SECURITY ASSESSMENT REPORT

Target: vardhaman.org
Date: November 27, 2025
Scan ID: 44

Prepared by Sarral Scan

1. Executive Summary

Sarral Scan performed a comprehensive security assessment of **vardhaman.org** on 2025-11-27. The objective was to identify potential security vulnerabilities and provide recommendations for remediation.

Findings Summary

Severity	Count
Critical	0
High	6
Medium	19
Low	10
Info	4

2. Detailed Findings

1. Exposed cPanel Interface

Severity: HIGH **Tool:** Subfinder

Description:

The presence of 'cpanel.vardhaman.org' indicates a cPanel interface is publicly accessible. This is a high-risk finding as cPanel provides administrative access to the web server. If compromised, an attacker could gain full control of the website and server.

Remediation:

Restrict access to the cPanel interface to a limited set of trusted IP addresses. Implement strong password policies and MFA. Regularly update cPanel to the latest version and monitor for suspicious activity. Consider using a non-standard port for cPanel access.

---

2. Insecure Login Page

Severity: HIGH **Tool:** Subfinder

Description:

The presence of 'login.vardhaman.org' indicates a login page. Without proper security measures (HTTPS, strong password policies, rate limiting, MFA), this page is vulnerable to credential theft and brute-force attacks.

Remediation:

Ensure the login page is served over HTTPS. Implement strong password policies and enforce MFA. Implement rate limiting to prevent brute-force attacks. Regularly monitor login attempts for suspicious activity. Consider using a CAPTCHA to prevent automated attacks.

---

3. Insecure Online Exam Portal

Severity: HIGH **Tool:** Subfinder

Description:

The presence of 'onlineexam.vardhaman.org' indicates an online exam portal. This portal likely handles sensitive student data and exam results. Without proper security measures, this portal is vulnerable to data breaches and unauthorized access.

Remediation:

Ensure the online exam portal is served over HTTPS. Implement strong authentication and authorization mechanisms. Regularly audit the portal for vulnerabilities. Protect student data with encryption. Implement measures to prevent cheating and unauthorized access to exams.

---

4. Potential cPanel Exposure

Severity: HIGH **Tool:** Amass Passive

Description:

The subdomain 'cpanel.vardhaman.org' suggests a publicly accessible cPanel interface. If not properly secured, this could allow attackers to gain complete control over the web server and associated data. Default credentials or outdated cPanel versions are common vulnerabilities.

Remediation:

Restrict access to the cPanel interface to authorized IP addresses only. Ensure cPanel is up-to-date with the latest security patches. Change the default cPanel port and disable unnecessary features. Implement strong authentication and regularly audit access logs.

---

5. Exposed cPanel Interface

Severity: HIGH **Tool:** Assetfinder

Description:

The subdomain 'cpanel.vardhaman.org' indicates a publicly accessible cPanel interface. This is a significant security risk as cPanel provides administrative access to the web server. If not properly secured, it could allow attackers to gain complete control of the website and server.

Remediation:

Restrict access to the cPanel interface to a limited set of trusted IP addresses. Enforce strong password policies and multi-factor authentication (MFA). Ensure cPanel is running the latest version with all security patches applied. Regularly monitor logs for suspicious activity. Consider moving cPanel

to a non-standard port.

6. Origin Server Exposure via Direct Access

Severity: HIGH **Tool:** Nmap Top 1000

Description:

If the origin server is directly accessible (e.g., through a misconfigured DNS record or a known IP address), attackers could bypass Cloudflare's protection and directly target the origin server's vulnerabilities. The multiple IP addresses listed in the Nmap output (even though not scanned) increase the attack surface.

Remediation:

Restrict access to the origin server to only Cloudflare's IP ranges. Implement strong authentication and authorization on the origin server. Regularly audit DNS records to prevent accidental exposure of the origin server's IP address. Consider using a private network for communication between Cloudflare and the origin server.

7. Registrar Concentration Risk

Severity: MEDIUM **Tool:** Whois

Description:

The domain is registered with a single registrar, PDR Ltd. d/b/a PublicDomainRegistry.com. If this registrar experiences a security breach or goes offline, it could impact the domain's management and availability.

Remediation:

Consider diversifying registrar services or implementing robust account security measures with the current registrar, including multi-factor authentication.

8. DNSSEC Not Enabled

Severity: MEDIUM **Tool:** Whois

Description:

DNSSEC is not enabled for the domain. This makes the domain vulnerable to DNS spoofing and cache poisoning attacks, where attackers can redirect users to malicious websites.

