BASE PROJECT: COMPANY VULNERABILITY ASSESSMENT REPORT

NAVRATHAM JEWLLARY

1. Executive Summary

1.1. Scope Purpose and Duration of Work

The vulnerability assessment report for Navratham Jewllary provides a detailed and comprehensive overview of the scope, purpose, and duration of work conducted. The methodology involved a series of steps, beginning with information gathering and reconnaissance, followed by determining the test scope, scanning, vulnerability analysis, and reporting. The report includes a thorough breakdown of the settings used for the scan, vulnerabilities breakdown by severity levels, and a comprehensive scan summary. Additionally, it covers vulnerability analysis, scanning target systems, and identification of job advertisements that may reveal information about the organization's systems and network. The report also outlines the use of port scans, VPN identification, and password breaking techniques, providing a comprehensive and in-depth analysis of the vulnerabilities and potential security risks within the organization's systems and network infrastructure.

STEPS FOLLOWED

- Scope, purpose, and duration of work
- Methodology steps: information gathering, determining test scope, scanning, vulnerability analysis, and reporting
- Breakdown of scan settings and vulnerabilities by severity levels
- Vulnerability analysis and scanning of target systems
- Identification of job advertisements revealing information about the organization's systems and network
- Use of port scans, VPN identification, and password breaking techniques
- Comprehensive analysis of vulnerabilities and potential security risks within the organization's systems and network infrastructure

1. **Scope, Purpose, and Duration of Work:**

The report begins with a detailed overview of the scope, purpose, and duration of the vulnerability assessment work conducted for Navratham Jewllary.

2. **Methodology Steps:**

The methodology involved a series of steps, including information gathering, determining the test scope, scanning, vulnerability analysis, and reporting. Each step is outlined to provide a clear understanding of the approach taken.

3. **Breakdown of Scan Settings and Vulnerabilities:**

The report provides a breakdown of the settings used for the scan, along with a comprehensive analysis of vulnerabilities by severity levels. This section likely includes critical, high, medium, low, and informational vulnerabilities.

4. Vulnerability Analysis and Scanning of Target Systems:

Details about the vulnerability analysis process and the scanning of target systems using vulnerability scanners like Nessus, Acunetix, etc., are included. This section may also cover SSL certificate scanning to determine their validity.

5. Identification of Job Advertisements:

The report may include details about the identification of job advertisements that reveal information about the organization's systems and network. This information can be crucial for understanding potential security risks.

6. Use of Port Scans, VPN Identification, and Password Breaking Techniques:

The report outlines the use of port scans to determine open ports, operating systems, and services. It also covers the identification of VPN servers using specific commands and the execution of password breaking techniques using tools like Hydra, Nessus, etc.

7. Comprehensive Analysis of Vulnerabilities and Security Risks:

The report provides a comprehensive and in-depth analysis of the vulnerabilities and potential security risks within the organization's systems and network infrastructure. This analysis is crucial for understanding the overall security posture and potential areas of improvement

2. Methodology

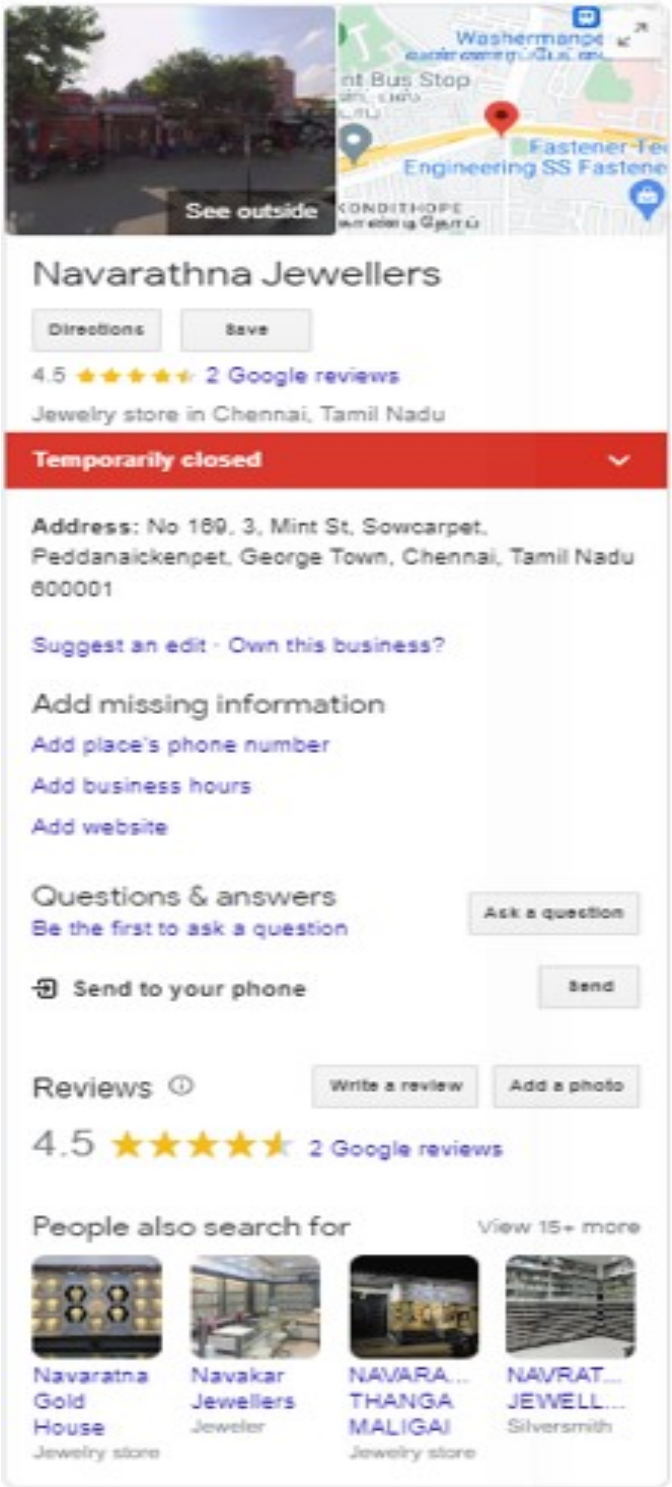
The methodology consisted of # of steps beginning with the determination of test scope, and ending with reporting. These tests were performed by security experts using potential attackers' modes of operation while controlling execution to prevent harm to the systems being tested. The approach included but is not limited to manual and automated vulnerability scans, verification of findings (automated and otherwise). This verification step and manual scanning process eliminated false positives and erroneous outputs, resulting in more efficient tests.

- Information Gathering / Reconnaissance
- Determining scope of the test
- Scanning
- Vulnerability Analysis
- Reporting

WHOIS

2.1. Information Gathering

Before directly accessing the target we researched everything we could locate from third party resources. This included DNS records, previous hacking attempts, job listings, email addresses, etc. This information was used in later tests.



WHOIS

2.1.1. IP Addresses and Domains

Here is a list of the IP addresses and domains gathered using search engines:

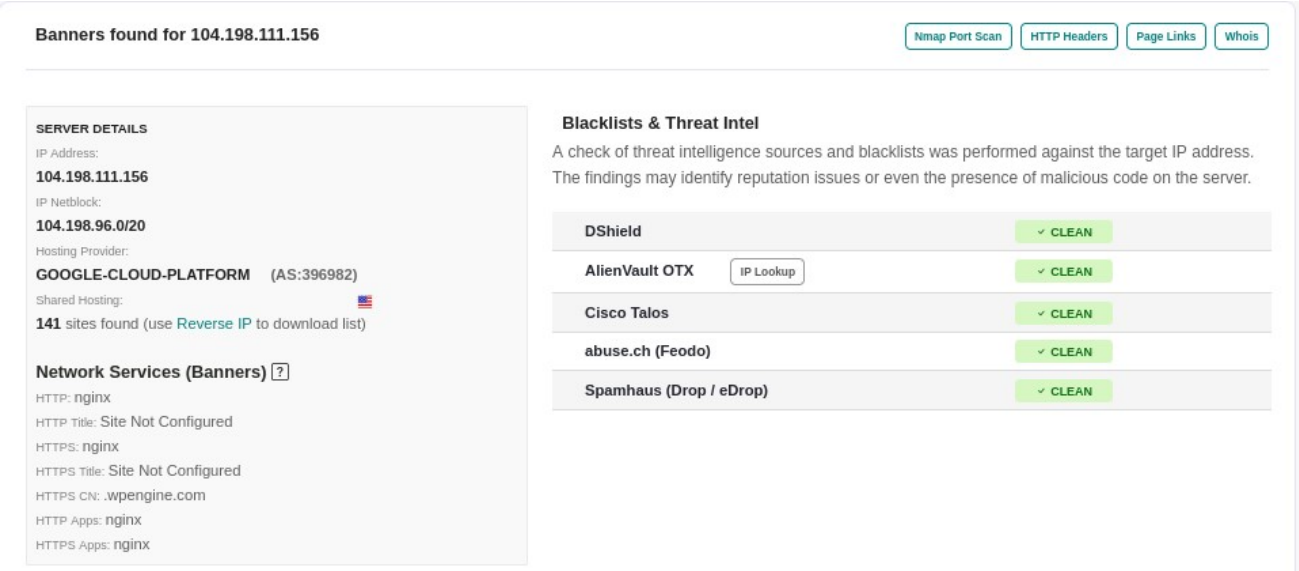


Fig 2.1.1: IP ADDRESSES

```
Starting Nmap 7.40 ( https://nmap.org ) at 2024-01-26 14:03 UTC
Nmap scan report for 156.111.198.104.bc.googleusercontent.com (104.198.111.156)
Host is up (0.070s latency).
PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
80/tcp   open     http
110/tcp  filtered pop3
143/tcp  filtered imap
443/tcp  open     https
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.03 seconds
```

