SECURITY ASSESSMENT REPORT

Target: vardhaman.org
Date: November 27, 2025
Scan ID: 48

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	4
Medium	19
Low	8
Info	6

2. Detailed Findings

1. Exposed cPanel Interface

Severity: HIGH

Tool: Subfinder

Description:

The subdomain 'cpanel.vardhaman.org' exposes the cPanel interface. If not properly secured with strong authentication and up-to-date software, it could be vulnerable to brute-force attacks or exploits targeting cPanel vulnerabilities, potentially leading to full server compromise.

Remediation:

Ensure cPanel is running the latest version with all security patches applied. Enforce strong password policies and consider implementing two-factor authentication. Restrict access to cPanel based on IP address if possible.

2. Exposed cPanel Subdomain

Severity: HIGH

Tool: Amass Passive

Description:

The subdomain 'cpanel.vardhaman.org' is exposed. cPanel is a web hosting control panel, and direct access to it can allow attackers to manage the server, potentially leading to complete compromise.

Remediation:

Restrict access to the cPanel interface to authorized IP addresses only. Implement strong authentication mechanisms, including multi-factor authentication. Ensure cPanel is running the latest version with all security patches applied. Consider using a non-standard port for cPanel access.

3. Exposed cPanel Interface

Severity: HIGH

Tool: Assetfinder

Description:

The presence of 'cpanel.vardhaman.org' indicates a publicly accessible cPanel interface. If not properly secured with strong authentication and access controls, it could be vulnerable to brute-force attacks, credential stuffing, or exploitation of known cPanel vulnerabilities, potentially leading to full server compromise.

Remediation:

Implement strong multi-factor authentication for all cPanel accounts. Restrict access to cPanel to a limited set of trusted IP addresses. Regularly update cPanel to the latest version to patch known vulnerabilities. Consider using a non-standard port for cPanel access and implementing rate limiting to prevent brute-force attacks.

4. Potentially Vulnerable Online Exam Platform

Severity: HIGH **Tool:** Assetfinder

Description:

The 'onlineexam.vardhaman.org' and 'www.onlineexam.vardhaman.org' subdomains indicate an online exam platform. This platform is a high-value target for attackers, as it may contain sensitive student data and exam content. Vulnerabilities in the platform could allow attackers to gain unauthorized access to this data, manipulate exam results, or disrupt the exam process.

Remediation:

Conduct a thorough security audit and penetration test of the online exam platform. Implement strong authentication and access controls. Encrypt all sensitive data. Regularly update the platform to the latest version. Implement security measures to prevent cheating and plagiarism.

5. Registrar Concentration Risk

Severity: MEDIUM **Tool:** Whois

Description:

The domain is registered with PDR Ltd. d/b/a PublicDomainRegistry.com. While not inherently a vulnerability, relying solely on one registrar introduces a single point of failure. If the registrar experiences issues (e.g., security breach, service outage), it could impact the domain's availability.

Remediation:

Consider diversifying domain registration across multiple reputable registrars for redundancy. Implement strong account security measures with the current registrar, including multi-factor authentication.

6. Reliance on Cloudflare DNS

Severity: MEDIUM

Tool: Whois

Description:

The domain uses Cloudflare's DNS servers (owen.ns.cloudflare.com and riya.ns.cloudflare.com). While Cloudflare is a reputable provider, dependence on a single DNS provider introduces a potential single point of failure. A Cloudflare outage or compromise could impact domain resolution.

Remediation:

Consider using a secondary DNS provider for redundancy. Implement DNSSEC to protect against DNS spoofing and cache poisoning attacks, although the current record shows it is unsigned.

7. Unsigned DNSSEC

Severity: MEDIUM

Tool: Whois

Description:

The DNSSEC field is 'unsigned', indicating that DNSSEC is not enabled for this domain. DNSSEC helps prevent DNS spoofing and cache poisoning attacks by digitally signing DNS records.