Remediation:

Enable DNSSEC for the domain through the DNS provider (Cloudflare). This will cryptographically sign DNS records, ensuring their authenticity.

9. Potential Origin Server Exposure

Severity: MEDIUM **Tool:** NSLookup

Description:

The domain vardhaman.org resolves to Cloudflare IP addresses (172.67.157.215, 104.21.8.203, 2606:4700:3037::6815:8cb, 2606:4700:3032::ac43:9dd7). If the origin server's IP address is also publicly accessible, attackers could bypass Cloudflare's protection and directly target the origin server, potentially leading to denial-of-service attacks, data breaches, or other malicious activities.

Remediation:

Verify that the origin server's IP address is not publicly exposed. Implement strict firewall rules on the origin server to only allow traffic from Cloudflare's IP ranges. Consider using Cloudflare's Argo Tunnel to create an encrypted tunnel between the origin server and Cloudflare, further hiding the origin server's IP address. Regularly audit DNS records to ensure no accidental exposure of the origin server IP.

10. Exposed Webmail Interface

Severity: MEDIUM **Tool:** Subfinder

Description:

The presence of 'webmail.vardhaman.org' indicates a webmail interface is publicly accessible. If not properly secured, this could be a target for brute-force attacks, credential stuffing, or exploitation of vulnerabilities in the webmail software.

Remediation:

Implement strong password policies, multi-factor authentication (MFA), and regularly update the webmail software to the latest version. Monitor login attempts for suspicious activity. Consider limiting access to the webmail interface to specific IP ranges if possible.

11. Exposed Webdisk Interface

Severity: MEDIUM **Tool:** Subfinder

Description:

The presence of 'webdisk.vardhaman.org' indicates a webdisk interface is publicly accessible. This could allow unauthorized access to files stored on the server if not properly secured.

Remediation:

Implement strong authentication and authorization mechanisms for the webdisk interface. Regularly audit the files stored on the webdisk to ensure no sensitive information is exposed. Update the webdisk software to the latest version.

12. Exposed Webmail Interface

Severity: MEDIUM **Tool:** Amass Passive

Description:

The subdomain 'webmail.vardhaman.org' suggests a publicly accessible webmail interface. If not properly secured and regularly updated, it could be vulnerable to brute-force attacks, credential stuffing, or exploits targeting known vulnerabilities in the webmail software.

Remediation:

Ensure the webmail software is up-to-date with the latest security patches. Implement strong password policies and multi-factor authentication. Regularly audit access logs for suspicious activity. Consider limiting access to the webmail interface to specific IP ranges or VPN connections.

13. Exposed Login Portal

Severity: MEDIUM **Tool:** Amass Passive

Description:

The subdomain 'login.vardhaman.org' indicates a publicly accessible login portal. This is a prime target for credential-based attacks. Weak password policies or vulnerabilities in the login mechanism could lead to unauthorized access.

Remediation:

Implement strong password policies, multi-factor authentication, and rate limiting on login attempts. Regularly audit the login portal for vulnerabilities and ensure it is protected against common web attacks such as SQL injection and cross-site scripting (XSS).

---

14. FTP Server Exposure

Severity: MEDIUM **Tool:** Amass Passive

Description:

The subdomain 'ftp.vardhaman.org' indicates a publicly accessible FTP server. If not properly configured, it could allow anonymous access or be vulnerable to brute-force attacks. Sensitive data stored on the FTP server could be compromised.

Remediation:

Disable anonymous FTP access. Implement strong password policies and consider using SFTP (SSH File Transfer Protocol) or FTPS (FTP Secure) instead of plain FTP. Regularly audit the FTP server for vulnerabilities and ensure it is protected against brute-force attacks.

---

15. Outdated or Unsecured Online Exam Platform

Severity: MEDIUM **Tool:** Amass Passive

Description:

The subdomains 'www.onlineexam.vardhaman.org' and 'onlineexam.vardhaman.org' suggest an online exam platform. If the platform is outdated or not properly secured, it could be vulnerable to cheating, data breaches, or denial-of-service attacks.

Remediation:

Ensure the online exam platform is up-to-date with the latest security patches. Implement strong authentication and authorization mechanisms. Protect against common web attacks such as SQL injection and cross-site scripting (XSS). Regularly audit the platform for vulnerabilities and monitor for suspicious activity.

16. Exposed Webmail Interface

Severity: MEDIUM **Tool:** Assetfinder

Description:

The subdomain 'webmail.vardhaman.org' likely hosts a webmail interface. If not properly secured with strong authentication and up-to-date software, it could be vulnerable to brute-force attacks, credential stuffing, or exploits targeting the webmail software itself, potentially leading to email compromise.

