# FINDINGS

Below are the findings from the OSINT tools that were run for this project.

First, Whois was used to find :

| Field | Description |
|---|---|
| Domain Name | VBSHILPA.COM |
| Registrar | Network Solutions, LLC |
| Domain Creation Date | 2002-06-19T09:08:07Z |
| Domain Expiry Date | ██████████████ |
| Last Updated Date | ██████████████ |
| Name Servers (NS) | ████████████████████████ ████████████████████████ |
| Registrant Name | Shilpa Medicare Limited |
| Registrant Email | ███████████████ |
| Registrant Address | ████████████████████████████ |
| Registrant Phone | ██████████ |
| Domain Status Codes | ███████████████ |
| DNSSEC Signed (optional) | ████████ |

SubdomainFinderc99 produced the below results:

| Subdomain | Status Code | Status Description | IP Address | Protected by Cloudflare |
|---|---|---|---|---|
| www.vbshilpa.com | 200 | OK (Active) | ██████████████ | |
| ████████████████ | ███ | ██████████ | ██████ ██████████ | ████ |
| ████████████████ | ███ | ██████████ | ██████ ██████████ | ████ |
| ████████████████ | ███ | ██████████ | ██████ ██████████ | ████ |

HaveIBeenPwned GUI was used to look for any breaches on the registrant/admin email that was found with the whois checkup.

| No. | Platform | Breach Date | Records Exposed | Compromised Data |
|---|---|---|---|---|
| 1 | ██████ | Sept 2013 | 5 million | Dates of birth, Email addresses, Names, Passwords, Phone numbers, Physical addresses, PINs |

| | | | | |
|---|---|---|---|---|
| 2 | ▬ | May 2015 | 4.3 million | Email addresses, Genders, IP addresses, Geographic locations, Names, Passwords, Phone numbers, Usernames |
| 3 | ▬▬▬ | Aug 2017 | 711 million | Email addresses, Passwords |
| 4 | ▬ | Jan 2019 | 17 million | Auth tokens, Device information, Email addresses, Genders, Names, Passwords, Phone numbers, Social media profiles, Usernames |
| 5 | ▬▬ | Feb 2019 | 763 million | Dates of birth, Email addresses, Employers, Genders, IP addresses, Job titles, Names, Phone numbers, Physical addresses |
| 6 | ▬ | June 2019 | 3.5 million | Device information, Email addresses, Names, Phone numbers, IP addresses, Geographic locations |
| 7 | ▬▬ | Oct 2020 | 20 million | Dates of birth, Email addresses, IP addresses, Names, Passwords, Phone numbers, Physical addresses |
| 8 | ▬▬ | Jan 2021 (scraped 2023) | 200 million | Email addresses, Names, Social media profiles, Usernames |
| 9 | ▬▬ | Mar 2021 | 22.5 million | Email addresses, Names, Phone numbers, Physical addresses, Purchases |
| 10 | ▬▬ ▬ | Aug 2021 | 28 million | Names, dates of birth, unique email addresses, physical addresses (presumedly corporate locations), phone numbers and job titles. |
| 11 | ▬ | Sept 2021 | 15 million | email addresses, names, phone numbers, physical addresses, purchases and passwords |
| 12 | ▬ | Dec 2023 | 4.7 million | Device information, Email addresses, IP addresses, Names, Passwords, Phone numbers, Physical addresses, Salutations,Support tickets |
| 13 | ▬▬ ▬▬ | Feb 2024 | 122 million | email addresses, physical addresses, phone numbers, employers, job titles, names and for many individuals, a link to their LinkedIn profile. |

Lastly, the following technology information was gathered from whatweb about the domain:

| Category | Technology / Detail | Version |
|---|---|---|
| Web Server | ▬▬ | - |
| Programming Language | ▬ | ▬ |

| CMS | ███████ ████████ █ ██ ███ | |
|---|---|---|
| JavaScript Framework | ████ | ███████ |
| SSL/TLS Info | ██████████ | - |
| IP Address | █████████ | - |
| Redirection | █████████████████ | - |
| Cookies Detected | ███ | - |
| X-Powered-By | ██████ | - |