Remediation:

Implement DNSSEC by generating DNSSEC keys and configuring them with both the domain registrar and the DNS provider (Cloudflare). This will add a layer of trust and integrity to the DNS records.

8. Exposed Webmail Interface

Severity: MEDIUM

Tool: Subfinder

Description:

The subdomain 'webmail.vardhaman.org' exposes the webmail interface. Vulnerabilities in the webmail software or weak user credentials could allow attackers to gain access to email accounts, potentially leading to data breaches or phishing attacks.

Remediation:

Ensure the webmail software is running the latest version with all security patches applied. Enforce strong password policies and consider implementing two-factor authentication. Regularly audit user accounts and disable inactive accounts.

9. Exposed Webdisk Interface

Severity: MEDIUM **Tool:** Subfinder

Description:

The subdomain 'webdisk.vardhaman.org' exposes the webdisk interface. If not properly secured, it could allow unauthorized access to files stored on the server, potentially leading to data breaches.

Remediation:

Ensure the webdisk software is running the latest version with all security patches applied. Enforce strong authentication and access controls. Regularly audit file permissions and user access.

10. Exposed Mail Server

Severity: MEDIUM **Tool:** Subfinder

Description:

The subdomain 'mail.vardhaman.org' likely points to a mail server. Misconfigured mail servers can be vulnerable to relay attacks, spamming, or information disclosure.

Remediation:

Ensure the mail server is properly configured with strong authentication and anti-spam measures. Regularly monitor mail server logs for suspicious activity. Implement SPF, DKIM, and DMARC records to prevent email spoofing.

11. Exposed Login Page

Severity: MEDIUM **Tool:** Subfinder

Description:

The subdomain 'login.vardhaman.org' exposes a login page. If not properly secured with strong authentication and protection against brute-force attacks, it could be vulnerable to credential stuffing or password cracking.

Remediation:

Implement strong password policies and multi-factor authentication. Implement rate limiting and account lockout mechanisms to prevent brute-force attacks. Ensure the login page is protected against common web vulnerabilities such as cross-site scripting (XSS) and SQL injection.

12. Potentially Vulnerable Online Exam Platform

Severity: MEDIUM **Tool:** Subfinder

Description:

The subdomain 'onlineexam.vardhaman.org' suggests an online exam platform. If not properly secured, it could be vulnerable to cheating, data breaches, or unauthorized access to exam content.

Remediation:

Ensure the online exam platform is running the latest version with all security patches applied. Implement strong authentication and access controls. Regularly audit the platform for vulnerabilities and implement measures to prevent cheating.

13. Exposed Webmail Subdomain

Severity: MEDIUM **Tool:** Amass Passive

Description:

The subdomain 'webmail.vardhaman.org' is exposed. This provides a direct entry point for attackers to attempt to gain access to user email accounts through brute-force attacks or exploiting vulnerabilities in the webmail software.

Remediation:

Implement strong password policies and multi-factor authentication for all email accounts. Regularly update the webmail software to the latest version with security patches. Monitor for suspicious login attempts and implement account lockout policies.

14. Exposed Webdisk Subdomain

Severity: MEDIUM **Tool:** Amass Passive

Description:

The subdomain 'webdisk.vardhaman.org' is exposed. Webdisk allows users to manage files on the server. If not properly secured, it can be exploited to upload malicious files or gain unauthorized access to sensitive data.

Remediation:

Restrict access to the webdisk interface to authorized users only. Implement strong authentication mechanisms. Regularly audit the webdisk for suspicious files. Ensure the webdisk software is running the latest version with all security patches applied.

15. Exposed FTP Subdomain

Severity: MEDIUM **Tool:** Amass Passive

Description:

The subdomain 'ftp.vardhaman.org' is exposed. FTP (File Transfer Protocol) is an insecure protocol if not properly configured. Anonymous FTP access or weak credentials can allow attackers to upload or download files, potentially leading to data breaches or malware infections.