Remediation:

Ensure the webmail interface is running the latest version of the software with all security patches applied. Enforce strong password policies, implement multi-factor authentication (MFA), and regularly monitor logs for suspicious activity. Consider rate limiting login attempts to prevent brute-force attacks.

17. Exposed Login Interface

Severity: MEDIUM **Tool:** Assetfinder

Description:

The subdomain 'login.vardhaman.org' suggests a dedicated login portal. Similar to the webmail interface, this is a prime target for credential-based attacks. Weaknesses in the authentication mechanism or the underlying application could lead to unauthorized access.

Remediation:

Implement strong password policies, enforce multi-factor authentication (MFA), and regularly monitor logs for suspicious activity. Ensure the login portal is protected against common web application vulnerabilities such as SQL injection and cross-site scripting (XSS). Consider rate limiting login attempts to prevent brute-force attacks.

18. Potential Subdomain Takeover (cdn.vardhaman.org)

Severity: MEDIUM **Tool:** Assetfinder

Description:

The subdomain 'cdn.vardhaman.org' suggests the use of a Content Delivery Network (CDN). If the CDN configuration is not properly managed (e.g., the DNS record points to a CDN provider but the CDN service is not properly configured or has expired), an attacker could potentially claim the subdomain and serve malicious content.

Remediation:

Verify that the CDN configuration for 'cdn.vardhaman.org' is properly configured and actively managed. Ensure the DNS record points to the correct CDN endpoint and that the CDN service is properly configured to serve content from the vardhaman.org domain. Regularly monitor the CDN configuration for any changes or misconfigurations.

---

19. Potential Subdomain Takeover (go.vardhaman.org)

Severity: MEDIUM **Tool:** Assetfinder

Description:

The subdomain 'go.vardhaman.org' suggests the use of a URL shortener or redirection service. If the service is not properly managed or configured, an attacker could potentially claim the subdomain and redirect users to malicious websites.

Remediation:

Verify that the URL shortener or redirection service configuration for 'go.vardhaman.org' is properly configured and actively managed. Ensure the DNS record points to the correct service endpoint and that the service is properly configured to redirect to valid and trusted URLs. Regularly monitor the service configuration for any changes or misconfigurations.

---

20. Email Address Exposure

Severity: MEDIUM **Tool:** WebScraperRecon

Description:

The scan identified a significant number of email addresses associated with the domain. This information can be used by attackers for targeted phishing campaigns, spamming, or social engineering attacks.

Remediation:

Implement measures to protect email addresses from being easily scraped, such as using CAPTCHAs or obfuscation techniques on web pages. Educate employees about phishing and social engineering tactics.

---

21. Missing HSTS Header

Severity: MEDIUM **Tool:** WebScraperRecon

Description:

The absence of the HTTP Strict Transport Security (HSTS) header allows attackers to perform man-in-the-middle attacks by downgrading HTTPS connections to HTTP.

Remediation:

Configure the web server to send the HSTS header with a long max-age value (e.g., one year) and include subdomains. Consider preloading HSTS to further enhance security.

---

22. Missing Content Security Policy (CSP) Header

Severity: MEDIUM **Tool:** WebScraperRecon

Description:

The lack of a Content Security Policy (CSP) header makes the website vulnerable to cross-site scripting (XSS) attacks by allowing the execution of malicious scripts from untrusted sources.

Remediation:

Implement a strict CSP header that whitelists only trusted sources for scripts, styles, images, and other resources. Regularly review and update the CSP to ensure it remains effective.

---

23. WordPress Vulnerabilities

Severity: MEDIUM **Tool:** WebScraperRecon

Description:

The website is running on WordPress, which is a popular target for attackers. Outdated WordPress core, themes, or plugins can contain known vulnerabilities that can be exploited to compromise the website.

Remediation:

Regularly update WordPress core, themes, and plugins to the latest versions to patch any known security vulnerabilities. Implement a web application firewall (WAF) to protect against common WordPress attacks. Use strong passwords for all WordPress user accounts.

24. Potential Cloudflare Misconfiguration or Vulnerability

Severity: MEDIUM **Tool:** Nmap Top 1000

Description:

While Cloudflare provides security benefits, misconfigurations or undiscovered vulnerabilities within their infrastructure could expose the target domain. This includes issues like improper WAF rules, vulnerable Cloudflare apps, or weaknesses in their proxy implementation.

Remediation:

Regularly review Cloudflare's security advisories and apply necessary updates. Ensure proper configuration of Cloudflare's WAF, DDoS protection, and other security features. Conduct periodic security assessments of the Cloudflare setup.

