Website Vulnerability Scanner Report

✔ **https://allenstown-alt.org/**

Target added due to a redirect from http://allenstown-alt.org

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:

Critical:	0
High:	0
Medium:	0
Low:	5
Info:	3

Scan information:

Start time:	Aug 19, 2026 / 20:15:12 UTC-04
Finish time:	Aug 19, 2026 / 20:15:40 UTC-04
Scan duration:	28 sec
Tests performed:	40
Scan status:	Finished

Findings

Missing security header: Strict-Transport-Security

CONFIRMED

port 443/tcp

URL	Evidence
https://allenstown-alt.org/	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
OWASP Top 10 - 2025 : A02 - Security Misconfiguration

Missing security header: Referrer-Policy

CONFIRMED

port 443/tcp

URL	Evidence
https://allenstown-alt.org/	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
OWASP Top 10 - 2025 : A02 - Security Misconfiguration

Missing security header: Content-Security-Policy

CONFIRMED

port 443/tcp

URL	Evidence
https://allenstown-alt.org/	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-1021
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration
OWASP Top 10 - 2025 : A02 - Security Misconfiguration

Missing security header: X-Content-Type-Options

CONFIRMED

port 443/tcp

URL	Evidence
https://allenstown-alt.org/	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
OWASP Top 10 - 2025 : A02 - Security Misconfiguration

Server software and technology found

port 443/tcp

UNCONFIRMED

Software / Version	Category
Apache HTTP Server	Web servers
Nginx 1.29.8	Web servers, Reverse proxies
DreamWeaver	Editors

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:
CWE : CWE-200
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration
OWASP Top 10 - 2025 : A02 - Security Misconfiguration

Security.txt file is missing

port 443/tcp

CONFIRMED

URL
Missing: https://allenstown-alt.org/.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:
CWE : CWE-1188
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration
OWASP Top 10 - 2025 : A02 - Security Misconfiguration

HTTP OPTIONS enabled

port 443/tcp

CONFIRMED

URL	Method	Summary
https://allenstown-alt.org/	OPTIONS	We did a HTTP OPTIONS request. The server responded with a 200 status code and the header: `Allow: GET,POST,OPTIONS,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
OWASP Top 10 - 2025 : A02 - Security Misconfiguration

Email Address Exposure

port 443/tcp

UNCONFIRMED

URL	Method	Parameters	Evidence
https://allenstown-alt.org/	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	Email Address: allenstown-alt@comcast.net Request / Response
https://allenstown-alt.org/elections/2022/2022-elections.htm	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	Email Address: allenstown-alt@mafware.com Request / Response

Details

Risk description:
The risk is that exposed email addresses within the application could be accessed by unauthorized parties. This could lead to privacy violations, spam, phishing attacks, or other forms of misuse.

Recommendation:
Compartmentalize the application to have 'safe' areas where trust boundaries can be unambiguously drawn. Do not allow email addresses to go outside of the trust boundary, and always be careful when interfacing with a compartment outside of the safe area.

References:
https://owasp.org/Top10/A04_2021-Insecure_Design/

Classification:
CISA KEV: False
CVE : -1
CWE : CWE-200
OWASP Top 10 - 2017 : A6: Security Misconfiguration
OWASP Top 10 - 2021 : A4: Insecure Design
OWASP Top 10 - 2025 : A06 - Insecure Design

Scan coverage information

List of tests performed (40)

Port 443

- ✔ Scanned for missing HTTP header - Content Security Policy
- ✔ Scanned for missing HTTP header - Referrer
- ✔ Scanned for missing HTTP header - Strict-Transport-Security
- ✔ Scanned for missing HTTP header - X-Content-Type-Options
- ✔ Scanned for website technologies

- ✔ Scanned for emails
- ✔ Scanned for enabled HTTP OPTIONS method
- ✔ Scanned for absence of the security.txt file
- ✔ Scanned for version-based vulnerabilities of server-side software
- ✔ Scanned for client access policies
- ✔ Scanned for robots.txt file
- ✔ Scanned for use of untrusted certificates
- ✔ Scanned for enabled HTTP debug methods
- ✔ 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 passwords submitted in URLs
- ✔ 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 login interfaces
- ✔ 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 missing HTTP header - Rate Limit
- ✔ Scanned for PEM-encoded private key material
- ✔ Scanned for partial PEM-encoded private key material

Scan parameters

target:	https://allenstown-alt.org/
scan_type:	Light
authentication:	False

Scan stats

Unique Injection Points Detected:	133
URLs spidered:	13
Total number of HTTP requests:	22
Average time until a response was received:	353ms