Remediation:

Disable anonymous FTP access. Enforce strong password policies for FTP accounts. Consider using SFTP (Secure FTP) or FTPS (FTP over SSL/TLS) instead of plain FTP. Restrict FTP access to authorized IP addresses only.

16. Online Exam Portal Exposure

Severity: MEDIUM **Tool:** Amass Passive

Description:

The subdomains 'www.onlineexam.vardhaman.org' and 'onlineexam.vardhaman.org' are exposed. These portals likely handle sensitive student data and exam content. Vulnerabilities in the application could lead to data breaches, cheating, or unauthorized access to exam materials.

Remediation:

Conduct a thorough security audit and penetration test of the online exam portal. Implement strong authentication and authorization mechanisms. Encrypt sensitive data both in transit and at rest. Regularly update the application to the latest version with security patches. Implement input validation and output encoding to prevent injection attacks.

17. Exposed Webmail Interface

Severity: MEDIUM **Tool:** Assetfinder

Description:

The 'webmail.vardhaman.org' subdomain suggests a publicly accessible webmail interface. Vulnerabilities in the webmail software or weak user credentials could allow attackers to gain access to sensitive email communications.

Remediation:

Enforce strong password policies and multi-factor authentication for all webmail accounts. Regularly update the webmail software to the latest version. Implement security measures to prevent brute-force attacks and credential stuffing. Consider using a web application firewall (WAF) to protect against common webmail vulnerabilities.

18. Exposed Webdisk Interface

Severity: MEDIUM

Tool: Assetfinder

Description:

The 'webdisk.vardhaman.org' subdomain indicates a publicly accessible webdisk interface. If not properly secured, it could allow unauthorized access to files stored on the server.

Remediation:

Implement strong authentication and access controls for all webdisk accounts. Regularly audit the files stored on the webdisk to ensure that sensitive information is not exposed. Update the webdisk software to the latest version. Consider disabling webdisk if it is not actively used.

19. Insecure Login Page

Severity: MEDIUM

Tool: Assetfinder

Description:

The 'login.vardhaman.org' subdomain suggests a login page that could be vulnerable to various attacks, such as brute-force attacks, credential stuffing, and cross-site scripting (XSS).

Remediation:

Implement strong password policies and multi-factor authentication. Use a web application firewall (WAF) to protect against common web attacks. Implement rate limiting to prevent brute-force attacks. Ensure the login page is protected against XSS vulnerabilities by properly encoding user input.

20. CDN Misconfiguration

Severity: MEDIUM

Tool: Assetfinder

Description:

The 'cdn.vardhaman.org' subdomain indicates the use of a Content Delivery Network (CDN). Misconfiguration of the CDN could lead to sensitive data being exposed or the CDN being used to serve malicious content.

Remediation:

Review the CDN configuration to ensure that it is properly secured. Restrict access to the CDN configuration to authorized personnel. Regularly monitor the CDN for suspicious activity. Ensure that the CDN is configured to properly cache and serve content.

21. Origin Server Exposure (Potential)

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

Description:

While Cloudflare is protecting the target, misconfiguration or vulnerabilities on the origin server could still be exploited if an attacker bypasses Cloudflare. This could occur through direct IP access if the origin server's IP is exposed.

Remediation:

Ensure the origin server's firewall only allows traffic from Cloudflare's IP ranges. Regularly patch and update the origin server's operating system and applications. Implement strong authentication and authorization mechanisms on the origin server.

22. Cloudflare Misconfiguration (Potential)

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

Description:

Incorrectly configured Cloudflare settings can lead to vulnerabilities. For example, weak SSL/TLS configurations, improper caching rules, or insufficient WAF rules could be exploited.

Remediation:

Review Cloudflare's configuration settings, including SSL/TLS settings, caching rules, and WAF rules. Ensure that the most secure and appropriate settings are enabled. Regularly audit Cloudflare's configuration for potential misconfigurations.

