Website Vulnerability Scanner Report

✓ **https://app.dwatson.online/**

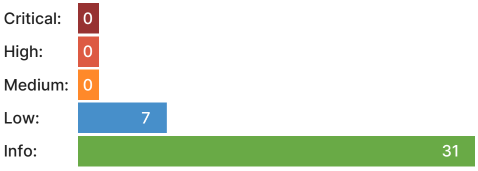
! The Light Website Scanner didn't check for critical issues like SQLi, XSS, Command Injection, XXE, etc.
Upgrade to run Deep scans with 40+ tests and detect more vulnerabilities.

Summary

Overall risk level:

Low

Risk ratings:



Scan information:

Start time:	Feb 09, 2026 / 03:22:14 UTC+05
Finish time:	Feb 09, 2026 / 03:22:53 UTC+05
Scan duration:	39 sec
Tests performed:	38/38
Scan status:	Finished

Findings

Missing security header: Strict-Transport-Security

port 443/tcp

CONFIRMED

URL	Evidence
https://app.dwatson.online/	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: Referrer-Policy

port 443/tcp

CONFIRMED

URL	Evidence
https://app.dwatson.online/	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: Content-Security-Policy

CONFIRMED

port 443/tcp

URL	Evidence
https://app.dwatson.online/	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

CONFIRMED

port 443/tcp

URL	Evidence
https://app.dwatson.online/	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

Robots.txt file found

CONFIRMED

port 443/tcp

URL
https://app.dwatson.online/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 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Password Submitted in URL

port 443/tcp

UNCONFIRMED

URL	Method	Parameters	Evidence

https://app.dwatson.online/	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
			The following form sends inputs of type password plainly in the URL:
			`<form id="loginForm">`
			`<div class="form-floating">`
			`<input type="text" class="form-control" id="email" placeholder="Login ID" required>`
			`<label for="email">Login ID</label>`
			`</div>`
			`<div class="form-floating">`
			`<input type="password" class="form-control" id="password" placeholder="Password" required>`
			`<label for="password">Password</label>`
			`</div>`
			`<div class="d-flex justify-content-between align-items-center mb-4">`
			`<div class="form-check">`
			`<input class="form-check-input" type="checkbox" id="rememberMe">`
			`<label class="form-check-label" for="rememberMe">Remember me</label>`
			`</div>`
			`<a href="#" class="text-decoration-none" style="color: #764ba2;">Forgot Password?</a>`
			`</div>`
			`<button type="submit" class="btn btn-login">`
			`Sign In <i class="fas fa-arrow-right ms-2"></i>`
			`</button>`
			`<!-- Designer Credit -->`
			`<div class="text-center mt-3" style="font-size: 0.85rem; color: #666;">`
			`This software is designed by <... (truncated)` Request / Response

Details

Risk description:
Passwords submitted in URLs have a higher chance of being leaked. The main reason is that URLs can be leaked in browser cross-site

requests via the Referer header. Additionally, URLs are usually stored in all kinds of logs. If any access or error logs of the server were publicly accessible, an attacker could also harvest password from it.

Recommendation:
You should submit passwords using POST rather than GET. This way sensitive data won't be shared to other locations via URLs.

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

Classification:
OWASP Top 10 - 2021 : A4 - Insecure Design

Server software and technology found

UNCONFIRMED

port 443/tcp

Software / Version	Category
cdnjs	CDN
Express	Web frameworks, Web servers
Font Awesome 6.0.0	Font scripts
Bootstrap 5.3.0	UI frameworks
HTTP/3	Miscellaneous
Node.js	Programming languages
Chart.js 3.9.1	JavaScript graphics
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

Login Interface Found

CONFIRMED

port 443/tcp

URL	Evidence

https://app.dwatson.online/	`<input type="text" class="form-control" id="email" placeholder="Login ID" required>`
	`<input type="password" class="form-control" id="password" placeholder="Password" required>`
	`<button type="submit" class="btn btn-login">`
	`Sign In <i class="fas fa-arrow-right ms-2"></i>`
	`</button>`
	Request / Response

Details

Risk description:

The risk is that an attacker could use this interface to mount brute force attacks against known passwords and usernames combinations leaked throughout the web.

Recommendation:
Ensure each interface is not bypassable using common knowledge of the application or leaked credentials using occasional password audits.

References:
https://pentest-tools.com/network-vulnerability-scanning/password-auditor
http://capec.mitre.org/data/definitions/16.html

Security.txt file is missing

CONFIRMED

port 443/tcp

URL
Missing: https://app.dwatson.online/.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

Nothing was found for vulnerabilities of server-side software.

Nothing was found for client access policies.

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 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 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 Secure flag of cookie.

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 (38/38)

- ✓ Scanned for missing HTTP header - Strict-Transport-Security
- ✓ Scanned for missing HTTP header - Referrer
- ✓ Scanned for missing HTTP header - Content Security Policy
- ✓ Scanned for login interfaces
- ✓ Scanned for passwords submitted in URLs
- ✓ Scanned for missing HTTP header - X-Content-Type-Options
- ✓ Scanned for website technologies
- ✓ Scanned for version-based vulnerabilities of server-side software
- ✓ Scanned for client access policies
- ✓ Scanned for robots.txt file
- ✓ Scanned for absence of the security.txt file
- ✓ Scanned for use of untrusted certificates
- ✓ Scanned for enabled HTTP debug methods
- ✓ Scanned for enabled HTTP OPTIONS method
- ✓ Scanned for secure communication
- ✓ Scanned for directory listing
- ✓ Scanned for passwords submitted unencrypted
- ✓ Scanned for error messages
- ✓ Scanned for debug messages
- ✓ Scanned for code comments
- ✓ Scanned for domain too loose set for cookies
- ✓ Scanned for mixed content between HTTP and HTTPS
- ✓ Scanned for cross domain file inclusion
- ✓ Scanned for internal error code
- ✓ Scanned for HttpOnly flag of cookie
- ✓ Scanned for Secure flag of cookie
- ✓ Scanned for secure password submission
- ✓ Scanned for sensitive data
- ✓ Scanned for unsafe HTTP header Content Security Policy
- ✓ Scanned for OpenAPI files
- ✓ Scanned for file upload
- ✓ Scanned for SQL statement in request parameter
- ✓ Scanned for password returned in later response
- ✓ Scanned for Path Disclosure
- ✓ Scanned for Session Token in URL
- ✓ Scanned for API endpoints
- ✓ Scanned for emails
- ✓ Scanned for missing HTTP header - Rate Limit

Scan parameters

target:	https://app.dwatson.online/
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:	380ms
Total number of HTTP request errors:	2