Fig 2.1.1: IP ADDRESSES FROM NMAP

WHOIS

2.1.2. Virtual Hosts

Virtual hosts sometimes share the same IP address with other website addresses. An attacker can compromise the server on which the target application runs using a vulnerability found on another website hosted on the same server.

Virtual Hosts found for 104.198.111.156

The following is a list of all hostnames found with DNS "A" records pointing to 104.198.111.156. **Threat Intel** and **Blacklist** checks have been performed on each hostname.

	HOSTNAME	LOOKUP
G	orvoad.org	HTTP Headers Page Links Whois DNS Lookup
G	cpcalendars.cbhvac.com	HTTP Headers Page Links Whois DNS Lookup
G	parlanti.wpengine.com	HTTP Headers Page Links Whois DNS Lookup
G	orthokdoctor.wpengine.com	HTTP Headers Page Links Whois DNS Lookup
G	c.research.trailer-studios.com	HTTP Headers Page Links Whois DNS Lookup
G	thesisustore.com	HTTP Headers Page Links Whois DNS Lookup
G	www.powwowschedule.com	HTTP Headers Page Links Whois DNS Lookup
G	fiercebold.wpengine.com	HTTP Headers Page Links Whois DNS Lookup
G	voadwyoming.wpengine.com	HTTP Headers Page Links Whois DNS Lookup
G	f.research.trailer-studios.com	HTTP Headers Page Links Whois DNS Lookup
G	cslstudy.wpenginie.com	HTTP Headers Page Links Whois DNS Lookup
G	keylaw.gsbridge.wpengine.com	HTTP Headers Page Links Whois DNS Lookup
G	chargesummit.wpengine.com	HTTP Headers Page Links Whois DNS Lookup
G	offices4less.com	HTTP Headers Page Links Whois DNS Lookup
G	learnercentered.org	HTTP Headers Page Links Whois DNS Lookup
G	michigan-open.org	HTTP Headers Page Links Whois DNS Lookup
G	brightbluedata.com	HTTP Headers Page Links Whois DNS Lookup
G	prvoad.org	HTTP Headers Page Links Whois DNS Lookup
G	powwowschedule.com	HTTP Headers Page Links Whois DNS Lookup
G	apexholdings.wpengine.com	HTTP Headers Page Links Whois DNS Lookup
G	voadas.wpengine.com	HTTP Headers Page Links Whois DNS Lookup
G	ncvoad.net	HTTP Headers Page Links Whois DNS Lookup
G	spmlaw.wpengine.com	HTTP Headers Page Links Whois DNS Lookup
G	theoverlookphilly.com	HTTP Headers Page Links Whois DNS Lookup
G	theeyedocblog.wpengine.com	HTTP Headers Page Links Whois DNS Lookup
G	osagepine.com	HTTP Headers Page Links Whois DNS Lookup
G	jeuxderoles.net	HTTP Headers Page Links Whois

WHOIS

2.1.3. Detailed DNS Records

DNS records identify URL/IP pairs. DNS servers connect the organization website to outside world. Exploitation of these servers may lead to malicious usage of the organization web and mail servers.

A records

IPv4 address	Revalidate in
104.198.111.156	6h

AAAA records

No AAAA records found.

CNAME record

No CNAME record found.

TXT records

No TXT records found.

NS records

Name server	Revalidate in
dns1.bigrock.in.	6h
dns2.bigrock.in.	6h
dns3.bigrock.in.	6h
dns4.bigrock.in.	6h

MX records

Mail server	Priority	Revalidate in
aspmx.l.google.com.	0 Primary	6h
alt1.aspmx.google.com.	5	6h
alt2.aspmx.google.com.	5	6h
aspmx2.googlemail.com.	10	6h
aspmx3.googlemail.com.	10	6h
aspmx4.googlemail.com.	10	6h
aspmx5.googlemail.com.	10	6h

Other records

SOA

SOA data		Revalidate in
Start of authority	dns1.bigrock.in.	2h
Email	nareshjoshi36@yahoo.com	
Serial	2023111701	
Refresh	2h	
Retry	2h	
Expire	48h	
Negative cache TTL	10h 40m	

WHOIS

2.1.4. WHOIS Information

'WHOIS' searches provide information regarding the domain name. It may include information such as domain ownership, where and when it was registered, expiration date, email address of the domain manager and the server names assigned to the domain.

navrathan.com

Updated 1 second ago

Domain Information

Domain:	navrathan.com
Registrar:	BigRock Solutions Ltd
Registered On:	2009-04-15
Expires On:	2024-04-15
Updated On:	2023-04-12
Status:	clientTransferProhibited
Name Servers:	dns1.bigrock.in dns2.bigrock.in dns3.bigrock.in dns4.bigrock.in

Registrant Contact

Name:	Embassy IT Solutions EITS
Street:	Bangalore
City:	BANGALORE
State:	Karnataka
Postal Code:	560094
Country:	IN
Phone:	+91.09886332347
Email:	prakash@embassyit.com

Administrative Contact

Name:	Embassy IT Solutions EITS
Street:	Bangalore
City:	BANGALORE
State:	Karnataka
Postal Code:	560094
Country:	IN
Phone:	+91.09886332347
Email:	prakash@embassyit.com

Login Pages Found During Server

Raw Whois Data

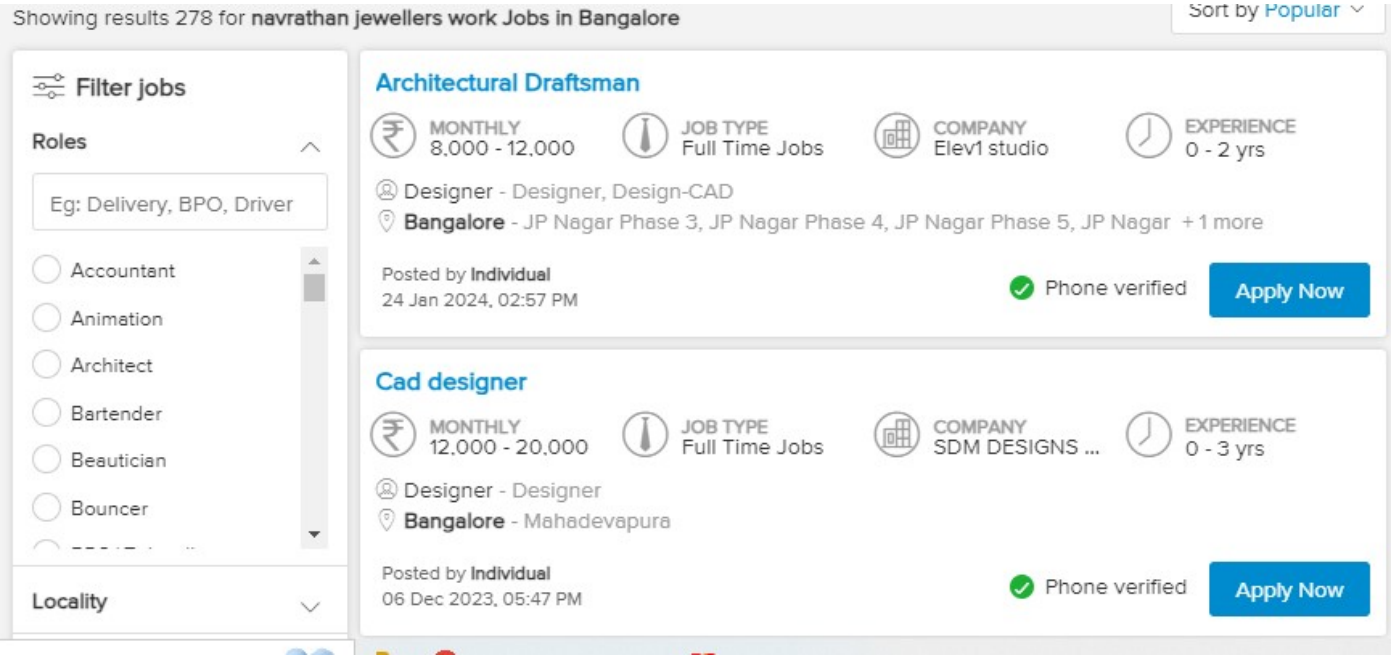
```
Domain Name: NAVRATHAN.COM
Registry Domain ID: 1552349844_DOMAIN_COM-VRSN
Registrar WHOIS Server: Whois.bigrock.com
Registrar URL: www.bigrock.com
Updated Date: 2023-11-11T11:18:45Z
Creation Date: 2009-04-15T14:49:46Z
Registrar Registration Expiration Date: 2024-04-15T14:49:46Z
Registrar: BigRock Solutions Ltd.
Registrar IANA ID: 1495
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Embassy IT Solutions EITS
Registrant Organization:
Registrant Street: Bangalore
Registrant City: BANGALORE
Registrant State/Province: Karnataka
Registrant Postal Code: 560094
Registrant Country: IN
Registrant Phone: +91.09886332347
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: prakash@embassyit.com
Registry Tech ID: Not Available From Registry
Tech Name: Embassy IT Solutions EITS
Tech Organization:
Tech Street: Bangalore
Tech City: BANGALORE
Tech State/Province: Karnataka
Tech Postal Code: 560094
Tech Country: IN
Tech Phone: +91.09886332347
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: prakash@embassyit.com
Name Server: dns1.bigrock.in
Name Server: dns2.bigrock.in
Name Server: dns3.bigrock.in
Name Server: dns4.bigrock.in
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse@bigrock.com
Registrar Abuse Contact Phone: +1-415-349-0015
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-01-27T04:08:31Z <<<
```