25. 415 Unsupported Media Type Error

Severity: MEDIUM **Tool:** WhatWeb

Description:

The server is consistently returning a 415 Unsupported Media Type error. This indicates that the server is unable to process the request due to an unsupported content type. This could be due to a misconfiguration in the server's content negotiation settings or a lack of support for the requested

media type.

Remediation:

Investigate the server's configuration to ensure it supports the expected content types. Review the application logs for more detailed error messages. Ensure that the client is sending requests with a supported Content-Type header. Check Cloudflare's configuration for any rules that might be interfering with content negotiation.

26. Potential CDN Misconfiguration

Severity: LOW **Tool:** Subfinder

Description:

The presence of 'cdn.vardhaman.org' indicates the use of a Content Delivery Network (CDN). Misconfiguration of the CDN could lead to sensitive data being cached and exposed.

Remediation:

Review the CDN configuration to ensure that sensitive data is not being cached. Implement proper cache control headers. Regularly audit the CDN logs for suspicious activity.

27. NPTEL subdomain security

Severity: LOW **Tool:** Subfinder

Description:

The presence of 'nptel.vardhaman.org' and 'www.nptel.vardhaman.org' indicates the use of NPTEL resources. It's important to ensure these subdomains are properly secured and configured to prevent unauthorized access or modification of content.

Remediation:

Review the NPTEL subdomain configuration to ensure proper access controls and security measures are in place. Regularly update the NPTEL resources to the latest versions. Monitor the subdomains for suspicious activity.

28. Content Delivery Network (CDN) Misconfiguration

Severity: LOW **Tool:** Amass Passive

Description:

The subdomain 'cdn.vardhaman.org' indicates the use of a Content Delivery Network. Misconfiguration of the CDN could lead to unauthorized access to cached content or denial-of-service attacks.

Remediation:

Review the CDN configuration to ensure it is properly secured. Restrict access to the CDN management interface to authorized personnel only. Regularly monitor the CDN for suspicious activity.

---

29. Information Disclosure via 'webdisk.vardhaman.org'

Severity: LOW **Tool:** Amass Passive

Description:

The subdomain 'webdisk.vardhaman.org' suggests a web-based file sharing service. Improper configuration could lead to unintended information disclosure or unauthorized access to files.

Remediation:

Review the webdisk configuration to ensure proper access controls are in place. Regularly audit the webdisk for vulnerabilities and monitor for suspicious activity. Implement strong authentication and authorization mechanisms.

---

30. Information Disclosure via Webdisk

Severity: LOW **Tool:** Assetfinder

Description:

The subdomain 'webdisk.vardhaman.org' suggests a web-based file storage or sharing service. If not properly secured, it could inadvertently expose sensitive information to unauthorized users.

Remediation:

Ensure that the webdisk service is properly configured with appropriate access controls and permissions. Regularly audit the files stored on the webdisk to ensure that sensitive information is not being inadvertently exposed. Consider implementing data loss prevention (DLP) measures to prevent the accidental sharing of sensitive information.

31. Phone Number Exposure

Severity: LOW **Tool:** WebScraperRecon

Description:

The scan identified a large number of phone numbers. While many appear to be false positives (dates), some may be legitimate. Exposed phone numbers can be used for spam calls, SMS phishing (smishing), or social engineering attacks.

Remediation:

Review the list of phone numbers and remove any that are no longer valid or necessary. Implement measures to prevent phone numbers from being easily scraped from the website. Educate staff about social engineering tactics that may involve phone calls.

32. Missing X-Frame-Options Header

Severity: LOW **Tool:** WebScraperRecon

Description:

The absence of the X-Frame-Options header makes the website susceptible to clickjacking attacks, where attackers can trick users into performing unintended actions by embedding the website in a malicious frame.

Remediation:

Configure the web server to send the X-Frame-Options header with the value 'DENY' or 'SAMEORIGIN' to prevent the website from being framed by unauthorized domains.

33. Exposed API Endpoints

Severity: LOW **Tool:** WebScraperRecon

Description:

The scan identified several API endpoints. While not inherently vulnerable, these endpoints should be carefully reviewed to ensure they are properly secured and do not expose sensitive data or functionality without proper authentication and authorization.

Remediation:

Review all identified API endpoints to ensure they are properly secured with appropriate authentication and authorization mechanisms. Implement rate limiting to prevent abuse. Regularly monitor API traffic for suspicious activity.

34. X-XSS-Protection Header Missing

Severity: LOW **Tool:** WebScraperRecon

Description:

The X-XSS-Protection header, while deprecated, can provide a basic level of protection against reflected XSS attacks in older browsers. Its absence might slightly increase the risk of such attacks.

