

SECURITY ASSESSMENT REPORT

Target: vardhaman.org
Date: November 26, 2025
Scan ID: 28

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	4
Medium	9
Low	4
Info	2

2. Detailed Findings

1. Login Portal Exposure

Severity: HIGH

Tool: Subfinder

Description:

The subdomain 'login.vardhaman.org' is a critical entry point for user authentication. Vulnerabilities in the login process, such as weak password policies, lack of multi-factor authentication, or susceptibility to brute-force attacks, could compromise user accounts.

Remediation:

Implement strong password policies, enforce multi-factor authentication, and implement account lockout mechanisms to prevent brute-force attacks. Regularly audit the login process for vulnerabilities and ensure the underlying authentication system is secure. Consider using a Web Application Firewall (WAF) to protect against common web attacks.

2. Online Exam Platform Exposure

Severity: HIGH

Tool: Subfinder

Description:

The subdomains 'www.onlineexam.vardhaman.org' and 'onlineexam.vardhaman.org' indicate an online exam platform. Vulnerabilities in this platform could lead to unauthorized access to exam content, student data, or the ability to manipulate exam results.

Remediation:

Conduct a thorough security audit of the online exam platform, including penetration testing. Implement strong access controls and authentication mechanisms. Encrypt sensitive data both in transit and at rest. Regularly update the platform to patch known vulnerabilities. Ensure proper input validation to prevent injection attacks.

3. Insecure Login Portal

Severity: HIGH

Tool: Assetfinder

Description:

The 'login.vardhaman.org' subdomain indicates a login portal. Without proper security measures like HTTPS, strong password policies, and protection against brute-force attacks, it could be vulnerable to credential theft and unauthorized access.

Remediation:

Enforce HTTPS, implement strong password policies (length, complexity, rotation), use multi-factor authentication, implement account lockout policies to prevent brute-force attacks, and regularly audit the login portal for vulnerabilities.

4. Online Exam Portal Vulnerabilities

Severity: HIGH**Tool:** Assetfinder**Description:**

The 'onlineexam.vardhaman.org' subdomain suggests an online examination portal. This portal likely handles sensitive student data and exam results. Vulnerabilities in the portal could lead to data breaches, unauthorized access to exams, or manipulation of results.

Remediation:

Conduct thorough security testing of the online exam portal, including penetration testing and vulnerability scanning. Implement strong authentication and authorization mechanisms. Encrypt sensitive data both in transit and at rest. Regularly audit the portal for vulnerabilities and apply security patches promptly.

5. Single Registrar Dependency

Severity: MEDIUM**Tool:** Whois**Description:**

The domain relies solely on PDR Ltd. d/b/a PublicDomainRegistry.com. A compromise or outage at this registrar could impact the domain's availability and control.

Remediation:

While not always feasible, consider diversifying registrar services if possible, or ensure robust account security measures (MFA, strong passwords) are in place with the current registrar.

6. Absence of DNSSEC

Severity: MEDIUM

Tool: Whois

Description:

DNSSEC is not enabled for the domain. This makes the domain vulnerable to DNS spoofing and cache poisoning attacks, potentially redirecting users to malicious websites.

Remediation:

Implement DNSSEC to digitally sign DNS records, ensuring their authenticity and integrity. This is typically configured through the DNS provider (Cloudflare in this case).

7. Exposed cPanel Interface

Severity: MEDIUM

Tool: Subfinder

Description:

The subdomain 'cpanel.vardhaman.org' is exposed. If not properly secured with strong authentication and access controls, it could allow unauthorized access to server management functionalities.

Remediation:

Implement strong multi-factor authentication for all cPanel accounts. Restrict access to cPanel based on IP address or VPN. Regularly update cPanel to the latest version to patch known vulnerabilities. Consider disabling cPanel access from the public internet if possible, using a VPN for administrative access.

8. Webmail Access Point

Severity: MEDIUM

Tool: Subfinder

Description:

The subdomain 'webmail.vardhaman.org' provides access to the organization's email system. Vulnerabilities in the webmail software or weak user credentials could lead to unauthorized access to sensitive email data.

Remediation:

Ensure the webmail software is up-to-date with the latest security patches. Enforce strong password policies and multi-factor authentication for all email accounts. Regularly audit email access logs for suspicious activity. Implement email security measures such as SPF, DKIM, and DMARC to prevent email spoofing and phishing attacks.

9. Potential Open Redirect (go.vardhaman.org)

Severity: MEDIUM**Tool:** Subfinder**Description:**

The subdomain 'go.vardhaman.org' suggests the presence of a URL shortening or redirection service. If not properly implemented, it could be vulnerable to open redirect attacks, where attackers can redirect users to malicious websites.

Remediation:

Implement strict validation of the target URLs for the redirection service. Ensure that users are warned before being redirected to an external website. Consider using a whitelist of allowed target domains. Regularly monitor the redirection service for suspicious activity.

10. Subdomain Takeover Risk (cdn.vardhaman.org)

Severity: MEDIUM**Tool:** Subfinder**Description:**

The subdomain 'cdn.vardhaman.org' likely points to a Content Delivery Network (CDN). If the CDN configuration is not properly managed, it could be vulnerable to subdomain takeover, where an attacker can claim the subdomain and serve malicious content.