Fig 2.1.4 whois details of navrathan.com

2.1.5. Job Advertisements

Job advertisements may reveal information about the organization systems and network. The requirements specified in job adverts sometimes disclose information regarding which programme languages and systems are used, providing attackers with more specific knowledge of the targets.

By analyzing the following job advertisements we obtained the information listed below.



This are the links that are Advertised by shopify.

- https://www.quikr.com/jobs/navrathan-jewellers-work+bangalore+zwqxj4157493934
- https://www.naukri.com/navratna-jewellers-jobs-careers-3245598
- https://www.trymintly.com/job/navaratna-maaligai-jobs-vacancy-b2b-sales-mumbai

2.1.6. Login Pages Found During Server Analysis

Login pages are the front line of an application's defence against unauthorized access. They also present a surface area of interest to attackers who will try to defeat the defences in order to access the functionality and data within the system. This section indentifies the URLs and screens of the login pages discovered during analysis.

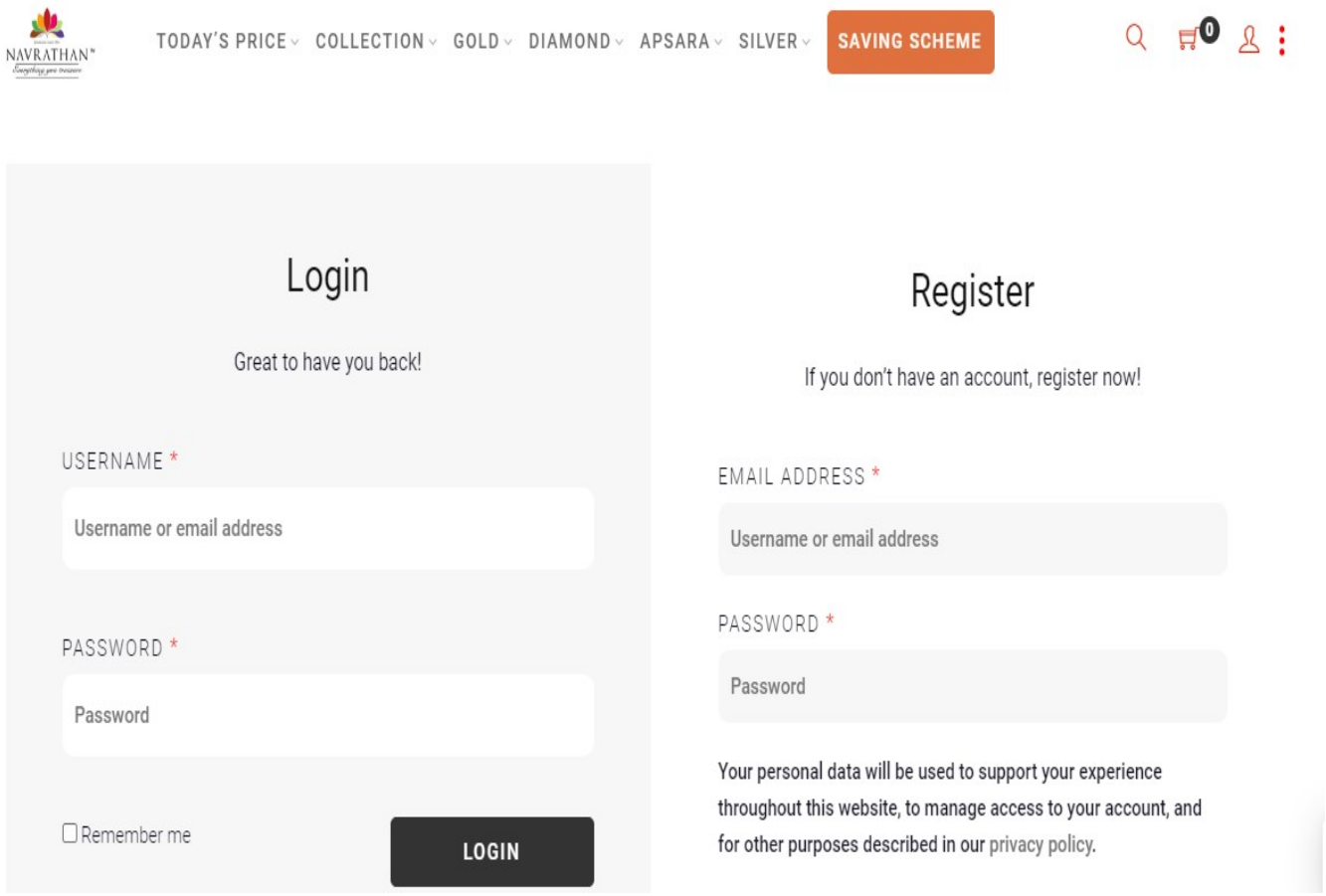


Fig 2.1.6 : found the login page of the navrathan.com

2.2. Determining the Scope

Navratna Jewellers Private Limited is an unlisted private company incorporated on 19 April, 2004. It is classified as a private limited company and is located in Mumbai, Maharashtra. It's authorized share capital is INR 5.00 lac and the total paid-up capital is INR 5.00 lac.

The current status of Navratna Jewellers Private Limited is - Active.

The last reported AGM (Annual General Meeting) of Navratna Jewellers Private Limited, per our records, was held on 30 September, 2022.

Navratna Jewellers Private Limited has two directors - Dilip Madhav Lagu and Asavari Dilip Lagu.

The Corporate Identification Number (CIN) of Navratna Jewellers Private Limited is U36910MH2004PTC145759. The registered office of Navratna Jewellers Private Limited is at 206,SHILPIN CENTRE,, 40 G.D.AMBEKAR MARG, WADALA,, MUMBAI, Maharashtra.

