SARRAL SECURITY

vardhaman.org

Security Assessment Findings Report

Business Confidential

Date: November 28, 2025
Project: SAR-060
Version 1.0

Copyright © Sarral Security

Confidentiality Statement

This document is the exclusive property of the Client and Sarral Security. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Contact Information

Name	Title	Contact Information
Sarral Scan	Automated Scanner	support@sarral.io
Client	Security Team	security@vardhaman.org

Copyright © Sarral Security

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range used throughout the document.

Severity	CVSS V3 Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and data loss.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps.
Low	0.1-3.9	Vulnerabilities are non-exploitable but reduce attack surface.
Informational	N/A	No vulnerability exists. Additional information provided.

Copyright © Sarral Security

Executive Summary

Sarral Security evaluated vardhaman.org's security posture on November 28, 2025. The following sections provide a high-level overview of vulnerabilities discovered.

Testing Summary

The assessment evaluated the target's external network security posture. The team performed vulnerability scanning and reconnaissance to identify potential risks such as exposed services, misconfigurations, and sensitive information disclosure.

Copyright © Sarral Security

Vulnerability Summary & Report Card

1	4	13	15	4
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: CSD Subdomain Hosting Software Activators	Critical	Immediately remove all software activators and related content from csd.vardhaman.org. Conduct a thorough security audit of the server to ensure that it has not been compromised.
SAR-002: Exposed cPanel Interface	High	1. Restrict access to cPanel interfaces to authorized IP addresses only using a firewall. 2. Enforce strong password policies for all cPanel accounts. 3. Implement multi-factor authentication (MFA) fo...
SAR-003: Exposed cPanel Interface	High	1. Restrict access to cpanel.vardhaman.org to a limited set of trusted IP addresses using a firewall. 2. Ensure cPanel is running the latest version with all security patches applied. 3. Enforce stron...
SAR-004: Exposed cPanel Interface	High	1. Ensure cPanel is only accessible via a VPN or whitelisted IP addresses. 2. Enforce strong password policies and multi-factor authentication for all cPanel accounts. 3. Regularly update cPanel to th...
SAR-005: Potentially Vulnerable Online Exam Platform	High	1. Conduct a thorough security audit and penetration test of the online exam platform. 2. Ensure the platform is running the latest version with all security patches applied. 3. Implement strong authe...
SAR-006: Reliance on Third-Party CDN/Security Provider	Medium	Implement robust monitoring of Cloudflare's status and performance. Develop a contingency plan for Cloudflare outages, including potentially routing traffic directly to the origin server (if feasible ...
SAR-007: Vulnerable Webmail Interface	Medium	1. Ensure the webmail software is up-to-date with the latest security patches. 2. Enforce strong password policies for all webmail accounts. 3. Implement multi-factor authentication (MFA) for all webm...
SAR-008: Insecure Online Exam Platform	Medium	1. Conduct a thorough security audit and penetration test of the online exam platform. 2. Implement secure coding practices to prevent common web vulnerabilities such as SQL injection and XSS. 3. Enfo...

Copyright © Sarral Security

SAR-009: Exposed Webmail Interface	Medium	1. Ensure the webmail software is running the latest version with all security patches applied. 2. Enforce strong password policies for all email accounts. 3. Implement two-factor authentication for a...
SAR-010: Exposed FTP Server	Medium	1. Disable FTP entirely if possible and migrate to a more secure protocol like SFTP or FTPS. 2. If FTP is necessary, restrict access to a limited set of trusted IP addresses using a firewall. 3. Enfor...
SAR-011: Potential Vulnerabilities in Online Exam Portal	Medium	1. Conduct a thorough security audit and penetration test of the online exam portal. 2. Ensure the portal is running the latest version of its software with all security patches applied. 3. Implement ...
SAR-012: Exposed Webmail Interface	Medium	1. Ensure the webmail application is running the latest version with all security patches applied. 2. Enforce strong password policies and multi-factor authentication for all email accounts. 3. Implem...
SAR-013: Exposed Webdisk Interface	Medium	1. Ensure the webdisk application is running the latest version with all security patches applied. 2. Enforce strong authentication and access controls for all webdisk accounts. 3. Regularly monitor w...
SAR-014: Mail Server Vulnerabilities	Medium	1. Ensure the mail server software is running the latest version with all security patches applied. 2. Implement strong authentication and access controls. 3. Configure SPF, DKIM, and DMARC records to...
SAR-015: Missing Security Headers	Medium	Implement a consistent set of security headers across all subdomains. Specifically, enable HSTS with a long max-age, configure a strict CSP, set X-Frame-Options to 'DENY' or 'SAMEORIGIN', enable X-Con...
SAR-016: Exposed cPanel and Webmail Login Pages	Medium	Restrict access to cPanel and webmail login pages to specific IP addresses or networks. Implement multi-factor authentication (MFA) for all cPanel and webmail accounts.
SAR-017: Outdated PHP Version	Medium	Upgrade PHP to a supported version (e.g., PHP 8.1 or later) on the affected subdomains. Ensure that all PHP extensions are also updated.
SAR-018: SAC Subdomain Data Exposure	Medium	Review the data stored and displayed on sac.vardhaman.org. Implement measures to protect sensitive information, such as redacting phone numbers or limiting access to social media profiles.

