SECURITY ASSESSMENT REPORT

Target: vardhaman.org
Date: November 24, 2025
Scan ID: 23

Prepared by Sarral Scan

1. Executive Summary

Sarral Scan performed a comprehensive security assessment of **vardhaman.org** on 2025-11-24. The objective was to identify potential security vulnerabilities and provide recommendations for remediation.

Findings Summary

Severity	Count
Critical	0
High	1
Medium	3
Low	5
Info	2

2. Detailed Findings

1. Exposed cPanel Interface

Severity: HIGH

Tool: Passive Recon

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.

Remediation:

Restrict access to the cPanel interface to authorized IP addresses only. Enforce strong password policies and consider multi-factor authentication. Ensure cPanel is running the latest stable version with all security patches applied.

2. Exposed Webmail Interface

Severity: MEDIUM

Tool: Passive Recon

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.

Remediation:

Ensure the webmail software is up-to-date with the latest security patches. Enforce strong password policies and consider multi-factor authentication for all email accounts. Regularly audit webmail logs for suspicious activity.

3. Potentially Vulnerable Online Exam Portal

Severity: MEDIUM

Tool: Passive Recon

Description:

The subdomain 'onlineexam.vardhaman.org' suggests an online exam portal. If the portal is not properly secured, it could be vulnerable to attacks such as SQL injection, cross-site scripting (XSS), or authentication bypass, potentially compromising exam data and student information.

Remediation:

Conduct a thorough security audit and penetration test of the online exam portal. Implement robust input validation and output encoding to prevent injection attacks. Ensure secure authentication and authorization mechanisms are in place. Regularly update the portal software and dependencies.

4. Open HTTP Proxy Port (8080)

Severity: MEDIUM **Tool:** Active Recon

Description:

An open HTTP proxy port (8080) could be exploited by attackers to proxy malicious traffic or gain unauthorized access to internal resources if not properly secured. It's crucial to ensure this port is only accessible to authorized users and services.

Remediation:

If the HTTP proxy is required, implement strong authentication and authorization mechanisms. Restrict access to trusted IP addresses or networks. Regularly monitor the proxy logs for suspicious activity. If the proxy is not required, disable the service and close the port.

5. Outdated Subdomain - rice2016.vardhaman.org

Severity: LOW **Tool:** Passive Recon

Description:

The subdomain 'rice2016.vardhaman.org' suggests a potentially outdated and neglected web application related to a conference or event from 2016. Outdated applications often contain known vulnerabilities that can be exploited.

Remediation:

Assess the purpose and necessity of the 'rice2016.vardhaman.org' subdomain. If no longer needed, remove it. If it is still required, update the underlying software and apply all security patches. Consider migrating the content to a more secure and actively maintained platform.

6. Open HTTP Port (80)

Severity: LOW **Tool:** Active Recon

Description:

The presence of an open HTTP port (80) without a redirect to HTTPS (443) could allow for unencrypted communication, potentially exposing sensitive information if not properly configured. While HTTPS is also open, the lack of a redirect leaves the site vulnerable to downgrade attacks.

Remediation:

Implement a permanent (301) redirect from HTTP (port 80) to HTTPS (port 443) at the server level. This ensures all traffic is encrypted.

7. Open Alternate HTTPS Port (8443)

Severity: LOW **Tool:** Active Recon

Description:

An open alternate HTTPS port (8443) might indicate a misconfiguration or a specific application using a non-standard port for secure communication. While HTTPS is used, using a non-standard port can sometimes be overlooked in security configurations.

Remediation:

Verify the purpose of the service running on port 8443. Ensure it is properly secured with up-to-date TLS configurations. If the service is not required, disable it and close the port. If required, document the reason for using a non-standard port and ensure it's included in security monitoring and patching procedures.

8. WhatWeb Scan Failure

Severity: LOW **Tool:** Active Recon

Description:

The WhatWeb scan failed to execute due to a missing dependency. This prevents the identification of technologies used on the target website, potentially missing vulnerabilities associated with those technologies.

Remediation:

Investigate and resolve the WhatWeb error by installing the missing dependency (/usr/bin/lib/messages). Re-run the WhatWeb scan to identify the technologies used on the target website.