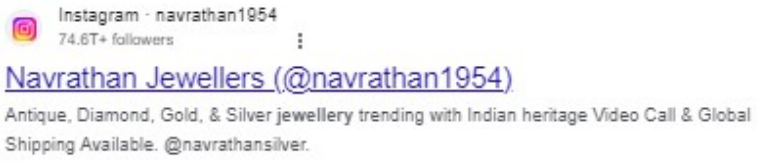


Fig : Instagram profile

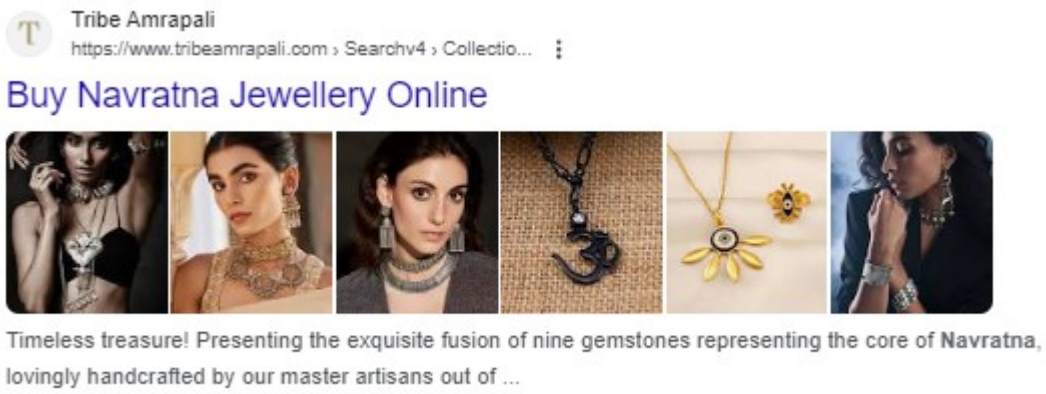


Fig : tribe amrapali is sealing navrathn jewellery

Port

REGISTERED DETAILS - NAVRATNA JEWELLERS PRIVATE LIMITED

CIN	INCORPORATION DATE / AGE	LAST REPORTED AGM DATE
U36910MH2004PTC145759	19 April, 2004 / 20 yrs	30 September, 2022
AUTHORIZED CAPITAL	**PAIDUP CAPITAL**	**INDUSTRY***
INR 5.0 Lacs	INR 5.0 Lacs	Manufacturing (Others)
TYPE	**CATEGORY**	**SUBCATEGORY**
Unlisted Private Company	Company limited by Shares	Non-govt company

EMAIL ADDRESS
Login for email address. This is to prevent spam.
WEBSITE
Website not known. Click here to let us know.

REGISTERED ADDRESS
206,SHILPIN CENTRE,
40 G.D.AMBEKAR MARG, WADALA,
MUMBAI - 400031

DIRECTORS - NAVRATNA JEWELLERS PRIVATE LIMITED

The company has 2 directors and no reported key management personnel.

The longest serving director currently on board is Dilip Madhav Lagu who was appointed on 19 April, 2004. Dilip Madhav Lagu has been on the board for more than 19 years. The most recently appointed director is Asavari Dilip Lagu, who was appointed on 23 April, 2004.

Dilip Madhav Lagu has the largest number of other directorships with a seat at a total of 7 companies. In total, the company is connected to 6 other companies through its directors.

19 April, 2004
DILIP MADHAV LAGU
Director

23 April, 2004
ASAVARI DILIP LAGU
Director

SIMILAR COMPANIES

NAME	INCORPORATION YEAR	STATE	PAID UP CAPITAL	
SHAMA COTTAGE PRODUCTS PRIVATE LIMITED	2011	Bihar	5.00 lac	Buy financial reports
S P JINDAL INDUSTRIES LIMITED	2012	Delhi	5.00 lac	Buy financial reports
SHRI DURGA TIMBER PRIVATE LIMITED	2021	Haryana	5.00 lac	Buy financial reports
SHARP REFILLS CO PVT LTD	1979	Gujarat	5.00 lac	Buy financial reports
NEXFLOORS EXIM PRIVATE LIMITED	2020	Delhi	5.00 lac	Buy financial reports
INSTROLL CEMENT PRIVATE LIMITED	2020	Bihar	5.00 lac	Buy financial reports
DHANUKA FLYASH BRICKS INDUSTRY PRIVATE LIMITED	2020	Bihar	5.00 lac	Buy financial reports
AGG JEWELLERS PRIVATE LIMITED	2019	Haryana	5.00 lac	Buy financial reports
GOLDEN KRAFTS (INDIA) PRIVATE LIMITED	1993	Delhi	5.00 lac	Buy financial reports
HYC INFRA INDIA PRIVATE LIMITED	2012	Haryana	5.00 lac	Buy financial reports

Port

2.3 Scanning

Various scans were performed to determine and verify vulnerabilities in the target systems.

This is the simple scan of the target here we the nmap function to get the data related to the target

Here we found some data that are 1. Version of the target.

2. OS footprinting.

3. A simple scan of the target ip address.

```
└─# nmap -sS -v -O navrathan.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-26 23:02 MST
Initiating Ping Scan at 23:02
Scanning navrathan.com (104.198.111.156) [4 ports]
Completed Ping Scan at 23:02, 0.40s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:02
Completed Parallel DNS resolution of 1 host. at 23:02, 0.52s elapsed
Initiating SYN Stealth Scan at 23:02
Scanning navrathan.com (104.198.111.156) [1000 ports]
Discovered open port 80/tcp on 104.198.111.156
Discovered open port 443/tcp on 104.198.111.156
Discovered open port 2222/tcp on 104.198.111.156
Completed SYN Stealth Scan at 23:03, 22.79s elapsed (1000 total ports)
Initiating OS detection (try #1) against navrathan.com (104.198.111.156)
Retrying OS detection (try #2) against navrathan.com (104.198.111.156)
Nmap scan report for navrathan.com (104.198.111.156)
Host is up (0.24s latency).
rDNS record for 104.198.111.156: 156.111.198.104.bc.googleusercontent.com
Not shown: 996 filtered tcp ports (no-response), 1 filtered tcp ports (host-prohibited)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
2222/tcp open  EtherNetIP-1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.84 seconds
           Raw packets sent: 2085 (95.424KB) | Rcvd: 33 (2.036KB)
```

Fig 2.3 : Simple scan of the target.

Port

2.3.1 .Port Scans

Here we have used the nmap function Primarily nmap is used to scan the targets. Besides nmap,tools like strobe, xprobe, amap are used to determine which ports are open, which operating systems are working on targets, and which services are used.

```
└# nmap -sS -v -P  navrathan.com
Warning: The -P option is deprecated. Please use -PE
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-26 23:08 MST
Initiating Ping Scan at 23:08
Scanning navrathan.com (104.198.111.156) [1 port]
Completed Ping Scan at 23:08, 0.34s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:08
Completed Parallel DNS resolution of 1 host. at 23:08, 0.01s elapsed
Initiating SYN Stealth Scan at 23:08
Scanning navrathan.com (104.198.111.156) [1000 ports]
Discovered open port 80/tcp on 104.198.111.156
Completed SYN Stealth Scan at 23:08, 25.43s elapsed (1000 total ports)
Nmap scan report for navrathan.com (104.198.111.156)
Host is up (0.28s latency).
rDNS record for 104.198.111.156: 156.111.198.104.bc.googleusercontent.com
Not shown: 997 filtered tcp ports (no-response), 1 filtered tcp ports (host-prohibited)
PORT     STATE  SERVICE
80/tcp   open   http
2222/tcp closed EtherNetIP-1

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 25.91 seconds
           Raw packets sent: 2008 (88.336KB) | Rcvd: 14 (620B)
```

Fig 2.3.1 : Port scan of the target.

2.3.1. Route Scans

Here we have used the nmap function and the traceroute commad to perform the route scan and some more Using tools like hping, scanrand, the network mapping of targets can be determined. It is also useful for detecting defensive measures like IDS, IPS, UTM, and firewalls.

```
└─# nmap -traceroute 104.198.111.156
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-26 23:13 MST
Nmap scan report for 156.111.198.104.bc.googleusercontent.com (104.198.111.156)
Host is up (0.32s latency).
Not shown: 997 filtered tcp ports (no-response), 1 filtered tcp ports (host-prohibited)
PORT     STATE  SERVICE
80/tcp   open   http
2222/tcp closed EtherNetIP-1

TRACEROUTE (using port 2222/tcp)
HOP RTT       ADDRESS
1   8.56 ms   192.168.190.215
2    ...
3   61.46 ms  10.50.122.185
4   61.30 ms  10.0.66.209
5    ... 6
7   61.43 ms  142.250.169.206
8   372.26 ms 156.111.198.104.bc.googleusercontent.com (104.198.111.156)

Nmap done: 1 IP address (1 host up) scanned in 33.71 seconds
```

