SECURITY ASSESSMENT REPORT

Target: vardhaman.org
Date: November 26, 2025
Scan ID: 42

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	14
Low	5
Info	7

2. Detailed Findings

1. Potentially Exposed cPanel Interface

Severity: HIGH **Tool:** Subfinder

Description:

The subdomain 'cpanel.vardhaman.org' suggests a cPanel interface is exposed. If accessible to the public without proper restrictions, it could be a target for attackers seeking to gain unauthorized access to server management functions. Default credentials or weak passwords could lead to complete server compromise.

Remediation:

Restrict access to the cPanel interface to authorized IP addresses only. Change default credentials immediately. Implement MFA for all cPanel accounts. Keep cPanel software updated with the latest security patches. Consider using a non-standard port for cPanel access.

---

2. Online Exam Platform Vulnerabilities

Severity: HIGH **Tool:** Subfinder

Description:

The subdomains 'www.onlineexam.vardhaman.org' and 'onlineexam.vardhaman.org' indicate an online exam platform. These platforms are often targets for cheating and data breaches. Vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure direct object references (IDOR) could allow attackers to manipulate exam results, access sensitive student data, or disrupt the exam process.

Remediation:

Conduct thorough security testing of the online exam platform, including penetration testing and vulnerability scanning. Implement secure coding practices to prevent common web vulnerabilities. Enforce strong authentication and authorization mechanisms. Regularly monitor the platform for suspicious activity. Ensure data is encrypted both in transit and at rest.

---

3. Exposed cPanel Interface

Severity: HIGH **Tool:** Amass Passive

Description:

The subdomain 'cpanel.vardhaman.org' suggests a publicly accessible cPanel interface. If not properly secured with strong authentication and up-to-date software, it could be a target for brute-force attacks or exploitation of known cPanel vulnerabilities.

Remediation:

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

4. Login Portal Vulnerabilities

Severity: HIGH **Tool:** Amass Passive

Description:

The subdomain 'login.vardhaman.org' indicates a login portal. Login portals are prime targets for credential stuffing, brute-force attacks, and other authentication-related attacks. Vulnerabilities in the login process could lead to unauthorized access to sensitive systems.

Remediation:

Implement strong password policies, enforce multi-factor authentication, implement rate limiting to prevent brute-force attacks, and regularly audit the login portal for security vulnerabilities. Ensure proper input validation and output encoding to prevent injection attacks.

5. Reliance on Single Registrar

Severity: MEDIUM **Tool:** Whois

Description:

The domain is registered with a single registrar, PDR Ltd. d/b/a PublicDomainRegistry.com. If this registrar experiences a security breach or goes offline, it could impact the domain's availability and management.

Remediation:

Implement strong account security measures with the registrar, including multi-factor authentication. Consider diversifying domain registration across multiple registrars for redundancy, although this is generally not recommended for a single domain.

6. DNSSEC Unsigned

Severity: MEDIUM **Tool:** Whois

Description:

The domain's DNSSEC status is 'unsigned'. DNSSEC helps prevent DNS spoofing and cache poisoning attacks by digitally signing DNS records. Without DNSSEC, the domain is more vulnerable to these types of attacks.

Remediation:

Implement DNSSEC by generating DNSSEC keys and configuring them with both the domain registrar and the DNS provider (Cloudflare in this case). This will digitally sign the DNS records and provide authentication.

7. Reliance on a Third-Party CDN (Cloudflare)

Severity: MEDIUM **Tool:** NSLookup

Description:

The domain relies on Cloudflare, a third-party CDN. While Cloudflare provides security benefits, a compromise or outage at Cloudflare could impact the availability and security of vardhaman.org. Misconfiguration of Cloudflare settings can also introduce vulnerabilities.

Remediation:

Regularly review and audit Cloudflare configuration settings to ensure they align with security best practices. Implement robust monitoring and alerting for Cloudflare services. Have a backup plan in case of a Cloudflare outage or compromise.

8. Potential for Cloudflare Misconfiguration

Severity: MEDIUM **Tool:** NSLookup

Description:

Incorrectly configured Cloudflare settings can expose the origin server's IP address, bypass security features, or introduce other vulnerabilities. For example, failing to properly configure WAF rules or SSL/TLS settings can leave the domain vulnerable.

Remediation:

Conduct regular security audits of Cloudflare configurations. Ensure proper WAF rule sets are in place and actively maintained. Verify SSL/TLS settings are correctly configured and using strong ciphers. Implement rate limiting and bot protection measures.