Copyright © Sarral Security

SAR-019: Single Registrar Dependency	Low	Consider diversifying domain registration across multiple registrars for critical services. Implement strong account security measures (e.g., MFA) with the registrar.
SAR-020: Lack of DNSSEC	Low	Implement DNSSEC 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.
SAR-021: Reliance on Cloudflare's Nameservers	Low	Develop a contingency plan for potential Cloudflare outages. This might involve having a secondary DNS provider ready to take over in case of an emergency. Regularly review Cloudflare's security advis...
SAR-022: Potential Information Disclosure	Low	1. Review the subdomain naming convention and consider using more generic or less descriptive names where possible. 2. Educate employees about the risks of social engineering and phishing attacks. 3. ...
SAR-023: Potential Information Disclosure via 'localhost'	Low	1. Investigate the purpose of 'localhost.vardhaman.org'. 2. If it's not needed, remove the DNS record. 3. If it's for internal testing, ensure it's properly isolated and not accessible from the public...
SAR-024: Information Disclosure via Subdomains	Low	1. Review the necessity of each subdomain and consider consolidating services where possible. 2. Ensure that each subdomain has appropriate security measures in place. 3. Regularly monitor subdomains ...
SAR-025: TRACE Method Enabled	Low	Disable the TRACE HTTP method on all web servers. This can typically be done in the server configuration (e.g., Apache, Nginx).
SAR-026: Grievance Redressal SSL Handshake Failure	Low	Review the SSL/TLS configuration of the web server hosting grievance.redressal.vardhaman.org. Ensure that modern SSL/TLS protocols are enabled and that the server's cipher suite is properly configured...
SAR-027: Alumni Portal OTP Login	Low	Review the OTP login implementation to ensure it is secure. Implement rate limiting to prevent brute-force attacks. Consider adding additional security measures, such as CAPTCHA.
SAR-028: Grievance Redressal Cell on Main Domain	Low	Review the grievance redressal cell implementation to ensure it is secure. Implement rate limiting to prevent abuse. Consider adding additional security measures, such as CAPTCHA.

Copyright © Sarral Security

SAR-029: Lack of HSTS on Mail Subdomain	Low	Enable HSTS on the mail.vardhaman.org subdomain with a long max-age and includeSubDomains directive.
SAR-030: SSL Handshake Failure	Low	Review the SSL/TLS configuration of the web server hosting grievance.redressal.vardhaman.org. Ensure that modern SSL/TLS protocols are enabled and that the server's cipher suite is properly configured...
SAR-031: 403 Forbidden on CDN and Assets	Low	Review the access control configuration of cdn.vardhaman.org and assets.vardhaman.org. Ensure that the necessary resources are accessible to the public.
SAR-032: 401 Unauthorized on cpcontacts, cpcalendars, and webdisk	Low	Review the authentication mechanisms for cpcontacts.vardhaman.org, cpcalendars.vardhaman.org, and webdisk.vardhaman.org. Ensure that strong passwords are required and that multi-factor authentication ...
SAR-033: 500 Internal Server Error	Low	Review the server logs for ece.vardhaman.org to identify the cause of the 500 Internal Server Error. Address the underlying issue to restore functionality.
SAR-034: Generic Subdomains - Need Further Investigation	Info	1. Inventory all subdomains and document their purpose and functionality. 2. Conduct vulnerability scans on each subdomain. 3. Ensure each subdomain is properly secured with appropriate authentication...
SAR-035: Name Resolution Errors	Info	Verify the DNS records for www.nptel.vardhaman.org and www.onlineexam.vardhaman.org. Ensure that the A and AAAA records are correctly configured and point to the appropriate IP addresses.
SAR-036: Connection Refused	Info	Investigate the configuration of localhost.vardhaman.org. Ensure that the intended service is running and listening on the correct port. If the subdomain is not needed, consider removing it.
SAR-037: 404 Not Found on Resources	Info	Investigate the configuration of the affected subdomains. Ensure that the necessary resources are present and that the web server is properly configured to serve them. If the subdomains are not needed...