Fig 2.3.2 : Using Traceroute command

```
┌──(root㉿kali)-[/home/sainath]
└─# hping3 -1 104.198.111.156
HPING 104.198.111.156 (eth0 104.198.111.156): icmp mode set, 28 headers + 0 data bytes
len=46 ip=104.198.111.156 ttl=57 id=22163 icmp_seq=0 rtt=436.4 ms
len=46 ip=104.198.111.156 ttl=57 id=22173 icmp_seq=1 rtt=487.7 ms
len=46 ip=104.198.111.156 ttl=57 id=22380 icmp_seq=2 rtt=227.8 ms
len=46 ip=104.198.111.156 ttl=57 id=22614 icmp_seq=3 rtt=250.9 ms
len=46 ip=104.198.111.156 ttl=57 id=22735 icmp_seq=4 rtt=219.9 ms
len=46 ip=104.198.111.156 ttl=57 id=22792 icmp_seq=5 rtt=332.3 ms
len=46 ip=104.198.111.156 ttl=57 id=23083 icmp_seq=7 rtt=244.2 ms
len=46 ip=104.198.111.156 ttl=57 id=23338 icmp_seq=8 rtt=246.3 ms
len=46 ip=104.198.111.156 ttl=57 id=23437 icmp_seq=9 rtt=482.5 ms
len=46 ip=104.198.111.156 ttl=57 id=23465 icmp_seq=10 rtt=446.4 ms
len=46 ip=104.198.111.156 ttl=57 id=23642 icmp_seq=11 rtt=245.5 ms
len=46 ip=104.198.111.156 ttl=57 id=23663 icmp_seq=12 rtt=346.9 ms
len=46 ip=104.198.111.156 ttl=57 id=23890 icmp_seq=13 rtt=332.2 ms
len=46 ip=104.198.111.156 ttl=57 id=24018 icmp_seq=14 rtt=285.8 ms
len=46 ip=104.198.111.156 ttl=57 id=24080 icmp_seq=15 rtt=244.5 ms
len=46 ip=104.198.111.156 ttl=57 id=24262 icmp_seq=16 rtt=244.6 ms
len=46 ip=104.198.111.156 ttl=57 id=24473 icmp_seq=17 rtt=485.8 ms
len=46 ip=104.198.111.156 ttl=57 id=24598 icmp_seq=18 rtt=279.3 ms
len=46 ip=104.198.111.156 ttl=57 id=24718 icmp_seq=19 rtt=242.5 ms
len=46 ip=104.198.111.156 ttl=57 id=24744 icmp_seq=20 rtt=362.1 ms
len=46 ip=104.198.111.156 ttl=57 id=24872 icmp_seq=21 rtt=317.8 ms
len=46 ip=104.198.111.156 ttl=57 id=25075 icmp_seq=22 rtt=276.8 ms
len=46 ip=104.198.111.156 ttl=57 id=25280 icmp_seq=23 rtt=240.1 ms
len=46 ip=104.198.111.156 ttl=57 id=25391 icmp_seq=24 rtt=518.7 ms
len=46 ip=104.198.111.156 ttl=57 id=25522 icmp_seq=25 rtt=482.2 ms
len=46 ip=104.198.111.156 ttl=57 id=25725 icmp_seq=26 rtt=272.8 ms
len=46 ip=104.198.111.156 ttl=57 id=25788 icmp_seq=27 rtt=240.7 ms
len=46 ip=104.198.111.156 ttl=57 id=25862 icmp_seq=28 rtt=274.2 ms
len=46 ip=104.198.111.156 ttl=57 id=25885 icmp_seq=29 rtt=315.0 ms
len=46 ip=104.198.111.156 ttl=57 id=25988 icmp_seq=30 rtt=273.1 ms
len=46 ip=104.198.111.156 ttl=57 id=26194 icmp_seq=31 rtt=238.8 ms
len=46 ip=104.198.111.156 ttl=57 id=26227 icmp_seq=32 rtt=237.1 ms
len=46 ip=104.198.111.156 ttl=57 id=26382 icmp_seq=33 rtt=475.8 ms
len=46 ip=104.198.111.156 ttl=57 id=26602 icmp_seq=34 rtt=272.1 ms
len=46 ip=104.198.111.156 ttl=57 id=26699 icmp_seq=35 rtt=227.1 ms
len=46 ip=104.198.111.156 ttl=57 id=26843 icmp_seq=36 rtt=354.4 ms
len=46 ip=104.198.111.156 ttl=57 id=27066 icmp_seq=37 rtt=313.6 ms
len=46 ip=104.198.111.156 ttl=57 id=27192 icmp_seq=38 rtt=272.7 ms
len=46 ip=104.198.111.156 ttl=57 id=27270 icmp_seq=39 rtt=235.5 ms
len=46 ip=104.198.111.156 ttl=57 id=27474 icmp_seq=40 rtt=239.1 ms
len=46 ip=104.198.111.156 ttl=57 id=27479 icmp_seq=41 rtt=234.4 ms
len=46 ip=104.198.111.156 ttl=57 id=27712 icmp_seq=42 rtt=233.0 ms
len=46 ip=104.198.111.156 ttl=57 id=27747 icmp_seq=43 rtt=390.6 ms
len=46 ip=104.198.111.156 ttl=57 id=27860 icmp_seq=44 rtt=360.3 ms
len=46 ip=104.198.111.156 ttl=57 id=28020 icmp_seq=45 rtt=315.6 ms
len=46 ip=104.198.111.156 ttl=57 id=28111 icmp_seq=46 rtt=269.7 ms
len=46 ip=104.198.111.156 ttl=57 id=28232 icmp_seq=47 rtt=232.8 ms
```

Fig 2.3.2 : Using hping3 command

2.3.2. SNMP Scans

Here by Using onesixtyone, SNMP scans,SNMP-CHECK were conducted to gain information. Our target ip address did't have the 161 port open ,so we won't get the out put as we expected.

```
└─# snmp-check 104.198.111.156
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 104.198.111.156:161 using SNMPv1 and community 'public'

[!] 104.198.111.156:161 SNMP request timeout
```

Fig 2.3.2 : Using SNMP-CHECK command

```
└─# onesixtyone 104.198.111.156
Scanning 1 hosts, 2 communities
```

Fig 2.3.3 : Using onesixtyone command

2.3.3. Server Identification

By Using tools like httprint, smtpscan, detected servers (HTTP, FTP, SMTP, POP, IMAP, etc) from previous scans are listed and classified by their brand/model/operation systems/version numbers.but here we get the imformation from the outside

Name Servers:	dns1.bigrock.in
	dns2.bigrock.in
	dns3.bigrock.in
	dns4.bigrock.in

Fig 2.3.4 : Server Identification of the target

2.3.4. VPN Identification

By Using the ike-scan, the network was traced for VPN servers.here we also get the information from the other websites.

```
└─# ike-scan 104.198.111.156
Starting ike-scan 1.9.5 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)

Ending ike-scan 1.9.5: 1 hosts scanned in 2.472 seconds (0.40 hosts/sec).  0 returned handshake; 0 returned notify
```

