SARRAL SECURITY

vardhaman.org

Security Assessment Findings Report

Business Confidential

Date: December 01, 2025
Project: SAR-085
Version 1.0

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

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.

Executive Summary

Sarral Security evaluated vardhaman.org's security posture on December 01, 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.

Vulnerability Summary & Report Card

0	0	6	5	2
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
SAR-001: Exposed cPanel and Webmail Login Pages	Medium	Restrict access to cPanel and Webmail login pages to authorized IP addresses only. Implement multi-factor authentication (MFA) to prevent unauthorized access even if credentials are compromised. Regul...
SAR-002: Missing Security Headers	Medium	Implement the following security headers: HSTS (Strict-Transport-Security), CSP (Content-Security-Policy), X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy and X-XSS-Protec...
SAR-003: Deprecated PHP Version	Medium	Upgrade PHP to a supported version (e.g., 8.1 or later) to ensure security patches are applied and vulnerabilities are mitigated.
SAR-004: WebDAV Enabled	Medium	Disable WebDAV methods if not required. If WebDAV is necessary, ensure proper authentication and authorization mechanisms are in place to restrict access to authorized users only.
SAR-005: Basic Authentication Enabled	Medium	Enforce HTTPS for all traffic to these subdomains. Consider using more secure authentication methods such as multi-factor authentication (MFA) or token-based authentication.
SAR-006: TLS 1.0 and TLS 1.1 Enabled	Medium	Disable TLS 1.0 and TLS 1.1 to enforce the use of more secure protocols (TLS 1.2 and TLS 1.3).
SAR-007: Exposed Email Addresses and Phone Numbers	Low	Implement measures to protect email addresses and phone numbers from being easily scraped from the website. Consider using CAPTCHAs or obfuscation techniques. Educate users about the risks of phishing...
SAR-008: TRACE Method Enabled	Low	Disable the TRACE HTTP method on the web server to prevent Cross-Site Tracing (XST) attacks.
SAR-009: Insecure Cookie Attributes	Low	Configure the web server to set the Secure attribute for all cookies, ensuring they are only transmitted over HTTPS connections.
SAR-010: Information Disclosure: Internal IP Address	Low	Remove the internal IP address from the website content and comments. Ensure that internal IP addresses are not exposed to the public.

SAR-011: Information Disclosure: Software Version	Low	Disable the X-Powered-By header or configure it to not expose the PHP version. This can be done in the PHP configuration file.
SAR-012: Information Disclosure: CDN Technology	Info	Remove the CDN technology from the headers. This can be done in the CDN configuration file.
SAR-013: Detection of Web Application Firewall	Info	No remediation is necessary as the WAF is a security control. Ensure the WAF is properly configured and maintained.

Technical Findings

Finding SAR-001: Exposed cPanel and Webmail Login Pages (Medium)

Description:	The cpanel.vardhaman.org and webmail.vardhaman.org subdomains are exposed, potentially allowing attackers to attempt brute-force attacks to gain unauthorized access to the system's control panel and email accounts. Successful exploitation could lead to server compromise and data breaches.
Risk:	Likelihood: Low Impact: Medium
System:	vardhaman.org
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021-Security Misconfiguration CWE: CWE-287
Evidence:	`Observed cpanel.vardhaman.org and webmail.vardhaman.org subdomains in Amass Passive, Subfinder, and Assetfinder output. WebScraperRecon confirms the presence of login pages.`

Remediation

Restrict access to cPanel and Webmail login pages to authorized IP addresses only. Implement multi-factor authentication (MFA) to prevent unauthorized access even if credentials are compromised. Regularly monitor login attempts and enforce strong password policies.