Copyright © Sarral Security

Technical Findings

Finding SAR-001: CSD Subdomain Hosting Software Activators (Critical)

Description:	The csd.vardhaman.org subdomain appears to be hosting links to software activators (e.g., KMSpico). This is a significant security risk, as these activators often contain malware or other malicious software. Hosting such content could damage the reputation of the organization and expose users to security threats.
Risk:	Likelihood: Low Impact: High
System:	vardhaman.org
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Immediately remove all software activators and related content from csd.vardhaman.org. Conduct a thorough security audit of the server to ensure that it has not been compromised.

BUSINESS CONFIDENTIAL
Copyright © Sarral Security

Finding SAR-002: Exposed cPanel Interface (High)

Description:	The subdomains 'cpanel.vardhaman.org', 'cpcalendars.vardhaman.org', and 'cpcontacts.vardhaman.org' suggest publicly accessible cPanel interfaces. If these interfaces are not properly secured with strong authentication and up-to-date software, they could be exploited by attackers to gain unauthorized access to the server and its data. Brute-force attacks, default credentials, and known cPanel vulnerabilities are potential attack vectors.
Risk:	Likelihood: Medium Impact: High
System:	vardhaman.org
Tools Used:	Subfinder
References:	N/A

Remediation

1. Restrict access to cPanel interfaces to authorized IP addresses only using a firewall. 2. Enforce strong password policies for all cPanel accounts. 3. Implement multi-factor authentication (MFA) for all cPanel accounts. 4. Keep cPanel software up-to-date with the latest security patches. 5. Regularly audit cPanel logs for suspicious activity. 6. Consider using a non-standard port for cPanel access.

Copyright © Sarral Security

Finding SAR-003: Exposed cPanel Interface (High)

Description:	The subdomain 'cpanel.vardhaman.org' is exposed. cPanel is a web hosting control panel, and exposing it directly to the internet without proper security measures (like strong authentication, rate limiting, and up-to-date software) can allow attackers to brute-force credentials, exploit vulnerabilities in cPanel itself, or gain unauthorized access to website files and databases.
Risk:	Likelihood: Medium Impact: High
System:	vardhaman.org
Tools Used:	Amass Passive
References:	N/A

Remediation

1. Restrict access to cpanel.vardhaman.org to a limited set of trusted IP addresses using a firewall. 2. Ensure cPanel is running the latest version with all security patches applied. 3. Enforce strong password policies for all cPanel accounts. 4. Implement two-factor authentication for all cPanel accounts. 5. Regularly audit cPanel logs for suspicious activity.

Copyright © Sarral Security

Finding SAR-004: Exposed cPanel Interface (High)

Description:	The subdomain 'cpanel.vardhaman.org' suggests a publicly accessible cPanel interface. If not properly secured with strong authentication and access controls, it could allow unauthorized access to server management functionalities, leading to data breaches, website defacement, and complete server compromise.
Risk:	Likelihood: Medium Impact: High
System:	vardhaman.org
Tools Used:	Assetfinder
References:	N/A

Remediation

1. Ensure cPanel is only accessible via a VPN or whitelisted IP addresses. 2. Enforce strong password policies and multi-factor authentication for all cPanel accounts. 3. Regularly update cPanel to the latest version to patch known vulnerabilities. 4. Implement rate limiting and brute-force protection mechanisms.

Copyright © Sarral Security

Finding SAR-005: Potentially Vulnerable Online Exam Platform (High)

Description:	The subdomain 'onlineexam.vardhaman.org' and 'www.onlineexam.vardhaman.org' indicates an online exam platform. This platform is a high-value target for attackers. Vulnerabilities could allow unauthorized access to exam questions, student data, and the ability to manipulate exam results. This could lead to academic dishonesty and reputational damage.
Risk:	Likelihood: Low Impact: High
System:	vardhaman.org
Tools Used:	Assetfinder
References:	N/A

Remediation

1. Conduct a thorough security audit and penetration test of the online exam platform. 2. Ensure the platform is running the latest version with all security patches applied. 3. Implement strong authentication and access controls. 4. Protect against common web vulnerabilities such as SQL injection and cross-site scripting (XSS). 5. Implement robust logging and monitoring to detect suspicious activity.