Fig 2.3.5 : Using ike-scan command

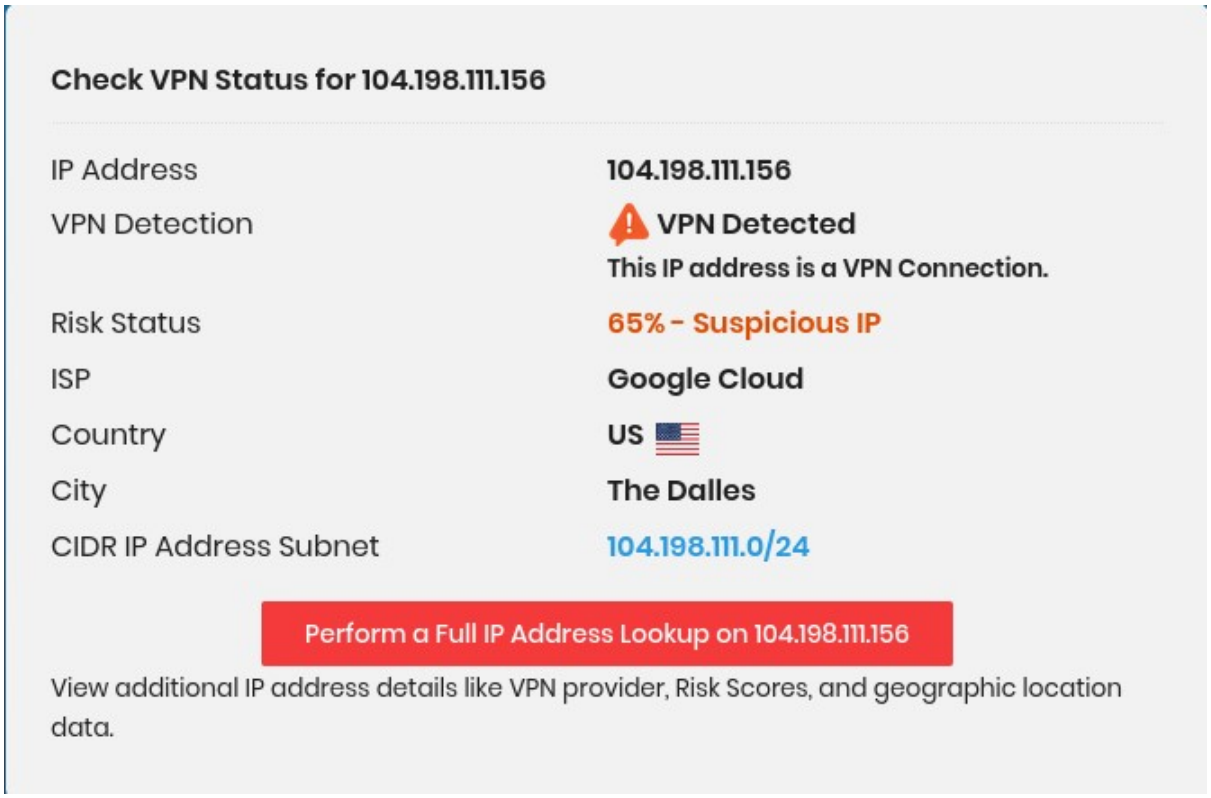


Fig 2.3.5 : VPN Identification

2.4. Vulnerability Analysis

2.4.1. Scanning Target Systems

Using vulnerability scanners like *nessus, acunetix, etc,* target systems were crosschecked with up-to-date vulnerability databases.

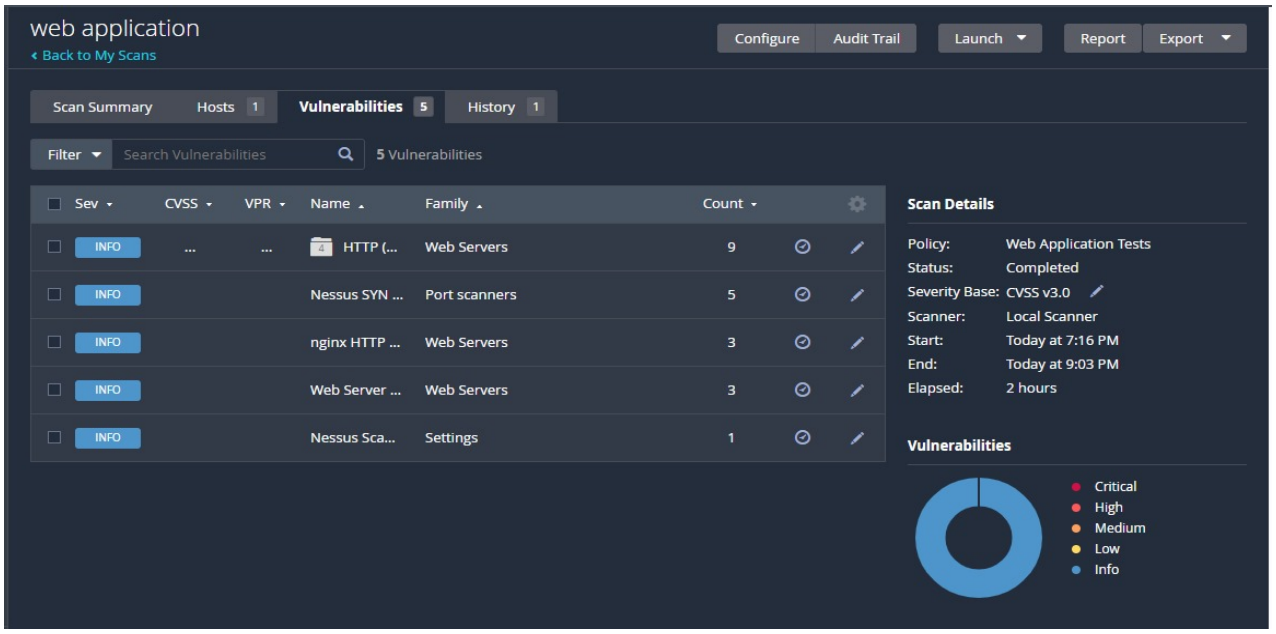


Fig 2.4.1.1: Vulnerabillities of web application on target website.

Navigation:
"Back to My Scans": A link/button allowing users to navigate back to the main page or previous section of the application.

Scan Summary:
Provides an overview of the scan results, including the number of hosts scanned, total vulnerabilities found, and a history of previous scans.

Filter and Search:
Options to filter and search vulnerabilities based on different criteria such as severity, CVSS score, name, etc.

Vulnerabilities Table:
A table displaying detailed information about the vulnerabilities discovered during the scan. This includes the severity level, CVSS score, vulnerability name, family, count, and various actions that can be taken such as configuring, auditing, launching, reporting, or exporting.

Scan Details:
Additional details about the scan process, including the type of scan performed (e.g., HTTP, Nessus SYN), scanned ports, status, policy used, start and end times, duration of the scan, and information about the scanner.

Settings:
Information about the settings used for the scan, such as the type of scanner employed (e.g., local scanner), along with timestamps indicating when the scan was initiated and completed.

Vulnerabilities Breakdown:
A breakdown of vulnerabilities by severity levels, including Critical, High, Medium, Low, and Informational (Info). This section likely provides a quick overview of the distribution of vulnerabilities based on their severity levels.

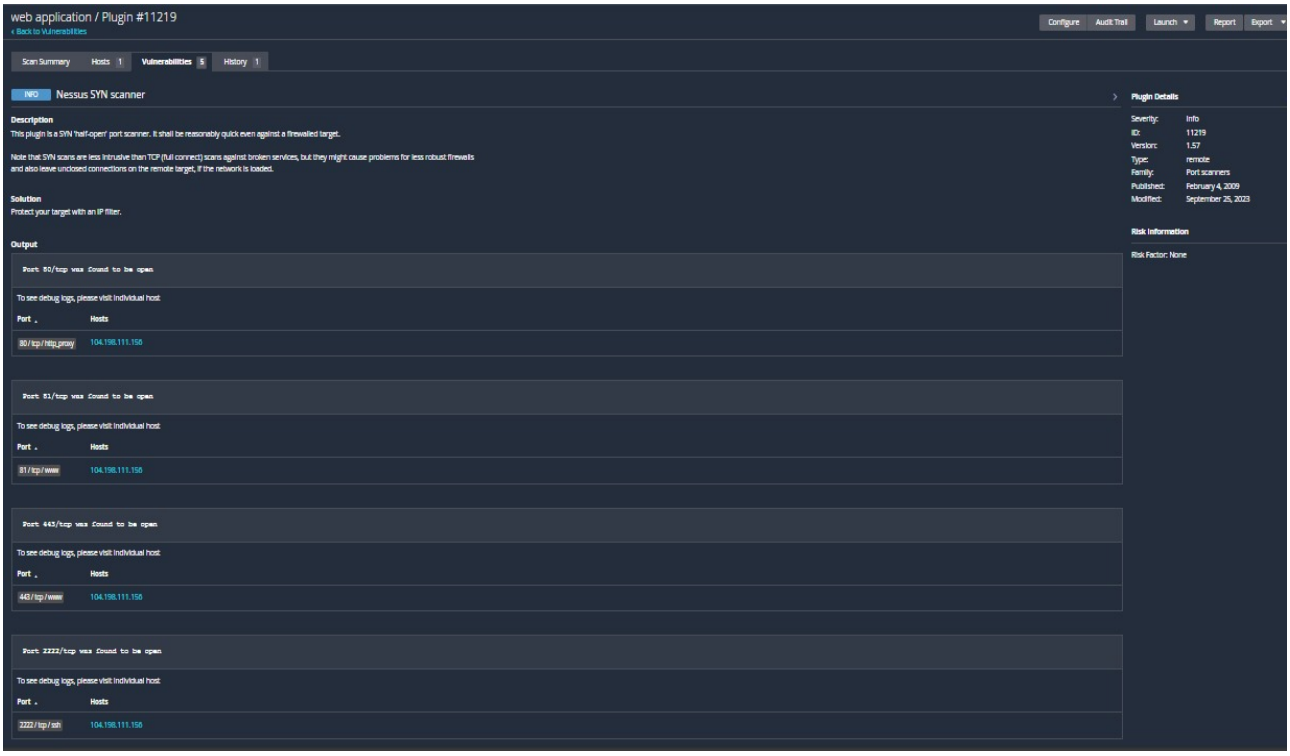


Fig 2.4.1.2: First plugin #11219 vulnarabilitie.

Scan Summary:

Hosts Scanned: 1

Vulnerabilities Found: 5

Plugin Information:

Plugin Name: NEO Nessus SYN Scanner

Severity: Information

Version: 1.57

Type: Port scanners

Description: A SYN port scanner designed for quick scans, even against firewalled targets. It emphasizes that SYN scans are less intrusive than TCP scans but may leave unclosed connections on the target if the network is loaded.

