

Cache-Control: no-cache

Set-Cookie:

XSRF-TOKEN=eyJpdiI6IkVGdzh6alk3aDQ1ZXpjUDNlSXlKdVE9PSIsInZhbHVlIjoiOGM5dFE2c2tDWDE4YjJkZWk1ZUJ0ZFZvaVFkdEZqSFkwd1J1VmRSbVF2SDVuNGgzS25meHc1ODlsQWI1VzJ3eEhBY3hCeTJocW9DeE1UQ3E0d1ZuV3c9PSIsIm1hYyI6ImUyNThiYzY5NzgyZjZjODRjNDllNjE4ZWE1ZDc1OTVkMGJhOTgxMjJhYmY2MzMzN2E1YmU0N2I4MmYwYTAyMTcifQ%3D%3D; expires=Mon, 26-Aug-2024 09:36:14 GMT; Max-Age=7200; path=/

Set-Cookie:

laravel_session=eyJpdiI6IngzTmZUdWYwMVdpTjdIdlJibUx3K0E9PSIsInZhbHVlIjoiUk5E
enVwVEE0VHF3dXhmTXlPNVpMMWJBN0FqU1lrR1d0RnNiejVTMHlcL21wK2V5VUt6Qj
BUNHo4MVBIeVZGK1BRVlFFekg2RklaNlRuWDgwa2t1ZUxRPT0iLCJtYWMiOiI5YWM3
ZDI4NGZhZThlYjJiNGIwYzJlNzdhMjFkM2Y0ZTVhMDY0NTg5YWFhNzJjYWFkNjk3NTRh
N2RmMzcxMzdhIn0%3D; expires=Mon, 26-Aug-2024 09:36:14 GMT; Max-Age=7200;
path=/; HttpOnly

X-Frame-Options: SAMEORIGIN

X-Mod-Pagespeed: 1.13.35.2-0

Vary: Accept-Encoding

Cache-Control: max-age=0, no-cache

Content-Length: 64001

Content-Type: text/html; charset=UTF-8

Nmap Scan

Starting Nmap 7.95 (https://nmap.org) at 2024-08-28 13:10 India Standard Time

Pre-scan script results:

| broadcast-avahi-dos:

| Discovered hosts:

| 224.0.0.251

| After NULL UDP avahi packet DoS (CVE-2011-1002).

|_ Hosts are all up (not vulnerable).

Nmap scan report for ec2-3-6-38-128.ap-south-1.compute.amazonaws.com (3.6.38.128)

Host is up (0.046s latency).

PORT STATE SERVICE

21/tcp filtered ftp

22/tcp open ssh

23/tcp filtered telnet

25/tcp filtered smtp

53/tcp filtered domain

80/tcp open http

|_http-dombased-xss: Couldn't find any DOM based XSS.

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|_http-csrf: Couldn't find any CSRF vulnerabilities.

110/tcp filtered pop3

135/tcp filtered msrpc

139/tcp filtered netbios-ssn

143/tcp filtered imap

443/tcp open https

|_http-dombased-xss: Couldn't find any DOM based XSS.

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|_http-csrf: Couldn't find any CSRF vulnerabilities.

445/tcp filtered microsoft-ds

3306/tcp filtered mysql

3389/tcp filtered ms-wbt-server

8080/tcp filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 59.17 seconds

Conclusion

No critical vulnerabilities were detected in the Nmap scan, but regular scans are advised to ensure ongoing security.Shodan identified 3 open ports, which could serve as potential entry points for attackers.It is recommended to review these open ports and secure or close them if they are not needed. Disabling unnecessary services can minimize exposure to threats.WHOIS lookup provided detailed information about the domain ownership. This information can be used to understand the entity behind the domain and assess potential risks associated with it.The IP is located in IN, which could indicate the origin of the services and provide insights into potential regional threats.No vulnerabilities were detected . Consider using other tools or methods, as our scan did not find any issues.