Copyright © Sarral Security

Finding SAR-006: Reliance on Third-Party CDN/Security Provider (Medium)

Description:	The domain vardhaman.org resolves to Cloudflare's IP addresses. This indicates the domain is likely using Cloudflare for CDN, security, or other services. While Cloudflare provides benefits, it also introduces a dependency. Outages or security breaches at Cloudflare could directly impact the availability and security of vardhaman.org. Furthermore, misconfiguration of Cloudflare settings could expose the origin server or introduce other vulnerabilities.
Risk:	Likelihood: Medium Impact: Medium
System:	vardhaman.org
Tools Used:	NSLookup
References:	N/A

Remediation

Implement robust monitoring of Cloudflare's status and performance. Develop a contingency plan for Cloudflare outages, including potentially routing traffic directly to the origin server (if feasible and secure). Regularly review and audit Cloudflare configurations to ensure they align with security best practices. Consider multi-CDN solutions for redundancy.

Copyright © Sarral Security

Finding SAR-007: Vulnerable Webmail Interface (Medium)

Description:	The 'webmail.vardhaman.org' subdomain indicates a publicly accessible webmail interface. Webmail interfaces are often targeted by attackers to gain access to user email accounts, which can then be used for phishing attacks, data theft, or further compromise of the network. Vulnerabilities in the webmail software itself, weak passwords, and lack of MFA can all contribute to this risk.
Risk:	Likelihood: Medium Impact: Medium
System:	vardhaman.org
Tools Used:	Subfinder
References:	N/A

Remediation

1. Ensure the webmail software is up-to-date with the latest security patches. 2. Enforce strong password policies for all webmail accounts. 3. Implement multi-factor authentication (MFA) for all webmail accounts. 4. Regularly audit webmail logs for suspicious activity. 5. Consider using a web application firewall (WAF) to protect the webmail interface from common attacks.

Copyright © Sarral Security

Finding SAR-008: Insecure Online Exam Platform (Medium)

Description:	The 'www.onlineexam.vardhaman.org' and 'onlineexam.vardhaman.org' subdomains suggest an online exam platform. If this platform is not properly secured, it could be vulnerable to various attacks, such as SQL injection, cross-site scripting (XSS), and authentication bypass. These vulnerabilities could allow attackers to access exam questions, manipulate scores, or gain unauthorized access to user accounts.
Risk:	Likelihood: Low Impact: High
System:	vardhaman.org
Tools Used:	Subfinder
References:	N/A

Remediation

1. Conduct a thorough security audit and penetration test of the online exam platform. 2. Implement secure coding practices to prevent common web vulnerabilities such as SQL injection and XSS. 3. Enforce strong authentication and authorization mechanisms. 4. Regularly monitor the platform for suspicious activity. 5. Ensure data is encrypted both in transit and at rest.

Copyright © Sarral Security

Finding SAR-009: Exposed Webmail Interface (Medium)

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, credential stuffing, or exploiting vulnerabilities in the webmail software. Compromised email accounts can be used for phishing attacks, data theft, or further lateral movement within the network.
Risk:	Likelihood: Medium Impact: Medium
System:	vardhaman.org
Tools Used:	Amass Passive
References:	N/A

Remediation

1. Ensure the webmail software is running the latest version with all security patches applied. 2. Enforce strong password policies for all email accounts. 3. Implement two-factor authentication for all email accounts. 4. Implement rate limiting to prevent brute-force attacks. 5. Regularly audit webmail logs for suspicious activity.

Copyright © Sarral Security

Finding SAR-010: Exposed FTP Server (Medium)

Description:	The subdomain 'ftp.vardhaman.org' is exposed. FTP (File Transfer Protocol) is an insecure protocol that transmits usernames and passwords in plaintext. If this server is actively used and not properly secured, attackers could intercept credentials and gain unauthorized access to files stored on the server. Even if anonymous access is enabled, it could be used to host malicious files.
Risk:	Likelihood: Low Impact: Medium
System:	vardhaman.org
Tools Used:	Amass Passive
References:	N/A

Remediation

1. Disable FTP entirely if possible and migrate to a more secure protocol like SFTP or FTPS. 2. If FTP is necessary, restrict access to a limited set of trusted IP addresses using a firewall. 3. Enforce strong password policies for all FTP accounts. 4. Monitor FTP logs for suspicious activity. 5. Consider disabling anonymous FTP access.

