SECURITY ASSESSMENT REPORT

Target: vardhaman.org
Date: November 26, 2025
Scan ID: 29

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	0
Medium	4
Low	3
Info	3

2. Detailed Findings

1. 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 by generating DNSSEC keys and configuring the domain's DNS records with the appropriate DS records at the registrar. Consult with Cloudflare's documentation for enabling DNSSEC on their platform.

2. Exposed cPanel Interface

Severity: MEDIUM **Tool:** Subfinder

Description:

The subdomain 'cpanel.vardhaman.org' is exposed. If not properly secured, this could allow unauthorized access to server management functionalities, potentially leading to complete server 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.

3. Exposed Webmail Interface

Severity: MEDIUM **Tool:** Subfinder

Description:

The subdomain 'webmail.vardhaman.org' is exposed. If vulnerable to exploits or brute-force attacks, attackers could gain access to user email accounts, leading to data breaches and phishing campaigns.

Remediation:

Ensure the webmail interface is running the latest version with all security patches applied. Implement strong authentication mechanisms, including multi-factor authentication. Monitor for suspicious login attempts and implement account lockout policies.

4. Potential Vulnerabilities in Online Exam Platform

Severity: MEDIUM

Tool: Subfinder

Description:

The subdomains 'onlineexam.vardhaman.org' and 'www.onlineexam.vardhaman.org' indicate an online exam platform. These platforms are often targets for cheating and data breaches. Vulnerabilities could allow unauthorized access to exam questions, 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 authentication and authorization mechanisms. Protect exam questions and student data with encryption. Regularly monitor the platform for suspicious activity.

5. Reliance on Cloudflare's Nameservers

Severity: LOW

Tool: Whois

Description:

The domain relies on Cloudflare's nameservers. While Cloudflare is a reputable provider, a compromise of Cloudflare's infrastructure could impact the availability and integrity of the domain. This is a general risk associated with using any third-party service.

Remediation:

Implement monitoring to detect any DNS changes or outages. Consider diversifying DNS providers for redundancy, although this adds complexity.

6. Potential Misconfiguration on Webdisk Subdomain

Severity: LOW **Tool:** Subfinder

Description:

The subdomain 'webdisk.vardhaman.org' suggests a web-based file sharing service. If not properly configured, it could allow unauthorized access to sensitive files or allow users to upload malicious content.

Remediation:

Review the configuration of the webdisk service to ensure proper access controls are in place. Implement file upload restrictions and scan uploaded files for malware. Regularly audit the contents of the webdisk for sensitive information.

7. Lack of HTTPS on Subdomains

Severity: LOW **Tool:** Subfinder

Description:

It's possible some of these subdomains are not using HTTPS. This would expose user data transmitted over these subdomains to eavesdropping.

Remediation:

Ensure all subdomains are properly configured to use HTTPS. Enforce HTTPS redirects to prevent users from accessing the HTTP version of the site. Use HSTS to instruct browsers to only access the site over HTTPS.

8. Registrar Abuse Contact Information

Severity: INFO **Tool:** Whois

Description:

The Whois record provides contact information for abuse reports related to the registrar. While not a vulnerability in itself, it's important to be aware of this information for reporting any malicious activity associated with the domain.

Remediation:

No direct mitigation is needed. This information is useful for reporting abuse if necessary.

9. Reliance on Third-Party CDN (Cloudflare)

Severity: INFO

Tool: NSLookup

Description:

The domain vardhaman.org relies on Cloudflare, a third-party Content Delivery Network (CDN). While CDNs offer performance and security benefits, they also introduce a dependency on the CDN 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. Establish a backup plan in case of Cloudflare outages or security incidents. Review Cloudflare's security policies and ensure they align with vardhaman.org's security requirements. Consider diversifying CDN providers for redundancy.

10. Projectdiscovery.io - Potential for Phishing/Spoofing

Severity: INFO

Tool: Subfinder

Description:

The presence of 'projectdiscovery.io' in the domain list, while likely legitimate, should be noted. It's important to ensure that any communication originating from this domain is verified to prevent phishing or spoofing attacks targeting vardhaman.org users.

Remediation:

Educate users about phishing and spoofing attacks. Implement SPF, DKIM, and DMARC records to help prevent email spoofing. Verify the authenticity of any communication originating from projectdiscovery.io before taking action.

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: 2025-11-26T05:25:31Z <<< 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: 104.21.8.203 Name: vardhaman.org Address: 172.67.157.215 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 [INF] Found 25 subdomains for
vardhaman.org in 30 seconds 2 milliseconds csm.vardhaman.org ece.vardhaman.org
iic.vardhaman.org webmail.vardhaman.org sac.vardhaman.org cdn.vardhaman.org
cpcontacts.vardhaman.org go.vardhaman.org mail.vardhaman.org nptel.vardhaman.org
webdisk.vardhaman.org cse.vardhaman.org inf.vardhaman.org login.vardhaman.org
onlineexam.vardhaman.org www.vardhaman.org alumni.vardhaman.org cpanel.vardhaman.org
```

```
csd.vardhaman.org faculty.vardhaman.org cpcalendars.vardhaman.org
studentscorner.vardhaman.org www.onlineexam.vardhaman.org vardhaman.org
www.nptel.vardhaman.org
```

Tool: Amass Passive

```
[System] Command timed out.
```

Tool: Assetfinder

```
```