---

9. Exposed Webmail Interface

Severity: MEDIUM **Tool:** Subfinder

Description:

The subdomain 'webmail.vardhaman.org' likely hosts a webmail interface. If not properly secured with strong authentication and up-to-date software, it could be vulnerable to brute-force attacks, credential stuffing, and exploits targeting known vulnerabilities in the webmail software.

Remediation:

Ensure the webmail software is the latest version with all security patches applied. Enforce strong password policies, implement multi-factor authentication (MFA), and regularly monitor logs for suspicious activity. Consider rate limiting login attempts.

---

10. Insecure FTP Access

Severity: MEDIUM **Tool:** Amass Passive

Description:

The subdomain 'ftp.vardhaman.org' indicates the presence of an FTP server. FTP is inherently insecure as it transmits credentials in plaintext. If not properly configured, it could allow unauthorized access to sensitive files.

Remediation:

Disable FTP and migrate to a more secure protocol like SFTP (SSH File Transfer Protocol) or FTPS (FTP Secure). If FTP is absolutely necessary, enforce strong password policies, restrict access to authorized IP addresses, and monitor FTP logs for suspicious activity.

11. Webmail Access Vulnerabilities

Severity: MEDIUM **Tool:** Amass Passive

Description:

The subdomain 'webmail.vardhaman.org' provides access to webmail. Webmail interfaces are often targets for phishing attacks and may contain vulnerabilities that could allow attackers to gain access to user accounts and sensitive information.

Remediation:

Ensure the webmail software is running the latest version with all security patches applied. Implement two-factor authentication for all user accounts. Regularly monitor webmail logs for suspicious activity and educate users about phishing attacks.

12. Potential Vulnerabilities in 'onlineexam.vardhaman.org' and 'www.onlineexam.vardhaman.org'

Severity: MEDIUM **Tool:** Amass Passive

Description:

The subdomains 'onlineexam.vardhaman.org' and 'www.onlineexam.vardhaman.org' suggest an online examination platform. These platforms often handle sensitive student data and are vulnerable to various attacks, including SQL injection, cross-site scripting (XSS), and authentication bypass.

Remediation:

Conduct regular security audits and penetration testing of the online examination platform. Implement secure coding practices to prevent common web vulnerabilities. Ensure proper data encryption and access controls to protect student data.

13. Exposed Webdisk Interface

Severity: MEDIUM **Tool:** Amass Passive

Description:

The subdomain 'webdisk.vardhaman.org' suggests a publicly accessible webdisk interface. If not properly secured with strong authentication and up-to-date software, it could be a target for brute-force attacks or exploitation of known vulnerabilities, leading to data leakage.

Remediation:

Ensure the webdisk software is running the latest version, enforce strong password policies, implement two-factor authentication, and restrict access to authorized IP addresses only. Regularly audit access logs.

---

14. Exposed cPanel Interface

Severity: MEDIUM **Tool:** Assetfinder

Description:

The subdomain '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, privilege escalation, and information disclosure.

Remediation:

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

---

15. Vulnerable Webmail Interface

Severity: MEDIUM **Tool:** Assetfinder

Description:

The subdomain 'webmail.vardhaman.org' indicates a publicly accessible webmail interface. Outdated or misconfigured webmail software can be vulnerable to various attacks, including cross-site scripting (XSS), cross-site request forgery (CSRF), and authentication bypass.

Remediation:

Ensure the webmail software (e.g., Roundcube, SquirrelMail) is running the latest version with all security patches applied. Implement strong password policies, enable two-factor authentication, and regularly audit the webmail configuration for security vulnerabilities. Consider using a web application firewall (WAF) to protect against common web attacks.

16. Potential Vulnerabilities in Online Exam Platform

Severity: MEDIUM **Tool:** Assetfinder

Description:

The subdomains 'www.onlineexam.vardhaman.org' and 'onlineexam.vardhaman.org' suggest an online exam platform. These platforms often handle sensitive student data and are attractive targets for attackers. Vulnerabilities in the platform could lead to data breaches, unauthorized access to exams, and manipulation of results.

Remediation:

Conduct a thorough security audit and penetration test of the online exam platform. Ensure that all input validation and output encoding are properly implemented to prevent XSS and SQL injection attacks. Implement strong authentication and authorization mechanisms. Regularly update the platform software and apply security patches.