Finding SAR-002: Missing Security Headers (Medium)

Description:	Several subdomains, including grievance.redressal.vardhaman.org, rice2016.vardhaman.org, cdn.vardhaman.org, ceta.vardhaman.org, results.vardhaman.org, ece.vardhaman.org, ortus.vardhaman.org, fdp.vardhaman.org, pat.vardhaman.org, epics.vardhaman.org, nptel.vardhaman.org, e-cell.vardhaman.org, login.vardhaman.org, faculty.vardhaman.org, student.vardhaman.org, ieee.vardhaman.org, assets.vardhaman.org, resources.vardhaman.org, acm.vardhaman.org, csm.vardhaman.org, and courses.vardhaman.org, are missing security headers such as HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy and X-XSS-Protection. This increases the risk of attacks such as Cross-Site Scripting (XSS), clickjacking, and man-in-the-middle attacks.
Risk:	Likelihood: Low Impact: Medium
System:	vardhaman.org
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021-Security Misconfiguration CWE: CWE-1035
Evidence:	`WebScraperRecon output shows 'security_headers' as null for the listed subdomains.`

Remediation

Implement the following security headers: HSTS (Strict-Transport-Security), CSP (Content-Security-Policy), X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy and X-XSS-Protection. Configure these headers with appropriate values to mitigate potential attacks.

Finding SAR-003: Deprecated PHP Version (Medium)

Description:	The subdomain results.vardhaman.org is running on PHP 5.6.40, which is a deprecated version. This version is no longer receiving security updates, making the server vulnerable to known exploits.
Risk:	Likelihood: Medium Impact: Medium
System:	vardhaman.org
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A06:2021-Vulnerable and Outdated Components CWE: CWE-937
Evidence:	`WebScraperRecon output for results.vardhaman.org shows 'X-Powered-By: PHP/5.6.40' in the headers.`

Remediation

Upgrade PHP to a supported version (e.g., 8.1 or later) to ensure security patches are applied and vulnerabilities are mitigated.

Finding SAR-004: WebDAV Enabled (Medium)

Description:	The webdisk.vardhaman.org subdomain has WebDAV methods enabled (COPY, DELETE, LOCK, MKCOL, MOVE, PROPFIND, PROPPATCH, PUT, UNLOCK). If not properly secured, this could allow unauthorized users to modify or delete files on the server.
Risk:	Likelihood: Low Impact: Medium
System:	vardhaman.org
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021-Security Misconfiguration CWE: CWE-939
Evidence:	`WebScraperRecon output for webdisk.vardhaman.org shows WebDAV methods enabled in the 'http_methods' field.`

Remediation

Disable WebDAV methods if not required. If WebDAV is necessary, ensure proper authentication and authorization mechanisms are in place to restrict access to authorized users only.

Finding SAR-005: Basic Authentication Enabled (Medium)

Description:	The webdisk.vardhaman.org and cpcontacts.vardhaman.org subdomains are using Basic Authentication, which transmits credentials in base64 encoding. This is susceptible to credential theft if the traffic is not properly secured with HTTPS.
Risk:	Likelihood: Low Impact: Medium
System:	vardhaman.org
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A02:2021-Cryptographic Failures CWE: CWE-319
Evidence:	`WebScraperRecon output for webdisk.vardhaman.org and cpcontacts.vardhaman.org shows 'WWW-Authenticate: Basic realm' in the headers.`

Remediation

Enforce HTTPS for all traffic to these subdomains. Consider using more secure authentication methods such as multi-factor authentication (MFA) or token-based authentication.

Finding SAR-006: TLS 1.0 and TLS 1.1 Enabled (Medium)

Description:	The server supports TLS 1.0 and TLS 1.1, which are considered deprecated and have known security vulnerabilities. While the server also supports TLS 1.2 and TLS 1.3, the presence of older protocols increases the attack surface.
Risk:	Likelihood: Low Impact: Medium
System:	vardhaman.org
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A06:2021 - Vulnerable and Outdated Components CWE: CWE-327
Evidence:	`TLSv1.0 enabled TLSv1.1 enabled`

Remediation

Disable TLS 1.0 and TLS 1.1 to enforce the use of more secure protocols (TLS 1.2 and TLS 1.3).

Finding SAR-007: Exposed Email Addresses and Phone Numbers (Low)

Description:	Email addresses and phone numbers were found on multiple subdomains, including rice2016.vardhaman.org, cdn.vardhaman.org, epics.vardhaman.org, nptel.vardhaman.org, e-cell.vardhaman.org, faculty.vardhaman.org, student.vardhaman.org, sac.vardhaman.org, acm.vardhaman.org, csm.vardhaman.org, and ftp.vardhaman.org. This information could be used for phishing attacks, spam campaigns, or social engineering attempts.
Risk:	Likelihood: Medium Impact: Low
System:	vardhaman.org
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A09:2021-Security Logging and Monitoring Failures CWE: CWE-200
Evidence:	`WebScraperRecon output shows lists of emails and phones found on the listed subdomains.`

Remediation

Implement measures to protect email addresses and phone numbers from being easily scraped from the website. Consider using CAPTCHAs or obfuscation techniques. Educate users about the risks of phishing and social engineering attacks.

