SECURITY ASSESSMENT REPORT

Target: vardhaman.org
Date: November 26, 2025
Scan ID: 30

Prepared by Sarral Scan

1. Executive Summary

Sarral Scan performed a comprehensive security assessment of **vardhaman.org** on 2025-11-26. The objective was to identify potential security vulnerabilities and provide recommendations for remediation.

Findings Summary

Severity	Count
Critical	0
High	5
Medium	11
Low	6
Info	1

2. Detailed Findings

1. Exposed cPanel Subdomain

Severity: HIGH

Tool: Subfinder

Description:

The subdomain 'cpanel.vardhaman.org' is exposed. cPanel is a web hosting control panel, and its exposure could allow attackers to attempt brute-force attacks, exploit known vulnerabilities in cPanel, or gain unauthorized access to server configurations.

Remediation:

Restrict access to the cPanel subdomain to authorized IP addresses only. Ensure cPanel is running the latest version with all security patches applied. Implement strong authentication mechanisms, including multi-factor authentication.

2. Exposed Login Subdomain

Severity: HIGH

Tool: Subfinder

Description:

The subdomain 'login.vardhaman.org' is exposed. This is a prime target for credential stuffing, brute-force attacks, and phishing campaigns. Successful attacks could grant unauthorized access to user accounts and sensitive data.

Remediation:

Implement strong password policies, multi-factor authentication, and rate limiting on login attempts. Monitor login attempts for suspicious activity. Ensure the login page is protected against common web vulnerabilities such as cross-site scripting (XSS) and SQL injection.

3. Exposed cPanel Interface

Severity: HIGH

Tool: Amass Passive

Description:

The subdomain 'cpanel.vardhaman.org' suggests a publicly accessible cPanel interface. If not properly secured with strong authentication and up-to-date software, it could be vulnerable to brute-force attacks, privilege escalation, and other exploits, potentially leading to full server compromise.

Remediation:

Restrict access to the cPanel interface to authorized IP addresses only. Enforce strong password policies and multi-factor authentication. Keep cPanel software updated with the latest security patches. Consider using a non-standard port for cPanel access.

4. Online Exam Platform Vulnerabilities

Severity: HIGH **Tool:** Amass Passive

Description:

The 'onlineexam.vardhaman.org' and 'www.onlineexam.vardhaman.org' subdomains indicate an online exam platform. These platforms often handle sensitive student data and are critical for academic integrity. Vulnerabilities in the platform could lead to unauthorized access to exam questions, manipulation of results, or exposure of student information.

Remediation:

Conduct regular security audits and penetration testing of the online exam platform. Implement strong authentication and authorization mechanisms. Protect against common web application vulnerabilities such as SQL injection and cross-site scripting (XSS). Ensure data is encrypted both in transit and at rest.

5. Unsecured 'login.vardhaman.org'

Severity: HIGH **Tool:** Assetfinder

Description:

The subdomain 'login.vardhaman.org' is a critical entry point. If not properly secured with HTTPS, strong authentication, and protection against common web application vulnerabilities (e.g., SQL injection, XSS), it could be a prime target for attackers to steal user credentials and gain unauthorized access to sensitive systems.

Remediation:

Enforce HTTPS on all login pages. Implement strong password policies and multi-factor authentication. Regularly perform security audits and penetration testing to identify and address vulnerabilities. Implement input validation and output encoding to prevent SQL injection and XSS attacks. Use a Web Application Firewall (WAF) to protect against common web application attacks.

6. Missing DNSSEC

Severity: MEDIUM **Tool:** Whois

Description:

The domain vardhaman.org does not have DNSSEC enabled. This makes the domain vulnerable to DNS spoofing and cache poisoning attacks, where attackers can redirect users to malicious websites by manipulating DNS records.

Remediation:

Implement DNSSEC (Domain Name System Security Extensions) to digitally sign DNS records, ensuring their authenticity and integrity. This will prevent attackers from tampering with DNS responses and redirecting users to malicious sites. Consult with Cloudflare's documentation for enabling DNSSEC.

7. 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.

8. Exposed Webmail Subdomain

Severity: MEDIUM **Tool:** Subfinder

Description:

The subdomain 'webmail.vardhaman.org' is exposed. This allows attackers to target user email accounts through phishing attacks, brute-force attacks, or exploiting vulnerabilities in the webmail software. Compromised email accounts can lead to further access to sensitive information.

Remediation:

Implement strong password policies and multi-factor authentication for all webmail accounts. Keep the webmail software up-to-date with the latest security patches. Implement email security measures such as SPF, DKIM, and DMARC to prevent email spoofing.