Copyright © Sarral Security

Finding SAR-011: Potential Vulnerabilities in Online Exam Portal (Medium)

Description:	The subdomains 'www.onlineexam.vardhaman.org' and 'onlineexam.vardhaman.org' indicate the presence of an online examination portal. These portals are often targets for attackers seeking to gain unauthorized access to exam content, manipulate results, or compromise student data. The security of this portal is critical.
Risk:	Likelihood: Low Impact: Medium
System:	vardhaman.org
Tools Used:	Amass Passive
References:	N/A

Remediation

1. Conduct a thorough security audit and penetration test of the online exam portal. 2. Ensure the portal is running the latest version of its software with all security patches applied. 3. Implement strong authentication and authorization mechanisms. 4. Protect against common web vulnerabilities such as SQL injection and cross-site scripting (XSS). 5. Regularly monitor the portal for suspicious activity.

Copyright © Sarral Security

Finding SAR-012: Exposed Webmail Interface (Medium)

Description:	The subdomain 'webmail.vardhaman.org' indicates a publicly accessible webmail interface. If vulnerable to exploits or brute-force attacks, attackers could gain access to user email accounts, potentially leading to sensitive information disclosure, phishing campaigns, and further compromise of internal systems.
Risk:	Likelihood: Medium Impact: Medium
System:	vardhaman.org
Tools Used:	Assetfinder
References:	N/A

Remediation

1. Ensure the webmail application is running the latest version with all security patches applied. 2. Enforce strong password policies and multi-factor authentication for all email accounts. 3. Implement rate limiting and brute-force protection mechanisms. 4. Regularly monitor webmail logs for suspicious activity.

Copyright © Sarral Security

Finding SAR-013: Exposed Webdisk Interface (Medium)

Description:	The subdomain 'webdisk.vardhaman.org' suggests a publicly accessible webdisk interface. If not properly secured, unauthorized users could potentially access, modify, or delete files stored on the webdisk, leading to data loss, data breaches, and system instability.
Risk:	Likelihood: Low Impact: Medium
System:	vardhaman.org
Tools Used:	Assetfinder
References:	N/A

Remediation

1. Ensure the webdisk application is running the latest version with all security patches applied. 2. Enforce strong authentication and access controls for all webdisk accounts. 3. Regularly monitor webdisk logs for suspicious activity. 4. Consider disabling webdisk if it is not actively used.

Copyright © Sarral Security

Finding SAR-014: Mail Server Vulnerabilities (Medium)

Description:	The subdomain 'mail.vardhaman.org' indicates a mail server. Mail servers are often targeted by attackers to send spam, phishing emails, or to gain access to sensitive information. Vulnerabilities in the mail server software could be exploited to compromise the server.
Risk:	Likelihood: Low Impact: Medium
System:	vardhaman.org
Tools Used:	Assetfinder
References:	N/A

Remediation

1. Ensure the mail server software is running the latest version with all security patches applied. 2. Implement strong authentication and access controls. 3. Configure SPF, DKIM, and DMARC records to prevent email spoofing. 4. Regularly monitor mail server logs for suspicious activity.

Copyright © Sarral Security

Finding SAR-015: Missing Security Headers (Medium)

Description:	Many subdomains lack essential security headers such as HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, and X-XSS-Protection. This makes the sites vulnerable to various attacks, including cross-site scripting (XSS), clickjacking, and man-in-the-middle (MITM) attacks.
Risk:	Likelihood: High Impact: Medium
System:	vardhaman.org
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Implement a consistent set of security headers across all subdomains. Specifically, enable HSTS with a long max-age, configure a strict CSP, set X-Frame-Options to 'DENY' or 'SAMEORIGIN', enable X-Content-Type-Options: nosniff, and set a restrictive Referrer-Policy and Permissions-Policy.

Copyright © Sarral Security

Finding SAR-016: Exposed cPanel and Webmail Login Pages (Medium)

Description:	The cpanel.vardhaman.org and webmail.vardhaman.org subdomains are directly accessible, potentially exposing the cPanel and webmail login interfaces to attackers. This increases the risk of brute-force attacks and credential stuffing.
Risk:	Likelihood: Low Impact: High
System:	vardhaman.org
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Restrict access to cPanel and webmail login pages to specific IP addresses or networks. Implement multi-factor authentication (MFA) for all cPanel and webmail accounts.