9. Missing DNSSEC

Severity: LOW

Tool: Active Recon

Description:

The DNSRecon tool reported 'No answer for DNSSEC query'. DNSSEC helps prevent DNS spoofing and cache poisoning attacks. The absence of DNSSEC makes the domain more vulnerable to these types of attacks.

Remediation:

Implement DNSSEC for the domain to ensure the integrity and authenticity of DNS records. This will help protect against DNS spoofing and cache poisoning attacks.

10. DNS Zone Transfer Vulnerability (Potential)

Severity: INFO

Tool: Active Recon

Description:

The DNS reconnaissance revealed the Bind version being used by the Cloudflare nameservers. While the version is '2025.11.1', which is in the future, it's important to ensure that the DNS servers are properly configured to prevent unauthorized zone transfers. An improperly configured DNS server could allow an attacker to obtain a complete copy of the zone file, revealing sensitive information about the network infrastructure.

Remediation:

Verify that the DNS servers are configured to prevent unauthorized zone transfers. Restrict zone transfers to only authorized servers. Regularly audit the DNS configuration to ensure it is secure.

11. Email Infrastructure Information Disclosure

Severity: INFO

Tool: Active Recon

Description:

The DNS records reveal the use of Microsoft Outlook for email services, including specific MX records and SPF records. While not directly a vulnerability, this information can be used by attackers to craft more targeted phishing attacks or attempt to exploit known vulnerabilities in the Microsoft Outlook infrastructure.

Remediation:

Implement robust email security measures, including anti-phishing and anti-spam filters. Educate users about the risks of phishing attacks and how to identify suspicious emails. Regularly review and update the SPF records to ensure they are accurate and prevent email spoofing.

3. Appendix: Raw Tool Output

The following section contains raw output from the security tools used during the assessment.

Tool: Passive Recon

```
{"unique_subdomains_count": 32, "subdomains": ["onlineexam.vardhaman.org",
"login.vardhaman.org", "conferences.vardhaman.org", "rice2016.vardhaman.org",
"alumni.vardhaman.org", "courses.vardhaman.org", "www.vardhaman.org",
"go.vardhaman.org", "www.onlineexam.vardhaman.org", "results.vardhaman.org",
"events.vardhaman.org", "www.nptel.vardhaman.org", "csd.vardhaman.org",
"csm.vardhaman.org", "cpcalendars.vardhaman.org", "ece.vardhaman.org",
"fdp.vardhaman.org", "iic.vardhaman.org", "cdn.vardhaman.org", "sac.vardhaman.org",
"cdc.vardhaman.org", "webdisk.vardhaman.org", "cpcontacts.vardhaman.org",
"inf.vardhaman.org", "webmail.vardhaman.org", "nptel.vardhaman.org", "vardhaman.org",
"studentscorner.vardhaman.org", "cse.vardhaman.org", "mail.vardhaman.org",
"faculty.vardhaman.org", "cpanel.vardhaman.org"], "resolved_hosts": [],
"live_services": [], "_raw_logs": "[11:23:05 PM] [+] Starting passive enumeration for:
vardhaman.org\n[11:23:05 PM] [+] Using temporary output directory:
/tmp/tmp32wzweyn\n[11:23:05 PM] [+] Running Subfinder...\n[11:23:40 PM] [+] Running
Findomain...\n[11:23:44 PM] [+] Running Assetfinder...\n[11:23:46 PM] [+] Running Amass
Passive...\n[11:33:46 PM] [+] Merging results...\n[11:33:46 PM] [+] Found 32 unique
subdomains.\n[11:33:46 PM] [+] Checking DNS resolution with dnsx...\n[11:43:46 PM] [+]
DNSX resolved 0 hosts.\n[11:43:46 PM] [+] Checking HTTP/HTTPS services with
httpx...\n[11:43:46 PM] [!] HTTPX Error Output: Usage: httpx [OPTIONS] URL\n\nError: No
such option: -s\n[11:43:46 PM] [+] HTTPX found 0 live services.\n[11:43:46 PM] [+] Recon
complete.\n{\"unique_subdomains_count\": 32, \"subdomains\":
[\"onlineexam.vardhaman.org\", \"login.vardhaman.org\", \"conferences.vardhaman.org\",
\"rice2016.vardhaman.org\", \"alumni.vardhaman.org\", \"courses.vardhaman.org\",
\"www.vardhaman.org\", \"go.vardhaman.org\", \"www.onlineexam.vardhaman.org\",
\"results.vardhaman.org\", \"events.vardhaman.org\", \"www.nptel.vardhaman.org\",
\"csd.vardhaman.org\", \"csm.vardhaman.org\", \"cpcalendars.vardhaman.org\",
\"ece.vardhaman.org\", \"fdp.vardhaman.org\", \"iic.vardhaman.org\",
\"cdn.vardhaman.org\", \"sac.vardhaman.org\", \"cdc.vardhaman.org\",
\"webdisk.vardhaman.org\", \"cpcontacts.vardhaman.org\", \"inf.vardhaman.org\",
\"webmail.vardhaman.org\", \"nptel.vardhaman.org\", \"vardhaman.org\",
\"studentscorner.vardhaman.org\", \"cse.vardhaman.org\", \"mail.vardhaman.org\",
\"faculty.vardhaman.org\", \"cpanel.vardhaman.org\"], \"resolved_hosts\": [],
\"live_services\": []}\n"}
```