17. Exposed HTTP/HTTPS Ports with Cloudflare Proxy

Severity: MEDIUM **Tool:** Nmap Top 1000

Description:

The scan shows ports 80, 443, 8080, and 8443 are open and running Cloudflare's HTTP proxy. While Cloudflare provides protection, exposing multiple ports, especially non-standard ones like 8080 and 8443, can increase the attack surface. It's crucial to ensure these ports are properly configured and secured, and that the underlying application is not directly accessible.

Remediation:

Review the Cloudflare configuration to ensure only necessary ports are exposed. Verify that the origin server is not directly accessible and that all traffic is routed through Cloudflare. Consider closing non-standard ports if they are not essential. Implement strong security policies on the origin server.

18. 415 Unsupported Media Type Error

Severity: MEDIUM **Tool:** WhatWeb

Description:

The server is consistently returning a 415 Unsupported Media Type error. This indicates that the server is unable to process the request due to the media type of the request data being unsupported. This could be due to incorrect content-type headers being sent by clients, or a misconfiguration on the server side regarding accepted media types.

Remediation:

1. Investigate server-side configuration to ensure correct handling of expected media types. 2. Review client-side applications to ensure they are sending the correct content-type headers in their requests. 3. Examine server logs for more detailed information about the specific requests triggering the 415 error. 4. If Cloudflare is caching the error, ensure the origin server is properly configured before purging the cache.

19. Information Disclosure via Subdomain Enumeration

Severity: LOW **Tool:** Subfinder

Description:

The enumeration of subdomains reveals information about the organization's infrastructure and services. While not a direct vulnerability, this information can be used by attackers to map the attack surface and identify potential targets.

Remediation:

Review the purpose and necessity of each subdomain. Consider using wildcard SSL certificates to obscure subdomain names. Implement proper access controls and security measures for all subdomains, regardless of their perceived importance.

20. Outdated or Unmaintained Subdomains (rice2016.vardhaman.org)

Severity: LOW

Tool: Amass Passive

Description:

The subdomain 'rice2016.vardhaman.org' suggests a potentially outdated or unmaintained website related to a conference in 2016. Outdated websites often contain unpatched vulnerabilities that can be exploited by attackers.

Remediation:

Assess the purpose and necessity of the subdomain. If no longer needed, remove the subdomain. If still required, update the website software and apply all security patches. Regularly monitor the website for security vulnerabilities.

21. Exposed Webdisk Interface

Severity: LOW

Tool: Assetfinder

Description:

The subdomain 'webdisk.vardhaman.org' suggests a publicly accessible webdisk interface. If not properly secured, it could be vulnerable to unauthorized file access, modification, and deletion.

Remediation:

Ensure the webdisk software is running the latest version with all security patches applied. Enforce strong authentication, restrict access to authorized users only, and regularly audit the webdisk configuration for security vulnerabilities. Consider disabling directory listing.

22. Filtered TCP Ports

Severity: LOW

Tool: Nmap Top 1000

Description:

The scan reports 996 filtered TCP ports. While filtered ports are not inherently vulnerable, they indicate the presence of a firewall or other network security device. It's important to ensure that the firewall rules are properly configured and that no unintended ports are being blocked.

Remediation:

Review the firewall configuration to ensure that only necessary ports are open and that all other ports are properly blocked. Regularly audit firewall rules to identify and remove any unnecessary or outdated rules.

---

23. Potential Misconfiguration of Content Negotiation

Severity: LOW **Tool:** WhatWeb

Description:

The 415 error suggests a potential issue with content negotiation. The server might not be correctly configured to handle different content types, leading to the rejection of valid requests. This could be exploited to cause denial of service or to bypass security measures that rely on specific content types.

Remediation:

1. Review the server's content negotiation settings to ensure they are correctly configured. 2. Verify that the server supports the content types expected by clients. 3. Implement proper error handling to provide informative error messages to clients when a 415 error occurs.

---

24. 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 itself, it's important to be aware of this information for reporting any malicious activity associated with the domain or registrar.

Remediation:

Monitor the domain for any signs of abuse or malicious activity. If any is detected, report it to the registrar's abuse contact email and phone number.

25. Client Transfer Prohibited

Severity: INFO **Tool:** Whois

Description:

The domain status 'clientTransferProhibited' prevents unauthorized transfers of the domain to another registrar. This is a security feature that helps protect against domain hijacking.

Remediation:

This status is a positive security measure. Ensure that the domain transfer lock remains enabled unless a legitimate transfer is required.

26. Unsecured 'go.vardhaman.org' Subdomain

Severity: INFO **Tool:** Subfinder

Description:

The 'go.vardhaman.org' subdomain could be used for URL shortening or redirection. If not properly secured, it could be abused by attackers to redirect users to malicious websites or to phish for credentials.