Remediation:

While CSP is the preferred method, consider adding the X-XSS-Protection header with the value '1; mode=block' for compatibility with older browsers. Focus primarily on implementing a strong CSP.

35. Non-Standard Ports (8080, 8443) Usage

Severity: LOW **Tool:** Nmap Top 1000

Description:

The presence of HTTP/HTTPS services on non-standard ports (8080 and 8443) might indicate misconfiguration or the presence of legacy applications. These ports could be overlooked during security audits and potentially expose vulnerable services.

Remediation:

Investigate the purpose of the services running on ports 8080 and 8443. Ensure they are properly secured and configured. If these ports are not necessary, consider disabling them. If they are necessary, ensure they are behind Cloudflare's protection and follow security best practices.

36. Abuse Contact Information

Severity: INFO **Tool:** Whois

Description:

The abuse contact email and phone number are generic to the registrar. While standard, it can sometimes delay or complicate reporting specific abuse related to the domain itself.

Remediation:

Ensure the registrar's abuse contact mechanisms are responsive and that internal procedures are in place to handle abuse reports effectively. Regularly monitor for potential abuse of the domain.

37. Client Transfer Prohibited Status

Severity: INFO **Tool:** Whois

Description:

The domain has 'clientTransferProhibited' status. While this prevents unauthorized transfers, it could also hinder legitimate transfers if needed quickly. This is not a vulnerability, but a configuration setting to be aware of.

Remediation:

Document the process for removing the 'clientTransferProhibited' status if a legitimate transfer is required in the future. Ensure authorized personnel are aware of this setting.

38. Uncommon Headers

Severity: INFO **Tool:** WhatWeb

Description:

The presence of uncommon headers like 'nel', 'cf-cache-status', 'report-to', 'cf-ray', and 'alt-svc' requires further investigation. While not inherently vulnerabilities, understanding their purpose and configuration is crucial for security posture.

Remediation:

Research the purpose of each uncommon header. Verify that they are configured correctly and securely. Ensure that they are not exposing sensitive information or creating unintended security risks. Consult Cloudflare documentation for details on their specific headers.

---

39. Presence of Cloudflare WAF

Severity: INFO **Tool:** WafW00f

Description:

The website is behind Cloudflare's WAF. While not a vulnerability in itself, it indicates a reliance on a third-party security solution. The effectiveness of the WAF depends on its configuration and the underlying application's security posture.

Remediation:

Regularly review and update Cloudflare WAF rules to ensure they are effective against the latest threats. Conduct thorough penetration testing to identify vulnerabilities that the WAF might be masking. Ensure the underlying application is secure and follows secure coding practices.

---

3. Appendix: Raw Tool Output

The following section contains raw output from the security tools used during the assessment.

Tool: Whois

```
Domain Name: vardhaman.org Registry Domain ID: REDACTED Registrar WHOIS Server:
http://whois.publicdomainregistry.com Registrar URL:
http://www.publicdomainregistry.com Updated Date: 2025-01-30T12:46:14Z Creation Date:
2008-04-24T13:24:44Z Registry Expiry Date: 2034-04-24T13:24:44Z Registrar: PDR Ltd.
d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Registrar Abuse Contact Email:
abuse@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 Domain
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name
Server: owen.ns.cloudflare.com Name Server: riya.ns.cloudflare.com DNSSEC: unsigned URL
of the ICANN Whois Inaccuracy Complaint Form: https://icann.org/wicf/ >>> Last update of
WHOIS database: 2025-11-27T07:28:12Z <<< For more information on Whois status codes,
please visit https://icann.org/epp Terms of Use: Access to Public Interest Registry
WHOIS information is provided to assist persons in determining the contents of a domain
name registration record in the Public Interest Registry registry database. The data in
this record is provided by Public Interest Registry for informational purposes only, and
Public Interest Registry does not guarantee its accuracy. This service is intended only
for query-based access. You agree that you will use this data only for lawful purposes
and that, under no circumstances will you use this data to (a) allow, enable, or
otherwise support the transmission by e-mail, telephone, or facsimile of mass
unsolicited, commercial advertising or solicitations to entities other than the data
recipient's own existing customers; or (b) enable high volume, automated, electronic
processes that send queries or data to the systems of Registry Operator, a Registrar, or
Identity Digital except as reasonably necessary to register domain names or modify
existing registrations. All rights reserved. Public Interest Registry reserves the
right to modify these terms at any time. By submitting this query, you agree to abide by
this policy. The Registrar of Record identified in this output may have an RDDS service
that can be queried for additional information on how to contact the Registrant, Admin,
or Tech contact of the queried domain name.
```