9. Exposed Online Exam Subdomain

Severity: MEDIUM **Tool:** Subfinder

Description:

The subdomain 'onlineexam.vardhaman.org' is exposed. This could be a target for cheating, data breaches, or denial-of-service attacks. Vulnerabilities in the online exam platform could allow attackers to manipulate exam results or gain unauthorized access to student data.

Remediation:

Implement robust security measures to prevent cheating and data breaches. Regularly audit the online exam platform for vulnerabilities. Implement access controls to restrict access to exam data. Ensure proper encryption of sensitive data.

10. Webmail Access Vulnerabilities

Severity: MEDIUM **Tool:** Amass Passive

Description:

The 'webmail.vardhaman.org' subdomain indicates a webmail interface. Webmail interfaces are common targets for phishing attacks, credential stuffing, and exploits targeting known vulnerabilities in the webmail software. Outdated webmail software can be a significant risk.

Remediation:

Ensure the webmail software is running the latest version with all security patches applied. Implement strong authentication mechanisms, including multi-factor authentication. Regularly monitor webmail logs for suspicious activity. Educate users about phishing attacks and best practices for password security.

11. Potentially Unsecured FTP Server

Severity: MEDIUM **Tool:** Amass Passive

Description:

The 'ftp.vardhaman.org' subdomain suggests the presence of an FTP server. FTP is an inherently insecure protocol, transmitting data in plaintext. If not properly configured, it could allow unauthorized access to sensitive files.

Remediation:

Disable FTP if not absolutely necessary. If FTP is required, use SFTP (SSH File Transfer Protocol) or FTPS (FTP Secure) instead, which encrypt data in transit. Restrict access to the FTP server to authorized IP addresses only. Enforce strong password policies for FTP accounts.

12. Webdisk Exposure

Severity: MEDIUM **Tool:** Amass Passive

Description:

The 'webdisk.vardhaman.org' subdomain suggests a web-based file storage and sharing service. If not properly secured, it could expose sensitive documents and data to unauthorized access.

Remediation:

Implement strong authentication and authorization controls. Regularly audit user permissions and access logs. Ensure that all files are scanned for malware before being uploaded. Encrypt sensitive data at rest. Keep the webdisk software up to date with the latest security patches.

13. Potential Vulnerabilities in Student Portal ('student.vardhaman.org')

Severity: MEDIUM **Tool:** Amass Passive

Description:

The 'student.vardhaman.org' subdomain likely hosts a student portal, which often contains sensitive personal and academic information. Vulnerabilities in the portal could lead to unauthorized access to student data, modification of records, or other malicious activities.

Remediation:

Conduct regular security audits and penetration testing of the student portal. Implement strong authentication and authorization mechanisms, including multi-factor authentication. Protect against common web application vulnerabilities such as SQL injection and cross-site scripting (XSS). Ensure data is encrypted both in transit and at rest.

14. Exposed cPanel Interface

Severity: MEDIUM **Tool:** Assetfinder

Description:

The subdomain 'cpanel.vardhaman.org' suggests a publicly accessible cPanel interface. If not properly secured with strong authentication and access controls, it could be vulnerable to brute-force attacks or unauthorized access, 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 Web Application Firewall (WAF) to protect against common cPanel exploits.

15. Exposed Webmail Interface

Severity: MEDIUM **Tool:** Assetfinder

Description:

The subdomain 'webmail.vardhaman.org' indicates a publicly accessible webmail interface. Vulnerabilities in the webmail software or weak user credentials could lead to unauthorized access to email accounts, potentially exposing sensitive information.

Remediation:

Enforce strong password policies and multi-factor authentication for all webmail accounts. Regularly update the webmail software to patch known vulnerabilities. Implement rate limiting to prevent brute-force attacks. Monitor webmail logs for suspicious activity.

16. Potential Vulnerabilities in 'onlineexam.vardhaman.org' and 'www.onlineexam.vardhaman.org'

Severity: MEDIUM **Tool:** Assetfinder

Description:

Subdomains related to online exams are potential targets for cheating or data breaches. Vulnerabilities in the exam platform could allow students to gain unauthorized access to exam questions or results. Poor security practices could also expose student data.

Remediation:

Regularly audit the online exam platform for security vulnerabilities. Implement strong authentication and access controls. Encrypt sensitive data at rest and in transit. Monitor exam activity for suspicious behavior. Conduct penetration testing to identify and address vulnerabilities.