Remediation:

Regularly verify that the CDN configuration is correct and that the subdomain is properly pointed to the CDN provider. Ensure that the CDN provider has implemented appropriate security measures to prevent subdomain takeover. Monitor the subdomain for any unauthorized changes.

11. Exposed cPanel Interface

Severity: MEDIUM

Tool: Assetfinder

Description:

The presence of '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 or exploits targeting cPanel vulnerabilities.

Remediation:

Ensure cPanel is running the latest version, enforce strong password policies, implement two-factor authentication, and restrict access to cPanel to authorized IP addresses only. Consider using a non-standard port for cPanel access.

12. Potentially Vulnerable Webmail Interface

Severity: MEDIUM

Tool: Assetfinder

Description:

The 'webmail.vardhaman.org' subdomain suggests a webmail interface. Outdated or misconfigured webmail software can be a target for attackers. Vulnerabilities in the webmail software could allow attackers to gain access to user email accounts.

Remediation:

Ensure the webmail software is running the latest version with all security patches applied. Implement strong authentication methods, including multi-factor authentication. Regularly audit the webmail server for vulnerabilities.

13. CDN Misconfiguration

Severity: MEDIUM

Tool: Assetfinder

Description:

The 'cdn.vardhaman.org' subdomain indicates a Content Delivery Network. Misconfigurations in the CDN setup could allow attackers to inject malicious content or deface the website.

Remediation:

Ensure the CDN is properly configured with appropriate access controls and security settings. Regularly audit the CDN configuration for vulnerabilities. Implement content integrity checks to prevent unauthorized modifications.

14. Registrar Abuse Contact Information

Severity: LOW

Tool: Whois

Description:

The Whois record includes a registrar abuse contact email and phone number. While standard, it's important to verify the legitimacy of any communications received through these channels to avoid phishing or social engineering attacks.

Remediation:

Educate personnel to verify the authenticity of communications from the registrar before taking any action. Independently verify contact information through the registrar's official website.

15. Potential for DNS Amplification Attacks

Severity: LOW

Tool: NSLookup

Description:

While not directly revealed by this NSLookup output, the use of publicly accessible DNS servers (implied by the 'Non-authoritative answer') can make the domain a potential target for DNS amplification attacks. Attackers can spoof requests to the domain's DNS servers, causing them to send large responses to a victim's IP address.

Remediation:

Ensure DNS servers are properly configured to mitigate DNS amplification attacks. Implement rate limiting and response rate limiting (RRL) on DNS servers. Consider using DNSSEC to authenticate DNS responses.

16. No Domains Found - Potential Information Gathering Failure

Severity: LOW**Tool:** Amass Passive**Description:**

The Amass passive scan failed to identify any domains or subdomains associated with the target. This could indicate a misconfiguration of the scan, an invalid target, or exceptionally strong privacy measures by the target organization. It prevents further vulnerability assessment.

Remediation:

Verify the target domain is correct and accessible. Review the Amass configuration to ensure proper settings and sufficient data sources are enabled. Consider running the scan with increased verbosity for debugging. If the target is intentionally obscuring its infrastructure, consider alternative information gathering techniques.

17. Unsecured 'go' Subdomain

Severity: LOW**Tool:** Assetfinder**Description:**

The 'go.vardhaman.org' subdomain likely hosts URL redirection services. If not properly secured, it could be abused for phishing attacks by redirecting users to malicious websites.

Remediation:

Implement strict access controls and logging for the 'go' subdomain. Regularly monitor the redirection URLs for suspicious activity. Consider using a URL shortening service with built-in security features.

18. Reliance on Cloudflare Nameservers

Severity: INFO

Tool: Whois

Description:

The domain relies on Cloudflare's nameservers. While Cloudflare provides robust infrastructure, a compromise of their services could impact the domain's availability. This is a common practice, but awareness is important.

Remediation:

Monitor Cloudflare's service status and consider implementing secondary DNS services from a different provider for redundancy, although this adds complexity.

19. Reliance on Third-Party CDN (Cloudflare)

Severity: INFO

Tool: NSLookup

Description:

The domain vardhaman.org relies on Cloudflare, a third-party CDN. While CDNs offer performance and security benefits, they also introduce a dependency on the provider's infrastructure and security. A compromise or outage at Cloudflare could impact the availability and security of vardhaman.org.

Remediation:

Implement robust monitoring of Cloudflare's status and performance. Develop a contingency plan for switching to an alternative CDN or origin server in case of a Cloudflare outage or security incident. Review Cloudflare's security policies and compliance certifications regularly.

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: 2025-11-26T04:46:05Z <<< 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 RDNS 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: 104.21.8.203 Name: vardhaman.org Address: 172.67.157.215 Name:
vardhaman.org Address: 2606:4700:3037::6815:8cb Name: vardhaman.org Address:
2606:4700:3032::ac43:9dd7
```

Tool: Subfinder

[illegible]

```
webmail.vardhaman.org cdn.vardhaman.org ece.vardhaman.org go.vardhaman.org
www.onlineexam.vardhaman.org login.vardhaman.org onlineexam.vardhaman.org
www.vardhaman.org
```

Tool: Amass Passive

[illegible]

[illegible]

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

Tool: DNSx

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