Tool: NSLookup

```
Server: 10.77.145.30 Address: 10.77.145.30#53 Non-authoritative answer: Name:
vardhaman.org Address: 172.67.157.215 Name: vardhaman.org Address: 104.21.8.203 Name:
vardhaman.org Address: 2606:4700:3037::6815:8cb Name: vardhaman.org Address:
2606:4700:3032::ac43:9dd7
```

Tool: Subfinder

```
__ _____ __ _______ __/ /_ / __(_)___ ____/ /__ _____ / ___/ / / / __ \/ /_/ / __ \/ __
/ _ \/ ___/ (__ ) /_/ / /_/ / __/ / / / /_/ / __/ / /____/\__,_/_.___/_/ /_/_/
/_/\__,_/\___/_/ projectdiscovery.io [INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for vardhaman.org nptel.vardhaman.org [INF] Found 25
subdomains for vardhaman.org in 3 seconds 875 milliseconds www.vardhaman.org
alumni.vardhaman.org cpanel.vardhaman.org iic.vardhaman.org
www.onlineexam.vardhaman.org ece.vardhaman.org login.vardhaman.org
webdisk.vardhaman.org www.nptel.vardhaman.org cpcontacts.vardhaman.org
csd.vardhaman.org go.vardhaman.org onlineexam.vardhaman.org
```

```
studentscorner.vardhaman.org vardhaman.org cdn.vardhaman.org csm.vardhaman.org
inf.vardhaman.org mail.vardhaman.org faculty.vardhaman.org webmail.vardhaman.org
cpcalendars.vardhaman.org cse.vardhaman.org sac.vardhaman.org
```

Tool: Amass Passive

```
login.vardhaman.org studentscorner.vardhaman.org courses.vardhaman.org
grievance.redressal.vardhaman.org webmail.vardhaman.org conferences.vardhaman.org
events.vardhaman.org assets.vardhaman.org ieee.vardhaman.org e-cell.vardhaman.org
nptel.vardhaman.org csd.vardhaman.org ece.vardhaman.org cdc.vardhaman.org
acm.vardhaman.org sac.vardhaman.org results.vardhaman.org cpcontacts.vardhaman.org
onlineexam.vardhaman.org csm.vardhaman.org iic.vardhaman.org
video-lectures.vardhaman.org inf.vardhaman.org www.vardhaman.org fdp.vardhaman.org
ceta.vardhaman.org mun.vardhaman.org erp.vardhaman.org mail.vardhaman.org
student.vardhaman.org epics.vardhaman.org www.onlineexam.vardhaman.org
resources.vardhaman.org cdn.vardhaman.org pat.vardhaman.org ftp.vardhaman.org
cpcalendars.vardhaman.org www.nptel.vardhaman.org webdisk.vardhaman.org
faculty.vardhaman.org go.vardhaman.org alumni.vardhaman.org rice2016.vardhaman.org
cpanel.vardhaman.org cse.vardhaman.org ortus.vardhaman.org vardhaman.org
ipr.vardhaman.org The enumeration has finished Discoveries are being migrated into the
local database
```

Tool: Assetfinder

```
vardhaman.org www.vardhaman.org conferences.vardhaman.org alumni.vardhaman.org
cdn.vardhaman.org cpanel.vardhaman.org cpcalendars.vardhaman.org
cpcontacts.vardhaman.org csd.vardhaman.org cse.vardhaman.org csm.vardhaman.org
ece.vardhaman.org faculty.vardhaman.org go.vardhaman.org iic.vardhaman.org
inf.vardhaman.org login.vardhaman.org mail.vardhaman.org nptel.vardhaman.org
onlineexam.vardhaman.org studentscorner.vardhaman.org webmail.vardhaman.org
vardhaman.org vardhaman.org csd.vardhaman.org vardhaman.org www.vardhaman.org
sac.vardhaman.org cse.vardhaman.org inf.vardhaman.org csm.vardhaman.org
ece.vardhaman.org iic.vardhaman.org vardhaman.org www.vardhaman.org csd.vardhaman.org
csm.vardhaman.org ece.vardhaman.org vardhaman.org www.vardhaman.org csd.vardhaman.org
cse.vardhaman.org csm.vardhaman.org ece.vardhaman.org inf.vardhaman.org
cpanel.vardhaman.org cpcalendars.vardhaman.org cpcontacts.vardhaman.org
webdisk.vardhaman.org webmail.vardhaman.org cpanel.vardhaman.org
cpcalendars.vardhaman.org cpcontacts.vardhaman.org mail.vardhaman.org vardhaman.org
webdisk.vardhaman.org webmail.vardhaman.org www.vardhaman.org nptel.vardhaman.org
www.nptel.vardhaman.org onlineexam.vardhaman.org www.onlineexam.vardhaman.org
cpanel.vardhaman.org mail.vardhaman.org vardhaman.org webdisk.vardhaman.org
webmail.vardhaman.org www.vardhaman.org cpanel.vardhaman.org vardhaman.org
webdisk.vardhaman.org webmail.vardhaman.org www.vardhaman.org
```