Copyright © Sarral Security

Finding SAR-017: Outdated PHP Version (Medium)

Description:	The faculty.vardhaman.org and studentscorner.vardhaman.org subdomains are running PHP 5.6.40, which is an outdated and unsupported version. This version is likely to have known security vulnerabilities that could be exploited by attackers.
Risk:	Likelihood: Medium Impact: Medium
System:	vardhaman.org
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Upgrade PHP to a supported version (e.g., PHP 8.1 or later) on the affected subdomains. Ensure that all PHP extensions are also updated.

Copyright © Sarral Security

Finding SAR-018: SAC Subdomain Data Exposure (Medium)

Description:	The sac.vardhaman.org subdomain exposes a large number of phone numbers and social media profiles. This information could be used for social engineering attacks or other malicious purposes.
Risk:	Likelihood: Low Impact: Medium
System:	vardhaman.org
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Review the data stored and displayed on sac.vardhaman.org. Implement measures to protect sensitive information, such as redacting phone numbers or limiting access to social media profiles.

Copyright © Sarral Security

Finding SAR-019: Single Registrar Dependency (Low)

Description:	The domain is registered with a single registrar, PublicDomainRegistry.com. While not inherently a vulnerability, a compromise or outage at this registrar could impact the domain's availability and management. If the registrar experiences a security breach or goes offline, managing the domain (e.g., updating DNS records) could become difficult or impossible.
Risk:	Likelihood: Low Impact: Medium
System:	vardhaman.org
Tools Used:	Whois
References:	N/A

Remediation

Consider diversifying domain registration across multiple registrars for critical services. Implement strong account security measures (e.g., MFA) with the registrar.

Copyright © Sarral Security

Finding SAR-020: Lack of DNSSEC (Low)

Description:	The domain is not using DNSSEC (Domain Name System Security Extensions). This means that DNS responses are not cryptographically signed, making the domain potentially vulnerable to DNS spoofing or cache poisoning attacks. An attacker could potentially redirect users to a malicious website by manipulating DNS records.
Risk:	Likelihood: Low Impact: Medium
System:	vardhaman.org
Tools Used:	Whois
References:	N/A

Remediation

Implement DNSSEC 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.

Copyright © Sarral Security

Finding SAR-021: Reliance on Cloudflare's Nameservers (Low)

Description:	The domain relies on Cloudflare's nameservers. While Cloudflare provides benefits like DDoS protection and CDN services, a widespread outage or compromise of Cloudflare's infrastructure could impact the domain's availability. This is a common practice, but it's important to acknowledge the dependency.
Risk:	Likelihood: Low Impact: Medium
System:	vardhaman.org
Tools Used:	Whois
References:	N/A

Remediation

Develop a contingency plan for potential Cloudflare outages. This might involve having a secondary DNS provider ready to take over in case of an emergency. Regularly review Cloudflare's security advisories and implement recommended security measures.

BUSINESS CONFIDENTIAL
Copyright © Sarral Security

Finding SAR-022: Potential Information Disclosure (Low)

Description:	The subdomain naming convention (e.g., ece.vardhaman.org, cse.vardhaman.org, sac.vardhaman.org) reveals information about the organization's structure and departments. While not a direct vulnerability, this information could be used by attackers to target specific individuals or departments with phishing attacks or social engineering attempts.
Risk:	Likelihood: Medium Impact: Low
System:	vardhaman.org
Tools Used:	Subfinder
References:	N/A

Remediation

1. Review the subdomain naming convention and consider using more generic or less descriptive names where possible. 2. Educate employees about the risks of social engineering and phishing attacks. 3. Implement email filtering and spam protection measures.

Copyright © Sarral Security

Finding SAR-023: Potential Information Disclosure via 'localhost' (Low)

Description:	The subdomain 'localhost.vardhaman.org' is unusual. While it likely resolves to 127.0.0.1, its presence in public DNS could indicate misconfiguration or internal testing environments being inadvertently exposed. It might reveal internal naming conventions or development practices.
Risk:	Likelihood: Low Impact: Low
System:	vardhaman.org
Tools Used:	Amass Passive
References:	N/A

Remediation

1. Investigate the purpose of 'localhost.vardhaman.org'. 2. If it's not needed, remove the DNS record. 3. If it's for internal testing, ensure it's properly isolated and not accessible from the public internet.