Tool: Active Recon

```
{"nmap_fast": "Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-23 23:43 EST\nNmap
scan report for vardhaman.org (104.21.8.203)\nHost is up (0.39s latency).\nOther
addresses for vardhaman.org (not scanned): 2606:4700:3032::ac43:9dd7
2606:4700:3037::6815:8cb 172.67.157.215\nNot shown: 96 filtered tcp ports
(no-response)\nPORT STATE SERVICE\n80/tcp open http\n443/tcp open https\n8080/tcp open
http-proxy\n8443/tcp open https-alt\n\nNmap done: 1 IP address (1 host up) scanned in
10.67 seconds", "whatweb": "/usr/bin/whatweb:257:in `require_relative': cannot load
such file -- /usr/bin/lib/messages (LoadError)\n\tfrom /usr/bin/whatweb:257:in `'",
"dnsrecon": "2025-11-23T23:44:05.519054-0500 INFO Starting enumeration for domain:
vardhaman.org\n2025-11-23T23:44:05.520372-0500 INFO std: Performing General Enumeration
against: vardhaman.org...\n2025-11-23T23:44:05.699716-0500 ERROR No answer for DNSSEC
query for vardhaman.org\n2025-11-23T23:44:05.906350-0500 INFO \t SOA
owen.ns.cloudflare.com 172.64.33.219\n2025-11-23T23:44:05.906510-0500 INFO \t SOA
owen.ns.cloudflare.com 108.162.193.219\n2025-11-23T23:44:05.906600-0500 INFO \t SOA
owen.ns.cloudflare.com 173.245.59.219\n2025-11-23T23:44:05.906641-0500 INFO \t SOA
owen.ns.cloudflare.com 2803:f800:50::6ca2:c1db\n2025-11-23T23:44:05.906678-0500 INFO \t
SOA owen.ns.cloudflare.com 2a06:98c1:50::ac40:21db\n2025-11-23T23:44:05.906834-0500
INFO \t SOA owen.ns.cloudflare.com
2606:4700:58::adf5:3bdb\n2025-11-23T23:44:06.146681-0500 INFO \t NS
owen.ns.cloudflare.com 173.245.59.219\n2025-11-23T23:44:06.237617-0500 INFO \t Bind
Version for 173.245.59.219 \"2025.11.1\"\n2025-11-23T23:44:06.237778-0500 INFO \t NS
owen.ns.cloudflare.com 108.162.193.219\n2025-11-23T23:44:06.314846-0500 INFO \t Bind
Version for 108.162.193.219 \"2025.11.1\"\n2025-11-23T23:44:06.315092-0500 INFO \t NS
owen.ns.cloudflare.com 172.64.33.219\n2025-11-23T23:44:06.397442-0500 INFO \t Bind
Version for 172.64.33.219 \"2025.11.1\"\n2025-11-23T23:44:06.397897-0500 INFO \t NS
owen.ns.cloudflare.com 2606:4700:58::adf5:3bdb\n2025-11-23T23:44:06.485027-0500 INFO \t
Bind Version for 2606:4700:58::adf5:3bdb \"2025.11.1\"\n2025-11-23T23:44:06.485506-0500
INFO \t NS owen.ns.cloudflare.com
2a06:98c1:50::ac40:21db\n2025-11-23T23:44:06.561932-0500 INFO \t Bind Version for
2a06:98c1:50::ac40:21db \"2025.11.1\"\n2025-11-23T23:44:06.562194-0500 INFO \t NS
owen.ns.cloudflare.com 2803:f800:50::6ca2:c1db\n2025-11-23T23:44:06.641538-0500 INFO \t