Tool: WebScraperRecon


```
{"target": "vardhaman.org", "base_url": "https://vardhaman.org", "alive": true,
"pages_visited": 550, "max_depth": 2, "emails": ["anvesh@vardhaman.org",
"asif_eee@vardhaman.org", "c.satyakumar@vardhaman.org", "dia@vardhaman.org",
"dmr@vardhaman.org", "drchandrasekharb@vardhaman.org", "fatimaunnisa@vardhaman.org",
"gadagammathanmai22ec@student.vardhaman.org", "girishkumar1595@vardhaman.org",
"gopalsoma8@gmail.com", "gpavanisuresh@gmail.com", "hemasri2708@gmail.com",
"info@Vardhaman.org", "info@vardhaman.org", "jagjivan.sports@vardhaman.org",
"k.santoshreddy@vardhaman.org", "madhuyvt@gmail.com",
"manish.srivastava@vardhaman.org", "manish.srivastava@yahoo.com",
```

```
"mr.pvreddy@vardhaman.org", "nareshece84@vardhaman.org", "ncc@vardhaman.org",
"pandirallapallirajeswarareddy@gmail.com", "pat@vardhaman.org",
"placements@vardhaman.org", "principal@vardhaman.org", "rphaniv@vardhaman.org",
"s.srinivas@vardhaman.org", "sho-shbad-cyb@tspolice.gov.in",
"suneetha1689@vardhaman.org", "swapna1365@vardhaman.org", "v.kavitha@vardhaman.org",
"vivek@vardhaman.org"], "phones": ["+91 80961 99891", "+91 8688901557", "+91 90070
77333", "+91 97030 20192", "+918341110307", "+918688901557", "0 0 1280 650", "0 0 16
16", "0 0 1600 1063", "0 0 3796 893", "0001-1086", "0001-1448", "000905090646071",
"0075435447515", "01-07-2015", "01-07-2018", "01-07-2021", "01-07-2023", "0128314068",
"02-11-2019", "029487-300", "029487-768", "03352231272", "06-01-2015", "06302734222",
"070008012", "07776669636", "08-05-2020", "084928388818", "09-01-2017", "09-04-2016",
"09-05-2021", "09-07-2016", "09681928488818", "1-10-1300", "1-12-1300", "1-15-1300",
"101915191656170", "102017652252", "102631223438313", "11-12-2021", "1160937130799",
"13-11-2022", "130546346", "14-03-2020", "14-06-2017", "145415081", "15-04-2012",
"1506055016", "151574675", "16-04-2009", "16-07-2018", "1613041285537",
"1613044960140", "1613121836128", "1613374292939", "1613390912301", "1613450540117",
"1613469422785", "1613554049779", "1613969388461-2", "1613969388468-10",
"1613979166401", "1614089588643", "1614089705139", "1614402272533", "1614402939672",
"1621592504687", "1621592522135", "1621592535420", "1621592553193", "1621595029698",
"1621595875094", "1621598498306", "1621598597816", "1621598674165", "1621598686297",
"1621654725562", "1623319674456", "1623478519444", "1623478536138", "1623728733110",
"1623729846877", "1623729864268", "1623847745446", "1623996586459", "1624008814470",
"1624019575510", "1624019590569", "1624019642822", "1624019657180", "1624019874893",
"1624019887559", "1624020311296", "1624020327471", "1624020477347", "1624020491664",
"1624281187779", "1624281220486", "1624353353954", "1624353367894", "1625889136416",
"1629353151650", "1629888902362", "1632129652974", "1632129711754",
"1635324830777-10-0", "1653538893889-11-5", "1659338395839", "1659338696993",
"1659338949541", "1672648186871", "1672648205830", "1683367083750",
"1688724792204-12-10", "1697525393438", "1698566473895", "1699084839663", "17-06-2015",
"17-06-2019", "1700109658119", "17122102216926", "1719986963117", "1728289709750",
"1729158381971", "1729158414201", "1740804584919", "1749528558556-5-10",
"1760417701283", "1760417733337", "1763464544495", "1764154780", "1764154934",
"1764154940", "1764154943", "1764154948", "1764154956", "1764154975", "1764155270",
"1764155281", "1764155304", "1764155308", "1764156044", "1764156511", "1764156533",
"1764156607", "1764156632", "1764156635", "1764156638", "1764156759", "1764156767",
"1764173865", "1764177921", "1764188458", "1764192283", "18790839599909",
"19780938589808", "2-1-1-300", "201341983", "2014-2015", "2015-2016", "2016-2017",
"201601120408010", "2017-2018", "2018-2019", "2018-2021", "2018-2025", "2019-2020",
"2019-2021", "2020-06-20", "2020-06-22", "2020-12-11", "2020-2021", "2021-01-12",
"2021-01-19", "2021-08-19", "2021-2022", "2022-2023", "2023-06-05", "2023-2024",
"2023-2026", "2024-06-07", "2024-2025", "2025-11-26 16", "2025-11-26 17", "2025-11-26
21", "2025-11-26 22", "2025-11-27 01", "2025-11-27 02", "2025-2026", "20250315144704",
"207349792-1", "22-05-2022", "2205789828089", "23-07-2023", "23-12-2023", "242588953",
"25010201196926", "26-4775-9905-352", "2613388376", "272868293421", "2781243-300",
"28-11-2015", "29-01-2023", "29-06-2021", "29-11-2017", "30-05-2018", "30-06-2018",
"30-06-2021", "30-06-2024", "30-06-2026", "333333333333", "3343524773455241575",
"335551550", "335551620", "335559685", "335559739", "335559740", "34683630342322223",
"35768993645", "3658555576405744525", "3691134178", "370604780", "3898284898",
"3958291878", "4-4761-82", "4044287-58", "4058544704000", "4159554674425546505",
"464149406", "464909485540", "49414867514655434", "505955595616574", "515854585717564",
"516770637579707", "54585055175", "5462544350464", "564958554", "56545801795",
"565919584550", "575818594451", "59515877415645535", "606965696626677", "62-8470-3864",
"62544350464", "627470667566756263637", "6301176577", "6446727576696",
"656328616970286", " ...[Truncated]
```