23. 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 the format of the request data. This could be due to incorrect Content-Type headers being sent by clients, or a misconfiguration on the server side regarding accepted media types.

Remediation:

1. Investigate server-side configuration to ensure correct handling of expected Content-Types. 2. Review client-side applications to ensure they are sending requests with appropriate Content-Type headers. 3. Check server logs for more detailed error messages to pinpoint the cause. 4. If Cloudflare is caching the error, ensure the origin server is properly configured before purging the cache.

24. NPTEL Subdomain Security

Severity: LOW **Tool:** Subfinder

Description:

The subdomain 'nptel.vardhaman.org' and 'www.nptel.vardhaman.org' are related to the National Programme on Technology Enhanced Learning. If not properly secured, it could be used for phishing or malware distribution, especially if it hosts downloadable content.

Remediation:

Ensure the NPTEL subdomain is properly secured with up-to-date software and strong authentication. Regularly scan the subdomain for malware and phishing attempts. Implement content security policies (CSP) to prevent malicious scripts from running.

25. CDN Misconfiguration

Severity: LOW **Tool:** Subfinder

Description:

The subdomain 'cdn.vardhaman.org' suggests a Content Delivery Network. Misconfigured CDNs can lead to unauthorized access or modification of content, potentially leading to website defacement or malware distribution.

Remediation:

Ensure the CDN is properly configured with strong access controls and caching policies. Regularly audit the CDN configuration for vulnerabilities. Implement measures to prevent unauthorized access or modification of content.

26. Potential Information Disclosure via 'resources' and 'assets' Subdomains

Severity: LOW

Tool: Amass Passive

Description:

The 'resources.vardhaman.org' and 'assets.vardhaman.org' subdomains may contain publicly accessible files that could reveal sensitive information about the organization's infrastructure, configurations, or internal processes.

Remediation:

Review the contents of the 'resources' and 'assets' subdomains to ensure that no sensitive information is publicly accessible. Implement access controls to restrict access to sensitive files. Regularly audit these subdomains for new or updated files that may contain sensitive information.

27. Grievance Redressal Portal Exposure

Severity: LOW

Tool: Amass Passive

Description:

The subdomain 'grievance.redressal.vardhaman.org' is exposed. This portal likely handles sensitive student or employee complaints. Vulnerabilities in the application could lead to data breaches or unauthorized access to personal information.

Remediation:

Conduct a security audit of the grievance redressal portal. Implement strong authentication and authorization mechanisms. Encrypt sensitive data both in transit and at rest. Regularly update the application to the latest version with security patches. Implement input validation and output encoding to prevent injection attacks.

28. Login Page Exposure

Severity: LOW

Tool: Amass Passive

Description:

The subdomain 'login.vardhaman.org' is exposed. This is a common target for brute-force and credential stuffing attacks.

Remediation:

Implement strong password policies and multi-factor authentication. Rate limit login attempts to prevent brute-force attacks. Monitor for suspicious login activity. Ensure the login page is protected against common web vulnerabilities such as cross-site scripting (XSS) and SQL injection.

29. Unsecured 'go' subdomain

Severity: LOW

Tool: Assetfinder

Description:

The 'go.vardhaman.org' subdomain is often used for URL shortening or redirection. If not properly secured, it could be abused by attackers to redirect users to malicious websites or to phish for credentials.

Remediation:

Implement access controls to prevent unauthorized users from creating or modifying redirects. Monitor the 'go' subdomain for suspicious activity. Use a URL shortening service that provides security features, such as malware scanning and phishing detection.

30. Port 8080 and 8443 Exposure

Severity: LOW

Tool: Nmap Top 1000

Description:

Ports 8080 (HTTP) and 8443 (HTTPS) are open and running Cloudflare's proxy. While not inherently vulnerable, their presence should be justified. If these ports are not actively used, they should be closed to reduce the attack surface.