Copyright © Sarral Security

Finding SAR-024: Information Disclosure via Subdomains (Low)

Description:	The presence of subdomains like 'ece.vardhaman.org', 'cse.vardhaman.org', 'alumni.vardhaman.org', 'sac.vardhaman.org', 'iic.vardhaman.org', 'inf.vardhaman.org', 'csd.vardhaman.org', and 'csm.vardhaman.org' reveals information about the organization's structure and departments. While not directly exploitable, this information can be used by attackers for social engineering or targeted attacks.
Risk:	Likelihood: Medium Impact: Low
System:	vardhaman.org
Tools Used:	Assetfinder
References:	N/A

Remediation

1. Review the necessity of each subdomain and consider consolidating services where possible. 2. Ensure that each subdomain has appropriate security measures in place. 3. Regularly monitor subdomains for unauthorized changes or content.

Copyright © Sarral Security

Finding SAR-025: TRACE Method Enabled (Low)

Description:	The TRACE HTTP method is enabled on several subdomains. This method can be used to conduct cross-site tracing (XST) attacks, potentially exposing sensitive information such as cookies.
Risk:	Likelihood: Medium Impact: Low
System:	vardhaman.org
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Disable the TRACE HTTP method on all web servers. This can typically be done in the server configuration (e.g., Apache, Nginx).

Copyright © Sarral Security

Finding SAR-026: Grievance Redressal SSL Handshake Failure (Low)

Description:	The grievance.redressal.vardhaman.org subdomain is experiencing SSL handshake failures, potentially due to outdated SSL/TLS protocols or misconfiguration. This could prevent users from accessing the site securely.
Risk:	Likelihood: Low Impact: Low
System:	vardhaman.org
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Review the SSL/TLS configuration of the web server hosting grievance.redressal.vardhaman.org. Ensure that modern SSL/TLS protocols are enabled and that the server's cipher suite is properly configured.

Copyright © Sarral Security

Finding SAR-027: Alumni Portal OTP Login (Low)

Description:	The alumni portal offers OTP login, which is good, but the implementation should be reviewed to ensure it is secure and not vulnerable to bypass or brute-force attacks.
Risk:	Likelihood: Medium Impact: Low
System:	vardhaman.org
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Review the OTP login implementation to ensure it is secure. Implement rate limiting to prevent brute-force attacks. Consider adding additional security measures, such as CAPTCHA.

Copyright © Sarral Security

Finding SAR-028: Grievance Redressal Cell on Main Domain (Low)

Description:	The main vardhaman.org domain links to a grievance redressal cell, which is good for transparency, but the implementation should be reviewed to ensure it is secure and not vulnerable to abuse.
Risk:	Likelihood: Low Impact: Low
System:	vardhaman.org
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Review the grievance redressal cell implementation to ensure it is secure. Implement rate limiting to prevent abuse. Consider adding additional security measures, such as CAPTCHA.

Copyright © Sarral Security

Finding SAR-029: Lack of HSTS on Mail Subdomain (Low)

Description:	The mail.vardhaman.org subdomain lacks HSTS, which means that users connecting to the mail server may be vulnerable to man-in-the-middle attacks.
Risk:	Likelihood: Medium Impact: Low
System:	vardhaman.org
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Enable HSTS on the mail.vardhaman.org subdomain with a long max-age and includeSubDomains directive.

Copyright © Sarral Security

Finding SAR-030: SSL Handshake Failure (Low)

Description:	The grievance.redressal.vardhaman.org subdomain is experiencing SSL handshake failures, potentially due to outdated SSL/TLS protocols or misconfiguration. This could prevent users from accessing the site securely.
Risk:	Likelihood: Low Impact: Low
System:	vardhaman.org
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Review the SSL/TLS configuration of the web server hosting grievance.redressal.vardhaman.org. Ensure that modern SSL/TLS protocols are enabled and that the server's cipher suite is properly configured.

BUSINESS CONFIDENTIAL
Copyright © Sarral Security

Finding SAR-031: 403 Forbidden on CDN and Assets (Low)

Description:	The cdn.vardhaman.org and assets.vardhaman.org subdomains are returning 403 Forbidden errors, indicating that access to these resources is restricted. This could prevent the website from loading properly.
Risk:	Likelihood: Low Impact: Low
System:	vardhaman.org
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Review the access control configuration of cdn.vardhaman.org and assets.vardhaman.org. Ensure that the necessary resources are accessible to the public.