Tool: Nmap Top 1000

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 02:31 EST Nmap scan report for
vardhaman.org (104.21.8.203) Host is up (0.079s latency). Other addresses for
vardhaman.org (not scanned): 2606:4700:3032::ac43:9dd7 2606:4700:3037::6815:8cb
172.67.157.215 Not shown: 996 filtered tcp ports (no-response) PORT STATE SERVICE
```

```
VERSION 80/tcp open http Cloudflare http proxy 443/tcp open ssl/http Cloudflare http
proxy 8080/tcp open http Cloudflare http proxy 8443/tcp open ssl/http Cloudflare http
proxy Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 51.91 seconds
```

Tool: WhatWeb

```
http://vardhaman.org [415 Unsupported Media Type] Country[RESERVED][ZZ],
HTTPServer[cloudflare], IP[172.67.157.215], Script, Title[415 Unsupported Media Type],
UncommonHeaders[nel,cf-cache-status,report-to,cf-ray,alt-svc] https://vardhaman.org
[415 Unsupported Media Type] Country[UNITED STATES][US], HTTPServer[cloudflare],
IP[104.21.8.203], Script, Title[415 Unsupported Media Type],
UncommonHeaders[cf-cache-status,nel,report-to,cf-ray,alt-svc]
```

Tool: WafW00f

```
? ,. ( . ) . " __ ?? (" ) )' ,' ) . (` '` (___()'`; ??? .; ) ' (( (" ) ;(, (( ( ;) " )")
/,___ /` _"., ,._'_.,)_(..,( . )_ _' )_') (. _..( ' ) \\ \\
|____|____|____|____|____|____|____|____|____| ~ WAFW00F : v2.3.1 ~ ~ Sniffing Web
Application Firewalls since 2014 ~ [*] Checking https://vardhaman.org [+] The site
https://vardhaman.org is behind Cloudflare (Cloudflare Inc.) WAF. [~] Number of
requests: 2
```

Tool: HTTPx

```
__ __ __ _ __ / /_ / /_/ /_____ | |/ / / __ \/ __/ __/ __ \| / / / / / /_/ /_/ /_/ / |
/_/ /_/\__/\__/ .___/_/|_| /_/ v1.1.5 projectdiscovery.io Use with caution. You are
responsible for your actions. Developers assume no liability and are not responsible for
any misuse or damage. [System] Command timed out.
```