Remediation:

Investigate the purpose of ports 8080 and 8443. If they are not required, close them on the origin server's firewall. If they are required, ensure they are properly secured and monitored.

31. Exposure of Uncommon Headers

Severity: LOW **Tool:** WhatWeb

Description:

The server is exposing uncommon HTTP headers such as 'nel', 'cf-cache-status', 'report-to', 'cf-ray', and 'alt-svc'. While not directly a vulnerability, exposing these headers can provide attackers with information about the underlying infrastructure and potentially aid in reconnaissance.

Remediation:

1. Review the server configuration and Cloudflare settings to determine if these headers are necessary. 2. If the headers are not required, disable or remove them to reduce the information available to potential attackers. 3. Implement a security policy to minimize the exposure of sensitive or unnecessary headers.

32. Client Transfer Prohibited Status

Severity: INFO **Tool:** Whois

Description:

The 'clientTransferProhibited' status prevents unauthorized domain transfers. This is generally a good security practice.

Remediation:

No action needed. This status is a positive security measure. Ensure the domain owner understands the implications of this status and how to remove it if a legitimate transfer is required.

33. Abuse Contact Information

Severity: INFO **Tool:** Whois

Description:

The presence of abuse contact information (email and phone) is a positive indicator, allowing for reporting of potential abuse related to the domain.

Remediation:

Regularly monitor the abuse contact email address for reports of malicious activity associated with the domain. Ensure the contact information is kept up-to-date.

34. Reliance on Third-Party CDN (Cloudflare)

Severity: INFO **Tool:** NSLookup

Description:

The domain vardhaman.org resolves to Cloudflare's IP addresses. While using a CDN like Cloudflare offers benefits such as DDoS protection and performance improvements, it also introduces a dependency on a third-party service. Outages or misconfigurations on Cloudflare's end could impact the availability and security of vardhaman.org.

Remediation:

Implement monitoring to detect Cloudflare outages or performance degradation. Review and understand Cloudflare's security policies and incident response procedures. Consider having a backup plan in case of a prolonged Cloudflare outage, such as a failover to a different CDN or hosting provider.

35. Multiple IPv4 and IPv6 Addresses

Severity: INFO **Tool:** NSLookup

Description:

The domain resolves to multiple IPv4 and IPv6 addresses. This is normal for CDNs and load-balanced services. However, it's important to ensure that all these addresses are legitimate and properly configured. Misconfigured or rogue IP addresses could potentially be used for malicious purposes.

Remediation:

Regularly verify the IP addresses associated with the domain to ensure they are all legitimate and authorized. Monitor for any unexpected changes in the IP address list. Ensure proper IPv6 configuration and security measures are in place.

36. Geographic Discrepancy in IP Addresses

Severity: INFO **Tool:** WhatWeb

Description:

The HTTP and HTTPS versions of the site resolve to different IP addresses, one geolocating to the United States and the other to a 'RESERVED' region. While this is likely due to Cloudflare's distributed network, it warrants further investigation to ensure traffic is being routed as expected and no malicious redirection is occurring.

Remediation:

1. Verify the DNS configuration for vardhaman.org to ensure both HTTP and HTTPS traffic are correctly pointed to Cloudflare's infrastructure. 2. Monitor traffic patterns to detect any anomalies or unexpected redirection. 3. Confirm Cloudflare's configuration is set up to handle traffic appropriately for the intended geographic regions.