Bind Version for 2803:f800:50::6ca2:c1db \"2025.11.1\"\n2025-11-23T23:44:06.641761-0500
INFO \t NS riya.ns.cloudflare.com 172.64.34.155\n2025-11-23T23:44:06.733461-0500 INFO
\t Bind Version for 172.64.34.155 \"2025.11.1\"\n2025-11-23T23:44:06.733703-0500 INFO
\t NS riya.ns.cloudflare.com 162.159.38.155\n2025-11-23T23:44:07.499948-0500 INFO \t
Bind Version for 162.159.38.155 \"2025.11.1\"\n2025-11-23T23:44:07.500281-0500 INFO \t
NS riya.ns.cloudflare.com 108.162.194.155\n2025-11-23T23:44:07.583969-0500 INFO \t Bind
Version for 108.162.194.155 \"2025.11.1\"\n2025-11-23T23:44:07.584388-0500 INFO \t NS
riya.ns.cloudflare.com 2803:f800:50::6ca2:c29b\n2025-11-23T23:44:07.662290-0500 INFO \t
Bind Version for 2803:f800:50::6ca2:c29b \"2025.11.1\"\n2025-11-23T23:44:07.662532-0500
INFO \t NS riya.ns.cloudflare.com
2606:4700:50::a29f:269b\n2025-11-23T23:44:07.743353-0500 INFO \t Bind Version for
2606:4700:50::a29f:269b \"2025.11.1\"\n2025-11-23T23:44:07.743607-0500 INFO \t NS
riya.ns.cloudflare.com 2a06:98c1:50::ac40:229b\n2025-11-23T23:44:07.827482-0500 INFO \t
Bind Version for 2a06:98c1:50::ac40:229b \"2025.11.1\"\n2025-11-23T23:44:08.608988-0500
INFO \t MX vardhaman-org.mail.protection.outlook.com
52.101.144.0\n2025-11-23T23:44:08.609403-0500 INFO \t MX
vardhaman-org.mail.protection.outlook.com 52.101.145.2\n2025-11-23T23:44:08.609539-0500
INFO \t MX vardhaman-org.mail.protection.outlook.com
52.101.145.0\n2025-11-23T23:44:08.609615-0500 INFO \t MX
vardhaman-org.mail.protection.outlook.com 52.101.144.3\n2025-11-23T23:44:08.609693-0500
INFO \t MX vardhaman-org.mail.protection.outlook.com
2a01:111:f403:cc2d::\n2025-11-23T23:44:08.609769-0500 INFO \t MX
vardhaman-org.mail.protection.outlook.com
2a01:111:f403:cc2c::\n2025-11-23T23:44:08.609843-0500 INFO \t MX
vardhaman-org.mail.protection.outlook.com
2a01:111:f403:cc2c::1\n2025-11-23T23:44:08.609933-0500 INFO \t MX
vardhaman-org.mail.protection.outlook.com
2a01:111:f403:cc2d::1\n2025-11-23T23:44:08.619554-0500 INFO \t A vardhaman.org
172.67.157.215\n2025-11-23T23:44:08.619803-0500 INFO \t A vardhaman.org
104.21.8.203\n2025-11-23T23:44:08.619907-0500 INFO \t AAAA vardhaman.org
2606:4700:3037::6815:8cb\n2025-11-23T23:44:08.619991-0500 INFO \t AAAA vardhaman.org
2606:4700:3032::ac43:9dd7\n2025-11-23T23:44:08.850530-0500 INFO \t TXT vardhaman.org
MS=ms48985209\n2025-11-23T23:44:08.850731-0500 INFO \t TXT vardhaman.org v=spf1
include:spf.protection.outlook.com -all\n2025-11-23T23:44:08.850773-0500 INFO \t TXT
vardhaman.org v=verifydomain ...[Truncated]
```