17. Reliance on Third-Party Registrar and DNS Provider

Severity: LOW **Tool:** Whois

Description:

The domain relies on PublicDomainRegistry.com for registration and Cloudflare for DNS services. While these are reputable providers, any compromise of their infrastructure could impact the domain.

Remediation:

Implement strong account security measures for both the registrar and DNS provider accounts, including multi-factor authentication. Regularly review the security policies and practices of these providers. Consider diversifying DNS providers for redundancy.

18. Potential Information Disclosure via 'go.vardhaman.org'

Severity: LOW **Tool:** Subfinder

Description:

The subdomain 'go.vardhaman.org' suggests the use of a URL shortener. If not properly secured, this could be used for phishing attacks or to track user activity. It could also potentially leak internal URLs if not configured correctly.

Remediation:

Review the configuration of the URL shortener. Ensure it is not leaking internal URLs. Implement security measures to prevent phishing attacks. Consider restricting access to the URL shortener to authorized users only.

19. Potential CDN Misconfiguration

Severity: LOW **Tool:** Subfinder

Description:

The subdomain 'cdn.vardhaman.org' indicates the use of a Content Delivery Network (CDN). Misconfiguration of the CDN could lead to information disclosure, 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. Regularly audit the CDN configuration for vulnerabilities. Ensure proper caching policies are in place.

20. Information Disclosure via 'results.vardhaman.org'

Severity: LOW **Tool:** Amass Passive

Description:

The 'results.vardhaman.org' subdomain likely hosts student results. Improper access controls or insecure coding practices could lead to unauthorized access to student grades and other sensitive academic information.

Remediation:

Implement robust access controls to ensure that only authorized users can access student results. Sanitize all user input to prevent SQL injection and other attacks. Encrypt sensitive data at rest and in transit. Regularly audit access logs for suspicious activity.

21. Potential Information Disclosure via 'go.vardhaman.org'

Severity: LOW **Tool:** Assetfinder

Description:

The subdomain 'go.vardhaman.org' often indicates a URL shortening service. If not properly secured, it could be used to mask malicious links or reveal internal URLs and directory structures.

Remediation:

Ensure the URL shortening service is properly configured to prevent abuse. Implement logging and monitoring to detect suspicious activity. Regularly review the shortened URLs to identify any malicious or unauthorized content.

22. Insecure CDN Configuration ('cdn.vardhaman.org')

Severity: LOW **Tool:** Assetfinder

Description:

An improperly configured CDN can lead to information disclosure or even allow attackers to serve malicious content. Ensure proper access controls and caching policies are in place.

Remediation:

Verify that the CDN is configured with appropriate access controls to prevent unauthorized access to cached content. Implement secure caching policies to prevent the caching of sensitive data. Regularly review CDN logs for suspicious activity.

23. Long Domain Expiry Date

Severity: INFO **Tool:** Whois

Description:

The domain has a long expiry date (2034). While not a direct vulnerability, a long expiry means that if the domain is compromised, the impact could be felt for a longer period.

Remediation:

Regularly review and update domain registration information and security settings. Implement strong account security measures for the registrar account, including multi-factor authentication. Monitor the domain for any unauthorized changes.

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: 2025-11-26T06:45:24Z <<< 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] Loading provider config from
/home/kali/.config/subfinder/provider-config.yaml [INF] Enumerating subdomains for
vardhaman.org www.vardhaman.org [INF] Found 25 subdomains for vardhaman.org in 30
seconds 3 milliseconds go.vardhaman.org studentscorner.vardhaman.org
webmail.vardhaman.org www.nptel.vardhaman.org www.onlineexam.vardhaman.org
login.vardhaman.org mail.vardhaman.org cpcalendars.vardhaman.org
cpcontacts.vardhaman.org cse.vardhaman.org ece.vardhaman.org alumni.vardhaman.org
csm.vardhaman.org vardhaman.org cpanel.vardhaman.org nptel.vardhaman.org
```

```
csd.vardhaman.org iic.vardhaman.org sac.vardhaman.org webdisk.vardhaman.org
faculty.vardhaman.org inf.vardhaman.org onlineexam.vardhaman.org cdn.vardhaman.org
```

Tool: Amass Passive

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

```
_ __ __ __| | _ __ ___ \ \/ / / _' || '_ \ / __| \ / | (_| || | | |\__ \ / \ \__,_||_|
|_||___//_/\_\ projectdiscovery.io [INF] Current dnsx version 1.1.4 (outdated) [System]
Command timed out.
```