37. 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: 2025-11-27T09:42:40Z <<< 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: 2606:4700:3032::ac43:9dd7 Name: vardhaman.org Address:
2606:4700:3037::6815:8cb
```

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 cdn.vardhaman.org [INF] Found 25
subdomains for vardhaman.org in 5 seconds 732 milliseconds go.vardhaman.org
sac.vardhaman.org vardhaman.org nptel.vardhaman.org csd.vardhaman.org ece.vardhaman.org
mail.vardhaman.org webmail.vardhaman.org www.onlineexam.vardhaman.org
alumni.vardhaman.org studentscorner.vardhaman.org cpcalendars.vardhaman.org
www.vardhaman.org www.nptel.vardhaman.org cse.vardhaman.org csm.vardhaman.org
```

```
iic.vardhaman.org inf.vardhaman.org onlineexam.vardhaman.org webdisk.vardhaman.org
cpcontacts.vardhaman.org login.vardhaman.org cpanel.vardhaman.org faculty.vardhaman.org
```

Tool: Amass Passive

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

```
{"www.nptel.vardhaman.org": {"target": "www.nptel.vardhaman.org", "base_url":
"https://www.nptel.vardhaman.org", "alive": false, "pages_visited": 0, "max_depth": 2,
"emails": [], "phones": [], "internal_ips": [], "social_profiles": [], "api_endpoints":
[], "comments": [], "visited_urls": [], "errors": ["[probe]
https://www.nptel.vardhaman.org -> HTTPSConnectionPool(host='www.nptel.vardhaman.org',
port=443): Max retries exceeded with url: / (Caused by NameResolutionError(\": Failed to
resolve 'www.nptel.vardhaman.org' ([Errno -2] Name or service not known)\"))", "[probe]
https://www.nptel.vardhaman.org -> HTTPSConnectionPool(host='www.nptel.vardhaman.org',
port=443): Max retries exceeded with url: / (Caused by NameResolutionError(\": Failed to
resolve 'www.nptel.vardhaman.org' ([Errno -2] Name or service not known)\"))", "[probe]
http://www.nptel.vardhaman.org -> HTTPConnectionPool(host='www.nptel.vardhaman.org',
port=80): Max retries exceeded with url: / (Caused by NameResolutionError(\": Failed to
resolve 'www.nptel.vardhaman.org' ([Errno -2] Name or service not known)\"))"],
"duration_sec": 0.36, "resolved_ips": ["104.21.8.203", "172.67.157.215",
"2606:4700:3032::ac43:9dd7", "2606:4700:3037::6815:8cb"], "http_probe": {}, "tls_info":
{}, "headers": {}, "security_headers": {}, "favicon_hash": {}, "technologies": [],
"waf": "", "http_methods": []}, "results.vardhaman.org": {"target":
"results.vardhaman.org", "base_url": "https://results.vardhaman.org", "alive": true,
"pages_visited": 1, "max_depth": 2, "emails": [], "phones": [], "internal_ips": [],
"social_profiles": [], "api_endpoints": [], "comments": [], "visited_urls":
["https://results.vardhaman.org"], "errors": [], "duration_sec": 2.28, "resolved_ips":
["104.21.8.203", "172.67.157.215", "2606:4700:3032::ac43:9dd7",
"2606:4700:3037::6815:8cb"], "http_probe": {"initial_url":
"https://results.vardhaman.org", "final_url": "https://results.vardhaman.org/",
"status_code": 200, "content_length": 68, "redirect_chain":
["https://results.vardhaman.org/"]}, "tls_info": {"hostname": "results.vardhaman.org",
"issuer": "countryName=US, organizationName=Let's Encrypt, commonName=E7", "subject":
"commonName=vardhaman.org", "not_before": "Oct 13 19:03:48 2025 GMT", "not_after": "Jan