Solution:

Recommends protecting targets with an IP filter to mitigate potential risks associated with the SYN scanner.

Plugin Output:

Provides details about the specific hosts and ports scanned by the plugin, along with any findings or observations.

Hosts:

104.196.111.150

Port 80/tcp: Identified as ntp.proxy

Port 181/tcp: Identified as www

Port 443/tcp: Identified as www

Port 2222/tcp: Identified as ssh

Risk Factor:

None

Additional Information:

The report may include timestamps indicating when the scan was initiated and completed, providing context for the scan results.

It might also include options for further analysis, such as viewing debug logs or accessing individual host details.

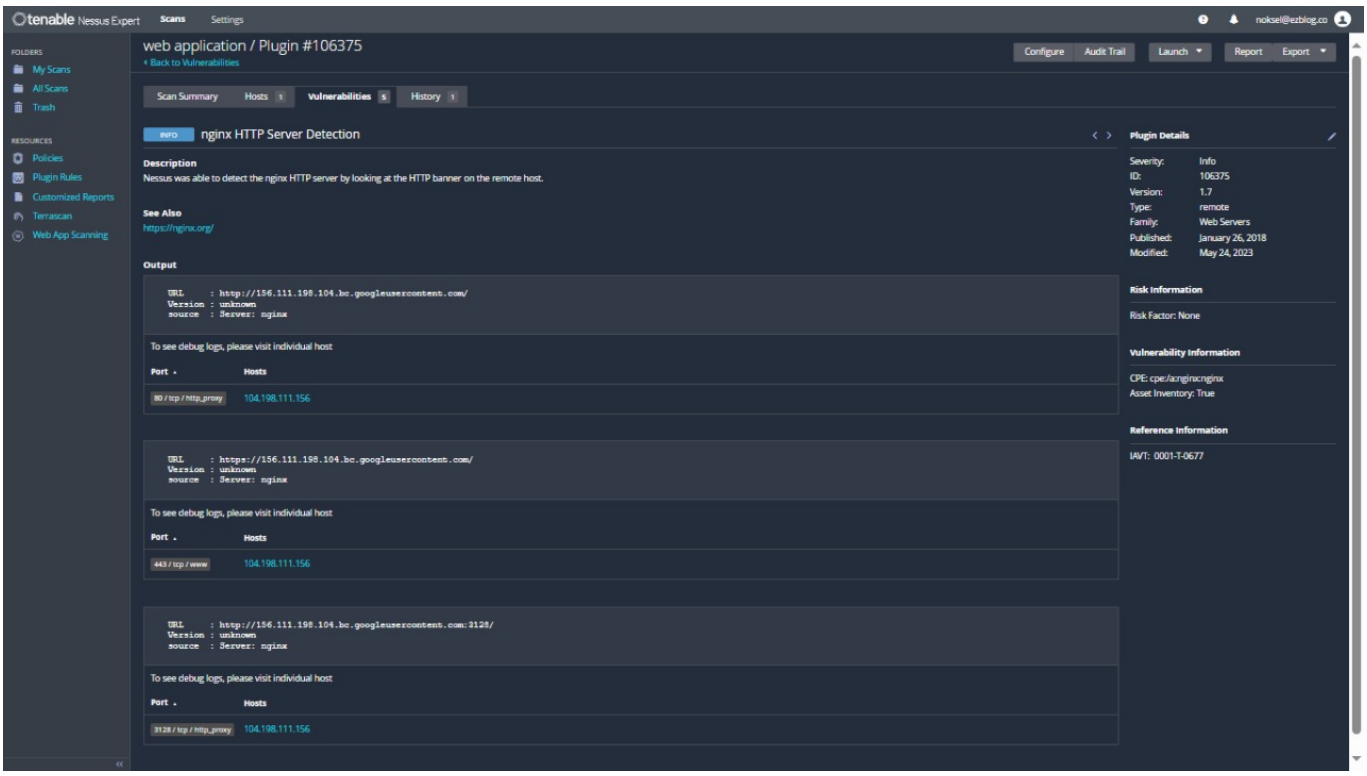


Fig 2.4.1.3: second Plugin #106375 vulnarabilite.

Report Summary:
Plugin Number: 106375
Plugin Name: nginx HTTP Server Detection
Vulnerabilities Identified: 1

Plugin Information:
Description: Nessus detected the nginx HTTP server by examining the HTTP banner on the remote host.

Vulnerability Details:
Detected Server: nginx HTTP Server
Detected Version: Unknown
Additional Information: The server response includes the header "Server: nginx."

Detected Hosts:
Host IP: 104.198.111.156
Detected Port: 80 (HTTP)
Server Response: Server: nginx

Recommendation:
Review the configuration of the nginx HTTP server to ensure proper security measures are in place.
Monitor and update the server regularly to mitigate potential security risks.

Additional Notes:
Further investigation may be required to assess the impact of the detected nginx server on the overall security posture of the web application.
Consider implementing security best practices to protect against potential vulnerabilities associated with the nginx server.

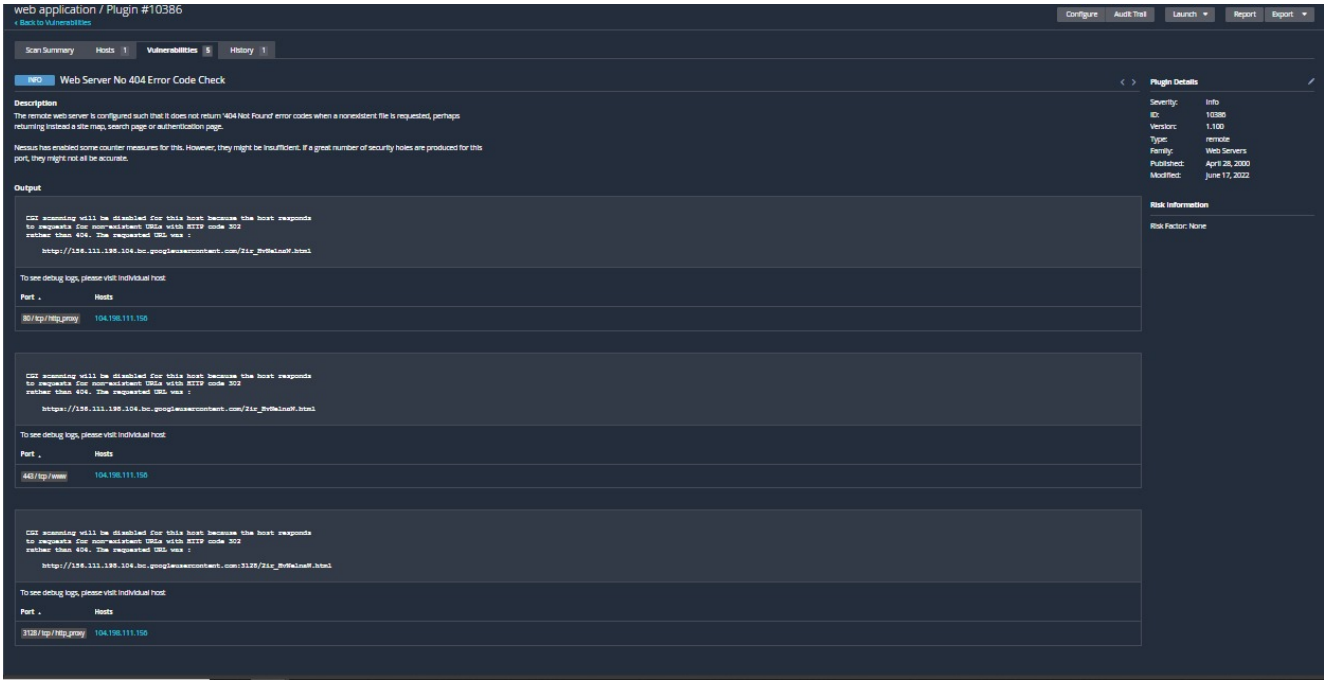


Fig 2.4.1.4: Plugin #10386 vulnarabilite

Report Summary:
Plugin Number: 10386
Plugin Name: Web Server No 404 Error Code Check
Vulnerabilities Identified: 5

Plugin Information:
Description: The remote web server is configured not to return 404 Not Found error codes when a nonexistent file is requested, potentially returning a site map, search page, or authentication page instead. Nessus has enabled some countermeasures for this, but they might be insufficient.

