Website Vulnerability Scanner Report (Light)

✓ **http://www.vendasta.com/**

Target added due to a redirect from https://vendasta.com

The Light Website Scanner didn't check for critical issues like SQLi, XSS, Command Injection, XXE, etc. Upgrade to run Deep scans with 40+ tests and detect more vulnerabilities.

Summary

Overall risk level:

Medium

Risk ratings:

High:	0
Medium:	1
Low:	4
Info:	14

Scan information:

Start time:	Jul 07, 2024 / 12:54:51
Finish time:	Jul 07, 2024 / 12:55:58
Scan duration:	1 min, 7 sec
Tests performed:	19/19
Scan status:	Finished

Findings

Communication is not secure

CONFIRMED

URL	Response URL	Evidence
http://www.vendasta.com/	http://www.vendasta.com/	Communication is made over unsecure, unencrypted HTTP.

Details

Risk description:

The risk is that an attacker who manages to intercept the communication at the network level can read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data).

Recommendation:
We recommend you to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the server.

Classification:
CWE : CWE-311
OWASP Top 10 - 2013 : A6 - Sensitive Data Exposure
OWASP Top 10 - 2017 : A3 - Sensitive Data Exposure
OWASP Top 10 - 2021 : A4 - Insecure Design

Missing security header: Referrer-Policy

CONFIRMED

URL	Evidence
http://www.vendasta.com/	Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response.

Details

Risk description:
The risk is that if a user visits a web page (e.g. "http://example.com/pricing/") and clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the `Referer` header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

Recommendation:
The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value `no-referrer` of this header instructs the browser to omit the Referer header entirely.

References:
https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

Classification:
CWE : CWE-693
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Missing security header: Content-Security-Policy

CONFIRMED

URL	Evidence
http://www.vendasta.com/	Response does not include the HTTP Content-Security-Policy security header or meta tag

Details

Risk description:
The risk is that if the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

Recommendation:
Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

References:
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Classification:
CWE : CWE-693
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Robots.txt file found

CONFIRMED

URL
http://www.vendasta.com/robots.txt

Details

Risk description:
There is no particular security risk in having a robots.txt file. However, it's important to note that adding endpoints in it should not be considered a security measure, as this file can be directly accessed and read by anyone.

Recommendation:
We recommend you to manually review the entries from robots.txt and remove the ones which lead to sensitive locations in the website (ex. administration panels, configuration files, etc).

References:
https://www.theregister.co.uk/2015/05/19/robotstxt/

Classification:
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Server software and technology found

UNCONFIRMED

Software / Version	Category
Facebook Pixel	Analytics
FancyBox 3.2.10	JavaScript libraries
Google Analytics GA4	Analytics
MySQL	Databases
PHP	Programming languages
Google Tag Manager	Tag managers
OneTrust	Cookie compliance
Varnish	Caching
YouTube	Video players
Microsoft Advertising	Advertising
Reddit Ads	Advertising
Angular	JavaScript frameworks
Linkedin Insight Tag	Analytics
Zone.js	JavaScript frameworks
jQuery Migrate 3.4.1	JavaScript libraries
WP-PageNavi	WordPress plugins
HTTP/3	Miscellaneous
jQuery 3.7.1	JavaScript libraries
jQuery Mobile 4.24.3	Mobile frameworks
Matomo Analytics	Analytics
OptinMonster	Marketing automation
Segment 4.13.1	Customer data platform
Swiper	JavaScript libraries
The Events Calendar	WordPress plugins
Webpack	Miscellaneous

Module Federation	Miscellaneous
WordPress 6.5.2	CMS, Blogs
ClickCease	Security
Divi	Page builders, WordPress themes, WordPress plugins
reCAPTCHA	Security
Hotjar	Analytics
Leadfeeder	Analytics
TypeScript	Programming languages
Zoominfo	Analytics
Yoast SEO 22.5	SEO, WordPress plugins
Yoast SEO Premium 22.4	SEO

Details

Risk description:
The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html

Classification:
OWASP Top 10 - 2013 : A5 - Security Misconfiguration
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Website is accessible.

Nothing was found for vulnerabilities of server-side software.

Nothing was found for client access policies.

Nothing was found for absence of the security.txt file.

Nothing was found for use of untrusted certificates.

Nothing was found for enabled HTTP debug methods.

Nothing was found for enabled HTTP OPTIONS method.

Nothing was found for directory listing.

Nothing was found for missing HTTP header - Strict-Transport-Security.

Nothing was found for missing HTTP header - X-Content-Type-Options.

Nothing was found for domain too loose set for cookies.

Nothing was found for HttpOnly flag of cookie.

Nothing was found for Secure flag of cookie.

Nothing was found for unsafe HTTP header Content Security Policy.

Scan coverage information

List of tests performed (19/19)

- Starting the scan...
- Checking for missing HTTP header - Referrer...
- Checking for missing HTTP header - Content Security Policy...
- Checking for secure communication...
- Checking for website technologies...
- Checking for vulnerabilities of server-side software...
- Checking for client access policies...
- Checking for robots.txt file...
- Checking for absence of the security.txt file...
- Checking for use of untrusted certificates...
- Checking for enabled HTTP debug methods...
- Checking for enabled HTTP OPTIONS method...
- Checking for directory listing...
- Checking for missing HTTP header - Strict-Transport-Security...
- Checking for missing HTTP header - X-Content-Type-Options...
- Checking for domain too loose set for cookies...
- Checking for HttpOnly flag of cookie...
- Checking for Secure flag of cookie...
- Checking for unsafe HTTP header Content Security Policy...

Scan parameters

Target:	http://www.vendasta.com/
Scan type:	Light
Authentication:	False

Scan stats

Unique Injection Points Detected:	44
URLs spidered:	2
Total number of HTTP requests:	11
Average time until a response was received:	931ms