11 19:03:47 2026 GMT", "san": ["*.vardhaman.org", "vardhaman.org"]}, "headers":
{"Date": "Thu, 27 Nov 2025 09:44:11 GMT", "Content-Type": "text/html; charset=UTF-8",
"Transfer-Encoding": "chunked", "Connection": "keep-alive", "Server": "cloudflare",
"X-Powered-By": "PHP/5.6.40", "Expires": "Thu, 19 Nov 1981 08:52:00 GMT",
"Cache-Control": "no-store, no-cache, must-revalidate, post-check=0, pre-check=0",
"Pragma": "no-cache", "Nel":
"{\"report_to\":\"cf-nel\",\"success_fraction\":0.0,\"max_age\":604800}", "Report-To":
"{\"group\":\"cf-nel\",\"max_age\":604800,\"endpoints\":[{\"url\":\"https://a.nel.cloud
flare.com/report/v4?s=aotfTMJu4bXC1miu389MFMmXO%2Fl%2B3q6KOHQkI%2B9AJOMuMUYXVQqTAW%2BZO
MNVovzWjZNbcOTwYtn3cyfdGtljKLyQA9IQrmSyZK2JbX6MJ5hQFBwU0ZYu6%2BUil5d6y7e8Dg%3D%3D\"}]}"
, "cf-cache-status": "DYNAMIC", "Content-Encoding": "zstd", "Set-Cookie":
"PHPSESSID=8245ovn7umkpn97t1j6vik0k32; Path=/", "CF-RAY": "9a50af7b4efb4dab-SIN",
"alt-svc": "h3=\":443\"; ma=86400"}, "security_headers": {"hsts": null, "csp": null,
"x_frame_options": null, "x_content_type_options": null, "referrer_policy": null,
"permissions_policy": null, "x_xss_protection": null}, "favicon_hash": {"url":
"https://results.vardhaman.org/favicon.ico", "md5": "c93e5f629765f3cc2ea4fc8b24e51bbf",
"sha1": "95a64d218a61fa296fa1c17ced3694e8ad22ddbf", "sha256":
"72313863af562ff37aaf5925333a4aa05ec3ba4e40a2e0dfc4534addaf9639fd"}, "technologies":
["PHP"], "waf": "Cloudflare", "http_methods": ["", "TRACE"]}, "ieee.vardhaman.org":
{"target": "ieee.vardhaman.org", "base_url": "https://ieee.vardhaman.org", "alive":
true, "pages_visited": 1, "max_depth": 2, "emails": [], "phones": [], "internal_ips":
[], "social_profiles": [], "api_endpoints": [], "comments": [], "visited_urls":
["https://ieee.vardhaman.org"], "errors": [], "duration_sec": 2.51, "resolved_ips":
["104.21.8.203", "172.67.157.215", "2606:4700:3032::ac43:9dd7",
"2606:4700:3037::6815:8cb"], "http_probe": {"initial_url":
"https://ieee.vardhaman.org", "final_url": "https://ieee.vardhaman.org/",
"status_code": 404, "content_length": 1234, "redirect_chain":
["https://ieee.vardhaman.org/"]}, "tls_info": {"hostname": "ieee.vardhaman.org",
"issuer": "countryName=US, organizationName=Let's Encrypt, commonName=E7", "subject":
"commonName=vardhaman.org", "not_before": "Oct 13 19:03:48 2025 GMT", "not_after": "Jan
11 19:03:47 2026 GMT", "san": ["*.vardhaman.org", "vardhaman.org"]}, "headers":
{"Date": "Thu, 27 Nov 2025 09:44:10 GMT", "Content-Type": "text/html;
charset=us-ascii", "Transfer-Encoding": "chunked", "C ...[Truncated]
```

Tool: Nmap Top 1000

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 04:45 EST Nmap scan report for
vardhaman.org (172.67.157.215) Host is up (0.063s latency). Other addresses for
vardhaman.org (not scanned): 2606:4700:3037::6815:8cb 2606:4700:3032::ac43:9dd7
104.21.8.203 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 27.44 seconds
```

Tool: WhatWeb

```
http://vardhaman.org [415 Unsupported Media Type] Country[UNITED STATES][US],
HTTPServer[cloudflare], IP[104.21.8.203], 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[RESERVED][ZZ], HTTPServer[cloudflare],
IP[172.67.157.215], 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
```