Remediation:

Implement proper access controls and logging for the 'go.vardhaman.org' subdomain. Monitor the subdomain for suspicious activity. Consider using a reputable URL shortening service instead of hosting your own.

27. Increased Attack Surface due to Multiple Subdomains

Severity: INFO **Tool:** Assetfinder

Description:

The presence of numerous subdomains increases the overall attack surface of the vardhaman.org domain. Each subdomain represents a potential entry point for attackers.

Remediation:

Regularly audit all subdomains for security vulnerabilities. Implement a centralized security monitoring and logging system to detect and respond to suspicious activity across all subdomains. Consider consolidating subdomains where possible to reduce the attack surface.

28. Lack of Application Information Behind Cloudflare

Severity: INFO **Tool:** Nmap Top 1000

Description:

The Nmap scan only identifies Cloudflare's HTTP proxy, not the specific application running behind it. This lack of information makes it difficult to assess the application's specific vulnerabilities. Knowing the application type and version is crucial for targeted vulnerability assessments.

Remediation:

Investigate the application running behind Cloudflare to determine its type and version. Conduct further vulnerability scanning and penetration testing specifically targeting the application. Implement a Web Application Firewall (WAF) with rules tailored to the application's known vulnerabilities.

29. Cloudflare Configuration Review

Severity: INFO **Tool:** WhatWeb

Description:

The presence of Cloudflare as a reverse proxy indicates that the website's traffic is being routed through Cloudflare's infrastructure. While Cloudflare provides security benefits, it's important to ensure that it is properly configured to protect the website from attacks. Misconfigured Cloudflare settings can expose the website to vulnerabilities.

Remediation:

1. Review Cloudflare's security settings to ensure they are properly configured. 2. Verify that Cloudflare's firewall is enabled and configured to block malicious traffic. 3. Regularly update Cloudflare's security rules to protect against new threats. 4. Ensure the origin server is properly

secured and not directly exposed to the internet.

30. Cloudflare WAF Detection

Severity: INFO **Tool:** WafW00f

Description:

The website is behind Cloudflare WAF. This means that common web application attacks are likely to be filtered. However, it does not guarantee complete protection, and sophisticated attacks or misconfigurations could still bypass the WAF.

Remediation:

Regularly review and update Cloudflare WAF rules to address emerging threats. Conduct thorough penetration testing to identify vulnerabilities that the WAF might not detect. Ensure proper configuration of the WAF to avoid bypasses.

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: 2025-11-26T10:36:49Z <<< 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: 2606:4700:3037::6815:8cb Name: vardhaman.org Address:
2606:4700:3032::ac43:9dd7
```

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 go.vardhaman.org [INF] Found 21
subdomains for vardhaman.org in 30 seconds 3 milliseconds cse.vardhaman.org
webmail.vardhaman.org nptel.vardhaman.org vardhaman.org ece.vardhaman.org
inf.vardhaman.org webdisk.vardhaman.org cpcalendars.vardhaman.org
cpcontacts.vardhaman.org mail.vardhaman.org www.nptel.vardhaman.org csd.vardhaman.org
sac.vardhaman.org iic.vardhaman.org csm.vardhaman.org onlineexam.vardhaman.org
```

```
alumni.vardhaman.org www.vardhaman.org cpanel.vardhaman.org
www.onlineexam.vardhaman.org
```

Tool: Amass Passive

```
acm.vardhaman.org sac.vardhaman.org epics.vardhaman.org assets.vardhaman.org
www.nptel.vardhaman.org ftp.vardhaman.org student.vardhaman.org
onlineexam.vardhaman.org csm.vardhaman.org cpcalendars.vardhaman.org
www.onlineexam.vardhaman.org e-cell.vardhaman.org results.vardhaman.org
inf.vardhaman.org cdn.vardhaman.org ece.vardhaman.org fdp.vardhaman.org
conferences.vardhaman.org mun.vardhaman.org resources.vardhaman.org
webdisk.vardhaman.org faculty.vardhaman.org iic.vardhaman.org ortus.vardhaman.org
ieee.vardhaman.org login.vardhaman.org cpanel.vardhaman.org
video-lectures.vardhaman.org ipr.vardhaman.org csd.vardhaman.org pat.vardhaman.org
webmail.vardhaman.org courses.vardhaman.org vardhaman.org www.vardhaman.org
studentscorner.vardhaman.org cpcontacts.vardhaman.org events.vardhaman.org
erp.vardhaman.org cse.vardhaman.org rice2016.vardhaman.org mail.vardhaman.org
go.vardhaman.org cdc.vardhaman.org nptel.vardhaman.org
grievance.redressal.vardhaman.org alumni.vardhaman.org ceta.vardhaman.org The
enumeration has finished Discoveries are being migrated into the local database
```