Copyright © Sarral Security

Finding SAR-032: 401 Unauthorized on cpcontacts, cpcalendars, and webdisk (Low)

Description:	The cpcontacts.vardhaman.org, cpcalendars.vardhaman.org, and webdisk.vardhaman.org subdomains are returning 401 Unauthorized errors, indicating that authentication is required to access these resources. This is expected behavior, but the authentication mechanisms should be reviewed to ensure they are secure.
Risk:	Likelihood: Low Impact: Low
System:	vardhaman.org
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Review the authentication mechanisms for cpcontacts.vardhaman.org, cpcalendars.vardhaman.org, and webdisk.vardhaman.org. Ensure that strong passwords are required and that multi-factor authentication (MFA) is enabled where possible.

Copyright © Sarral Security

Finding SAR-033: 500 Internal Server Error (Low)

Description:	The ece.vardhaman.org subdomain is returning a 500 Internal Server Error, indicating that there is a server-side error. This could be due to a misconfiguration, a software bug, or a resource exhaustion issue.
Risk:	Likelihood: Low Impact: Low
System:	vardhaman.org
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Review the server logs for ece.vardhaman.org to identify the cause of the 500 Internal Server Error. Address the underlying issue to restore functionality.

Copyright © Sarral Security

Finding SAR-034: Generic Subdomains - Need Further Investigation (Info)

Description:	Subdomains like 'student.vardhaman.org', 'events.vardhaman.org', 'resources.vardhaman.org', 'login.vardhaman.org', 'results.vardhaman.org', 'ece.vardhaman.org', 'erp.vardhaman.org', 'courses.vardhaman.org', 'cse.vardhaman.org', 'alumni.vardhaman.org', 'faculty.vardhaman.org', 'video-lectures.vardhaman.org', 'conferences.vardhaman.org', 'cdn.vardhaman.org', 'cdc.vardhaman.org', 'go.vardhaman.org', 'inf.vardhaman.org', 'studentscorner.vardhaman.org', 'fdp.vardhaman.org', 'assets.vardhaman.org' require further investigation to determine their purpose and security posture. Each subdomain represents a potential attack surface.
Risk:	Likelihood: Low Impact: Low
System:	vardhaman.org
Tools Used:	Amass Passive
References:	N/A

Remediation

1. Inventory all subdomains and document their purpose and functionality. 2. Conduct vulnerability scans on each subdomain. 3. Ensure each subdomain is properly secured with appropriate authentication, authorization, and access controls. 4. Regularly monitor each subdomain for suspicious activity.

Copyright © Sarral Security

Finding SAR-035: Name Resolution Errors (Info)

Description:	The www.nptel.vardhaman.org and www.onlineexam.vardhaman.org subdomains are experiencing name resolution errors, indicating a potential DNS configuration issue. This could prevent users from accessing these sites.
Risk:	Likelihood: Low Impact: Low
System:	vardhaman.org
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Verify the DNS records for www.nptel.vardhaman.org and www.onlineexam.vardhaman.org. Ensure that the A and AAAA records are correctly configured and point to the appropriate IP addresses.

Copyright © Sarral Security

Finding SAR-036: Connection Refused (Info)

Description:	The localhost.vardhaman.org subdomain is returning connection refused errors, indicating that there is no service listening on the specified port. This is likely due to a misconfiguration or an inactive service.
Risk:	Likelihood: Low Impact: Low
System:	vardhaman.org
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Investigate the configuration of localhost.vardhaman.org. Ensure that the intended service is running and listening on the correct port. If the subdomain is not needed, consider removing it.

Copyright © Sarral Security

Finding SAR-037: 404 Not Found on Resources (Info)

Description:	Several subdomains (resources, ieee, ceta, erp, ortus, rice2016, fdp, courses) are returning 404 Not Found errors, indicating that the requested resources are not available. This could be due to misconfiguration or missing content.
Risk:	Likelihood: Low Impact: Low
System:	vardhaman.org
Tools Used:	WebScraperRecon
References:	N/A

Remediation

Investigate the configuration of the affected subdomains. Ensure that the necessary resources are present and that the web server is properly configured to serve them. If the subdomains are not needed, consider removing them.

Copyright © Sarral Security