Website Vulnerability Scanner Report (Light)

Unlock the full capabilities of this scanner

See what the DEEP scanner can do

Perform in-depth website scanning and discover high risk vulnerabilities.

Testing areas	Light scan	Deep scan
Website fingerprinting	✓	✓
Version-based vulnerability detection	✓	✓
Common configuration issues	✓	✓
SQL injection	–	✓
Cross-Site Scripting	–	✓
Local/Remote File Inclusion	–	✓
Remote command execution	–	✓
Discovery of sensitive files	–	✓

✓ **https://wanderhub-a-travelling-website-1.onrender.com/listings/68539b6f308eb34b131fa761**

Target added due to a redirect from http://wanderhub-a-travelling-website-1.onrender.com/listings/68539b6f308eb34b131fa761

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:

Critical:	0
High:	0
Medium:	1
Low:	5
Info:	34

Scan information:

Start time:	Jun 20, 2025 / 06:35:09 UTC+03
Finish time:	Jun 20, 2025 / 06:35:36 UTC+03
Scan duration:	27 sec
Tests performed:	40/40
Scan status:	Finished

Findings

Insecure cookie setting: missing Secure flag

port 443/tcp

CONFIRMED

URL	Cookie Name	Evidence
https://wanderhub-a-travelling-website-1.onrender.com/listings/68539b6f308eb34b131fa761	connect.sid	Set-Cookie: connect.sid=s%3AMwfiLmT2Q0T3I8-IwCs0u_ohASxJPkhU.CiFT42j4G9iCmtrX0EwaXNVIyDlqqGyl4uYnrrtjufo Request / Response

Details

Risk description:
The risk exists that an attacker will intercept the clear-text communication between the browser and the server and he will steal the cookie of the user. If this is a session cookie, the attacker could gain unauthorized access to the victim's web session.

Recommendation:
Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

Classification:
CWE : CWE-614
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Missing security header: Referrer-Policy

CONFIRMED

port 443/tcp

URL	Evidence
https://wanderhub-a-travelling-website-1.onrender.com/listings/68539b6f308eb34b131fa761	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. Request / 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 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Missing security header: Strict-Transport-Security

CONFIRMED

port 443/tcp

URL	Evidence
https://wanderhub-a-travelling-website-1.onrender.com/listings/68539b6f308eb34b131fa761	Response headers do not include the HTTP Strict-Transport-Security header Request / Response

Details

Risk description:
The risk is that lack of this header permits an attacker to force a victim user to initiate a clear-text HTTP connection to the server, thus opening the possibility to eavesdrop on the network traffic and extract sensitive information (e.g. session cookies).

Recommendation:
The Strict-Transport-Security HTTP header should be sent with each HTTPS response. The syntax is as follows:

```
Strict-Transport-Security: max-age=<seconds>[; includeSubDomains]
```

The parameter `max-age` gives the time frame for requirement of HTTPS in seconds and should be chosen quite high, e.g. several months. A value below 7776000 is considered as too low by this scanner check.
The flag `includeSubDomains` defines that the policy applies also for sub domains of the sender of the response.

Classification:

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

Missing security header: Content-Security-Policy

port 443/tcp

CONFIRMED

URL	Evidence
https://wanderhub-a-travelling-website-1.onrender.com/listings/68539b6f308eb34b131fa761	Response does not include the HTTP Content-Security-Policy security header or meta tag Request / Response

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

Missing security header: X-Content-Type-Options

port 443/tcp

CONFIRMED

URL	Evidence
https://wanderhub-a-travelling-website-1.onrender.com/listings/68539b6f308eb34b131fa761	Response headers do not include the X-Content-Type-Options HTTP security header Request / Response

Details

Risk description:
The risk is that lack of this header could make possible attacks such as Cross-Site Scripting or phishing in Internet Explorer browsers.

Recommendation:
We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff` .

References:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

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

Server software and technology found

port 443/tcp

UNCONFIRMED

Software / Version	Category
Express	Web frameworks, Web servers
Bootstrap 5.3.0	UI frameworks
HTTP/3	Miscellaneous

Node.js	Programming languages
Render	PaaS
Cloudflare	CDN
jsDelivr	CDN

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

Security.txt file is missing

CONFIRMED

port 443/tcp

URL
Missing: https://wanderhub-a-travelling-website-1.onrender.com/.well-known/security.txt

Details

Risk description:
There is no particular risk in not having a security.txt file for your server. However, this file is important because it offers a designated channel for reporting vulnerabilities and security issues.