Tool: Assetfinder

```
vardhaman.org www.vardhaman.org conferences.vardhaman.org alumni.vardhaman.org
vardhaman.org vardhaman.org go.vardhaman.org csd.vardhaman.org vardhaman.org
www.vardhaman.org sac.vardhaman.org iic.vardhaman.org ece.vardhaman.org
csm.vardhaman.org cse.vardhaman.org inf.vardhaman.org cse.vardhaman.org
inf.vardhaman.org csm.vardhaman.org ece.vardhaman.org iic.vardhaman.org vardhaman.org
www.vardhaman.org csd.vardhaman.org csm.vardhaman.org ece.vardhaman.org vardhaman.org
www.vardhaman.org csd.vardhaman.org csd.vardhaman.org cse.vardhaman.org
csm.vardhaman.org ece.vardhaman.org inf.vardhaman.org cpanel.vardhaman.org
cpcalendars.vardhaman.org cpcontacts.vardhaman.org webdisk.vardhaman.org
webmail.vardhaman.org nptel.vardhaman.org cpanel.vardhaman.org
cpcalendars.vardhaman.org cpcontacts.vardhaman.org mail.vardhaman.org vardhaman.org
webdisk.vardhaman.org webmail.vardhaman.org www.vardhaman.org nptel.vardhaman.org
www.nptel.vardhaman.org onlineexam.vardhaman.org www.onlineexam.vardhaman.org
cpanel.vardhaman.org mail.vardhaman.org vardhaman.org webdisk.vardhaman.org
webmail.vardhaman.org www.vardhaman.org cpanel.vardhaman.org vardhaman.org
webdisk.vardhaman.org webmail.vardhaman.org www.vardhaman.org
```

Tool: Nmap Top 1000

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 05:38 EST Nmap scan report for
vardhaman.org (172.67.157.215) Host is up (0.070s latency). Other addresses for
vardhaman.org (not scanned): 2606:4700:3032::ac43:9dd7 2606:4700:3037::6815:8cb
104.21.8.203 Not shown: 996 filtered tcp ports (no-response) PORT STATE SERVICE VERSION
80/tcp open http Cloudflare http proxy 443/tcp open ssl/http Cloudflare http proxy
8080/tcp open http Cloudflare http proxy 8443/tcp open ssl/http Cloudflare http proxy
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 31.49 seconds
```

Tool: WhatWeb

```
http://vardhaman.org [415 Unsupported Media Type] Country[UNITED STATES][US],
HTTPServer[cloudflare], IP[104.21.8.203], Script, Title[415 Unsupported Media Type],
UncommonHeaders[nel,cf-cache-status,report-to,cf-ray,alt-svc] https://vardhaman.org
[415 Unsupported Media Type] Country[RESERVED][ZZ], HTTPServer[cloudflare],
IP[172.67.157.215], Script, Title[415 Unsupported Media Type],
UncommonHeaders[cf-cache-status,nel,report-to,cf-ray,alt-svc]
```

Tool: WafW00f

```
______ / \ ( W00f! ) \ ____/ ,, __ 404 Hack Not Found |`-.__ / / __ __ /" _/ /_/ \ \ / /
*===* / \ \_/ / 405 Not Allowed / )__// \ / /| / /---` 403 Forbidden \\/` \ | / _ \ `\
/_\\_ 502 Bad Gateway / / \ \ 500 Internal Error `_____``-` /_/ \_\\ ~ WAFW00F : v2.3.1
~ The Web Application Firewall Fingerprinting Toolkit [*] Checking
https://vardhaman.org [+] The site https://vardhaman.org is behind Cloudflare
(Cloudflare Inc.) WAF. [~] Number of requests: 2
```

Tool: HTTPx

```
__ __ __ _ __ / /_ / /_/ /_____ | |/ / / __ \/ __/ __/ __ \| / / / / / /_/ /_/ /_/ / |
/_/ /_/\__/\__/ .___/_/|_| /_/ v1.1.5 projectdiscovery.io Use with caution. You are
responsible for your actions. Developers assume no liability and are not responsible for
any misuse or damage. [System] Command timed out.
```