Vulnerability Details:
Severity: Unknown
Version: Unknown
Type: Web Servers

Detected Hosts:
Host IP: 198.112.198.104.bc.g
Port: Unknown
Description: The requested URL was non-existent and returned an HTTP status code of 302 (Redirect) instead of the expected 404 (Not Found) error code.
Host IP: 156.111.196.104.bc.google
Port: Unknown
Description: The requested URL was non-existent and returned an HTTP status code of 302 (Redirect) instead of the expected 404 (Not Found) error code.
Host IP: 104.198.111.155
Port: 443/tcp (HTTPS)
Description: The requested URL was non-existent and returned an HTTP status code of 302 (Redirect) instead of the expected 404 (Not Found) error code.

Host IP: 198.111.138.104.bc.google
Port: 3128 (HTTP Proxy)
Description: The requested URL was non-existent and returned an HTTP status code of 302 (Redirect) instead of the expected 404 (Not Found) error code.

Recommendation:
Review the web server configuration to ensure that it returns the appropriate 404 Not Found error codes for non-existent URLs.
Implement appropriate countermeasures to address the potential security implications of this misconfiguration.

Additional Notes:
Further investigation may be required to assess the impact of the misconfigured web server on the overall security posture of the application.
Consider implementing best practices for web server configuration and error handling to mitigate potential risks associated with non-existent URLs.

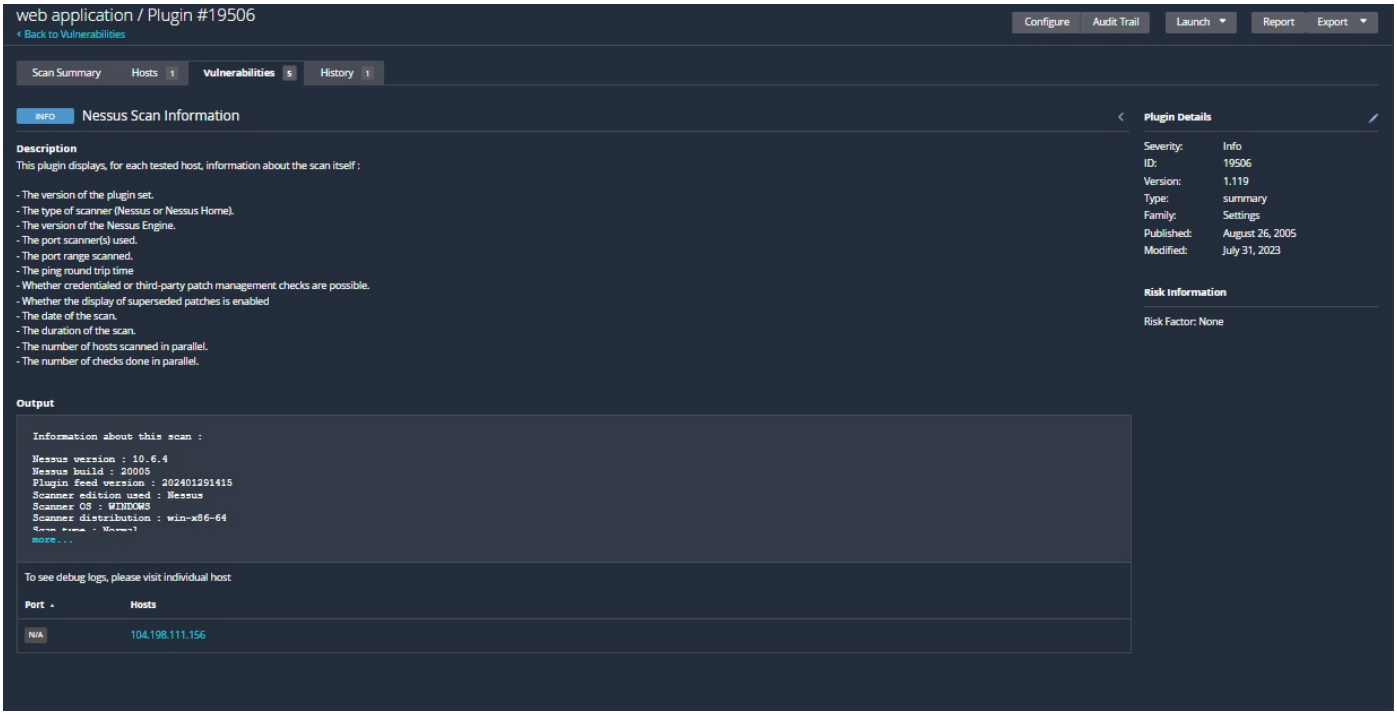


Fig 2.4.1.5 : Plugin #10386 vulnarabilit.

Report Summary:
Plugin Number: 19506
Plugin Name: Nessus Scan Information
Vulnerabilities Identified: N/A (This plugin provides information about the scan itself)

Plugin Information:
Description: This plugin displays detailed information about the scan itself, including the version of the plugin set, the type of scanner used (Nessus or Nessus Home), the version of the Nessus Engine, the port scanner(s) used, the port range scanned, ping round trip time, possibility of credentialed or third-party patch management checks, whether display of superseded patches is enabled, date of the scan, duration

of the scan, number of hosts scanned in parallel, and number of checks done in parallel.
Severity: Informational
Plugin Version: 1.119
Plugin Type: Summary
Family: Settings
Published: August 26, 2005
Modified: July 31, 2023

Scan Information:
Nessus Version: 10.6.4
Nessus Build: 20005
Plugin Feed Version: 202401291415
Scanner Edition Used: Nessus
Scanner OS: Windows
Scanner Distribution: win-x86-64

Risk Information:
Risk Factor: None
Additional Notes:
This plugin provides essential details about the Nessus scan itself, including the version of the scanner, the build information, plugin feed version, and scanner distribution.
The information presented is critical for understanding the context and environment in which the scan was conducted.
No specific vulnerabilities or risks are identified by this plugin; it serves to provide metadata about the scan process itself.

2.4.2. SSL Certificates

SSL certificates used in target systems were scanned to determine the validity of their security.

```
└─# sslscan 104.198.111.156
Version: 2.1.2-static
OpenSSL 3.0.12 24 Oct 2023

Connected to 104.198.111.156

Testing SSL server 104.198.111.156 on port 443 using SNI name 104.198.111.156

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   disabled
TLSv1.1   disabled
TLSv1.2   enabled
TLSv1.3   enabled

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Session renegotiation not supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.3  256 bits  TLS_AES_256_GCM_SHA384        Curve 25519 DHE 253
Accepted  TLSv1.3  256 bits  TLS_CHACHA20_POLY1305_SHA256  Curve 25519 DHE 253
Accepted  TLSv1.3  128 bits  TLS_AES_128_GCM_SHA256        Curve 25519 DHE 253
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-CHACHA20-POLY1305   Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256

  Server Key Exchange Group(s):
TLSv1.3  128 bits  secp256r1 (NIST P-256)
TLSv1.3  192 bits  secp384r1 (NIST P-384)
TLSv1.3  260 bits  secp521r1 (NIST P-521)
TLSv1.3  128 bits  x25519
TLSv1.3  224 bits  x448
TLSv1.2  128 bits  secp256r1 (NIST P-256)
TLSv1.2  192 bits  secp384r1 (NIST P-384)
TLSv1.2  260 bits  secp521r1 (NIST P-521)
TLSv1.2  128 bits  x25519
TLSv1.2  224 bits  x448

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  *.wpengine.com
Altnames: DNS:*.wpengine.com, DNS:wpengine.com
Issuer:   RapidSSL TLS RSA CA G1

Not valid before: Aug  1 00:00:00 2023 GMT
Not valid after:  Aug 28 23:59:59 2024 GMT
```

Fig 2.4.2 : SSL Certificates

CONCLUSION:

The conclusion of the vulnerability assessment report for Navratham Jewllary underscores the critical importance of addressing the identified vulnerabilities and potential security risks. It emphasizes the need for immediate action to remediate the vulnerabilities and strengthen the overall security posture of the organization's systems and network infrastructure. The conclusion likely recommends the implementation of robust security measures, such as patching known vulnerabilities, updating SSL certificates, and enhancing access controls to mitigate potential threats.

Furthermore, the conclusion may stress the significance of conducting regular vulnerability assessments and proactive security measures to prevent unauthorized access, data breaches, and other security incidents. It may also highlight the importance of ongoing monitoring and maintenance to ensure continuous protection against evolving security challenges. Additionally, the conclusion may emphasize the need for employee training and awareness programs to promote a culture of security within the organization.

Overall, the conclusion of the report serves as a call to action, urging the organization to prioritize and invest in comprehensive security measures to safeguard sensitive information, maintain customer trust, and uphold the integrity of its systems and network infrastructure.