Recommendation:
We recommend you to implement the security.txt file according to the standard, in order to allow researchers or users report any security issues they find, improving the defensive mechanisms of your server.

References:
https://securitytxt.org/

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

HTTP OPTIONS enabled

CONFIRMED

port 443/tcp

URL	Method	Summary
https://wanderhub-a-travelling-website-1.onrender.com/listings/68539b6f308eb34b131fa761	OPTIONS	We did a HTTP OPTIONS request. The server responded with a 200 status code and the header: `Allow: GET,PUT,DELETE,HEAD` Request / Response

Details

Risk description:
The only risk this might present nowadays is revealing debug HTTP methods that can be used on the server. This can present a danger if any of those methods can lead to sensitive information, like authentication information, secret keys.

Recommendation:
We recommend that you check for unused HTTP methods or even better, disable the OPTIONS method. This can be done using your

webserver configuration.

References:

https://techcommunity.microsoft.com/t5/iis-support-blog/http-options-and-default-page-vulnerabilities/ba-p/1504845
https://docs.nginx.com/nginx-management-suite/acm/how-to/policies/allowed-http-methods/

Classification:

CWE : CWE-16
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 robots.txt file.

Nothing was found for use of untrusted certificates.

Nothing was found for enabled HTTP debug methods.

Nothing was found for secure communication.

Nothing was found for directory listing.

Nothing was found for passwords submitted unencrypted.

Nothing was found for error messages.

Nothing was found for debug messages.

Nothing was found for code comments.

Nothing was found for missing HTTP header - Feature.

Nothing was found for passwords submitted in URLs.

Nothing was found for domain too loose set for cookies.

Nothing was found for mixed content between HTTP and HTTPS.

Nothing was found for cross domain file inclusion.

Nothing was found for internal error code.

Nothing was found for HttpOnly flag of cookie.

Nothing was found for login interfaces.

Nothing was found for secure password submission.

Nothing was found for sensitive data.

Nothing was found for unsafe HTTP header Content Security Policy.

Nothing was found for OpenAPI files.

Nothing was found for file upload.

Nothing was found for SQL statement in request parameter.

Nothing was found for password returned in later response.

Nothing was found for Path Disclosure.

Nothing was found for Session Token in URL.

Nothing was found for API endpoints.

Nothing was found for emails.

Nothing was found for missing HTTP header - Rate Limit.

Scan coverage information

List of tests performed (40/40)

- Starting the scan...
- Checking for missing HTTP header - Referrer...
- Checking for missing HTTP header - Strict-Transport-Security...
- Checking for missing HTTP header - Content Security Policy...
- Checking for Secure flag of cookie...
- Checking for missing HTTP header - X-Content-Type-Options...

- 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 secure communication...
- Checking for directory listing...
- Checking for passwords submitted unencrypted...
- Checking for error messages...
- Checking for debug messages...
- Checking for code comments...
- Checking for missing HTTP header - Feature...
- Checking for passwords submitted in URLs...
- Checking for domain too loose set for cookies...
- Checking for mixed content between HTTP and HTTPS...
- Checking for cross domain file inclusion...
- Checking for internal error code...
- Checking for HttpOnly flag of cookie...
- Checking for login interfaces...
- Checking for secure password submission...
- Checking for sensitive data...
- Checking for unsafe HTTP header Content Security Policy...
- Checking for OpenAPI files...
- Checking for file upload...
- Checking for SQL statement in request parameter...
- Checking for password returned in later response...
- Checking for Path Disclosure...
- Checking for Session Token in URL...
- Checking for API endpoints...
- Checking for emails...
- Checking for missing HTTP header - Rate Limit...

Scan parameters

target:	https://wanderhub-a-travelling-website-1.onrender.com/listings/68539b6f308eb34b131fa761
scan_type:	Light
authentication:	False

Scan stats

Unique Injection Points Detected:	1
URLs spidered:	1
Total number of HTTP requests:	10
Average time until a response was received:	412ms