Finding SAR-008: TRACE Method Enabled (Low)

Description:	The TRACE HTTP method is enabled on multiple subdomains. This method can be used to conduct Cross-Site Tracing (XST) attacks, potentially exposing sensitive information such as cookies.
Risk:	Likelihood: Low Impact: Low
System:	vardhaman.org
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021-Security Misconfiguration CWE: CWE-200
Evidence:	`WebScraperRecon output shows TRACE method enabled in the 'http_methods' field for multiple subdomains.`

Remediation

Disable the TRACE HTTP method on the web server to prevent Cross-Site Tracing (XST) attacks.

Finding SAR-009: Insecure Cookie Attributes (Low)

Description:	The PHPSESSID cookie on results.vardhaman.org lacks the Secure attribute. This means the cookie can be transmitted over unencrypted HTTP connections, potentially exposing the session ID to eavesdropping attacks.
Risk:	Likelihood: Low Impact: Low
System:	vardhaman.org
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021-Security Misconfiguration CWE: CWE-614
Evidence:	`WebScraperRecon output for results.vardhaman.org shows 'Set-Cookie: PHPSESSID=...; Path=/' without the Secure attribute.`

Remediation

Configure the web server to set the Secure attribute for all cookies, ensuring they are only transmitted over HTTPS connections.

Finding SAR-010: Information Disclosure: Internal IP Address (Low)

Description:	The subdomain nptel.vardhaman.org is leaking an internal IP address (192.168.0.25) in the comments. This information could be used by attackers to map the internal network and identify potential targets.
Risk:	Likelihood: Low Impact: Low
System:	vardhaman.org
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A03:2021-Injection CWE: CWE-200
Evidence:	`WebScraperRecon output for nptel.vardhaman.org shows internal IP address in the comments.`

Remediation

Remove the internal IP address from the website content and comments. Ensure that internal IP addresses are not exposed to the public.

Finding SAR-011: Information Disclosure: Software Version (Low)

Description:	The subdomains iic.vardhaman.org and ece.vardhaman.org are disclosing the version of PHP being used (PHP/8.2.29) in the X-Powered-By header. This information could be used by attackers to identify known vulnerabilities in that specific version of PHP.
Risk:	Likelihood: Low Impact: Low
System:	vardhaman.org
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021-Security Misconfiguration CWE: CWE-200
Evidence:	`WebScraperRecon output for iic.vardhaman.org and ece.vardhaman.org shows 'X-Powered-By: PHP/8.2.29' in the headers.`

Remediation

Disable the X-Powered-By header or configure it to not expose the PHP version. This can be done in the PHP configuration file.

Finding SAR-012: Information Disclosure: CDN Technology (Info)

Description:	The go.vardhaman.org subdomain is disclosing the CDN technology being used (Cloudfront) in the headers. This information could be used by attackers to identify potential CDN-specific vulnerabilities.
Risk:	Likelihood: Low Impact: Info
System:	vardhaman.org
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A05:2021-Security Misconfiguration CWE: CWE-200
Evidence:	`WebScraperRecon output for go.vardhaman.org shows 'via: 1.1 0fad2b2f93c2ade9df8e31249e9938a2.cloudfront.net (CloudFront)' in the headers.`

Remediation

Remove the CDN technology from the headers. This can be done in the CDN configuration file.

Finding SAR-013: Detection of Web Application Firewall (Info)

Description:	The target website is behind a Web Application Firewall (WAF). This indicates the presence of a security measure to protect against common web exploits.
Risk:	Likelihood: Info Impact: Info
System:	vardhaman.org
Tools Used:	AI_PHASE_SUMMARY
References:	OWASP: A09:2021 - Security Logging and Monitoring Failures CWE: CWE-223
Evidence:	`The site https://vardhaman.org is behind Cloudflare (Cloudflare Inc.) WAF.`

Remediation

No remediation is necessary as the WAF is a security control. Ensure the WAF is properly configured and maintained.