

Six Simple Data Security Self-Tests

*(Find Your Security
Holes Before the
Hackers Do)*

for
Manufacturers, Reps, and Distributors

Prepared by

James Thomas
CTO, Flow RMS

Curtis Seare
CEO, Flow RMS

Table of Contents

Introduction	03
<hr/>	
Test 1: HTTPS Check	04
<hr/>	
Test 2: Security Headers	05
<hr/>	
Test 3: Browser Errors	07
<hr/>	
Test 4: Password Practices	08
<hr/>	
Test 5: Credentials Exposure	09
<hr/>	
Test 6: Publicly Known Vulnerabilities	10
<hr/>	
Conclusion	11

Introduction

Data security isn't optional—especially if you're a manufacturer, rep, or distributor managing sensitive customer data. One breach can wreck your reputation, lose your business, and cost you millions in compliance penalties. But here's the good news: securing your systems doesn't have to be complicated.

This paper walks you through six practical, no-nonsense tests you can run today to evaluate your data security. These tests are quick, actionable, and designed for people who don't have time to waste on fluff. If you've ever worried about vulnerabilities in your systems—or if you've put off thinking about them altogether—this is your wake-up call.

Skip the jargon and finger-pointing. These six tests are your starting point for identifying weak spots, fixing them, and sleeping better at night knowing your data is locked down tight.

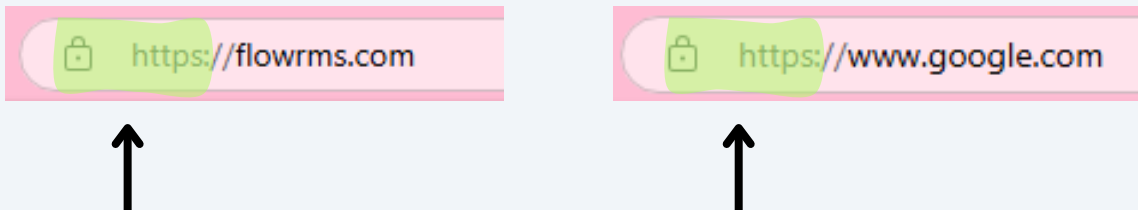
KEEP IN MIND:

All of these tests should be conducted on the login page of the software you are testing. This is the gateway to your system and often the first place hackers will attack. Ensuring it's secure is one of the best defenses against potential breaches.

Special note: These test works well for traditional server builds, but are too simple for more advanced and modern security setups like you'll see at Flow RMS, which uses strict-transport protocols, etc. But they are a good starting point to take to your vendors with the results and see if they have explanations.

Test One: HTTPS

Check for HTTPS – Start by ensuring the login page is served over HTTPS. If the URL doesn't start with "https://", data sent through that page, including your login credentials, might not be encrypted. This is an instant red flag that needs to be addressed.



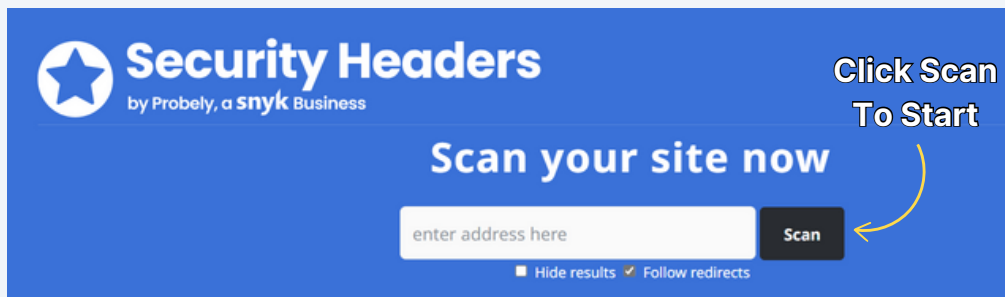
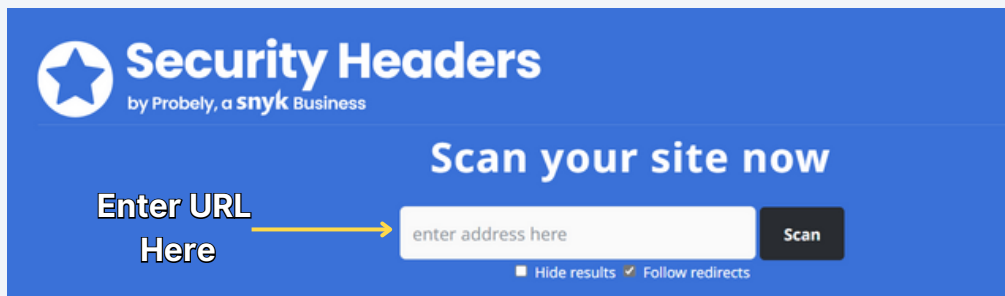
Secure connection: HTTPS encrypts data to protect your credentials

If the URL starts with 'http://' (no 's'), your data may not be secure. Look for the lock icon or 'https://' to ensure encryption

Test Two: Security Headers

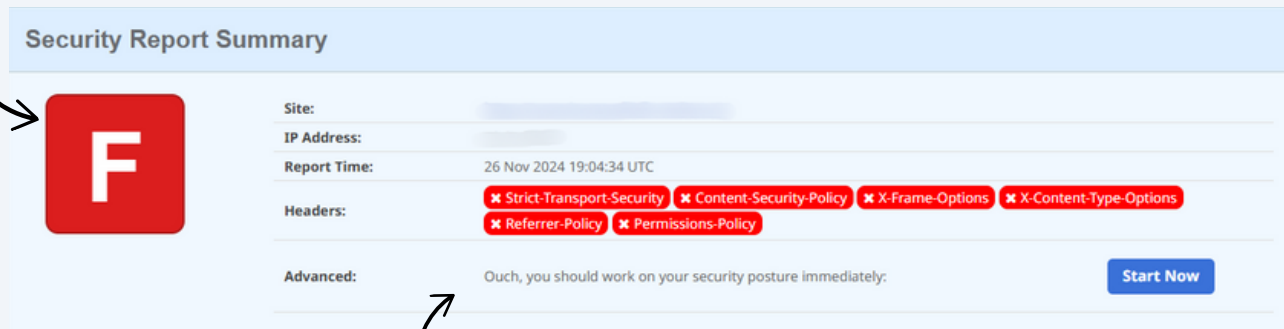
Run a Security Header Scan—Use a free tool like securityheaders.com to check whether your login page uses up-to-date security headers.

Security headers help prevent a wide range of attacks, such as cross-site scripting and clickjacking.



Test Two: Security Headers

This 'F' grade means the platform is missing key security protections.

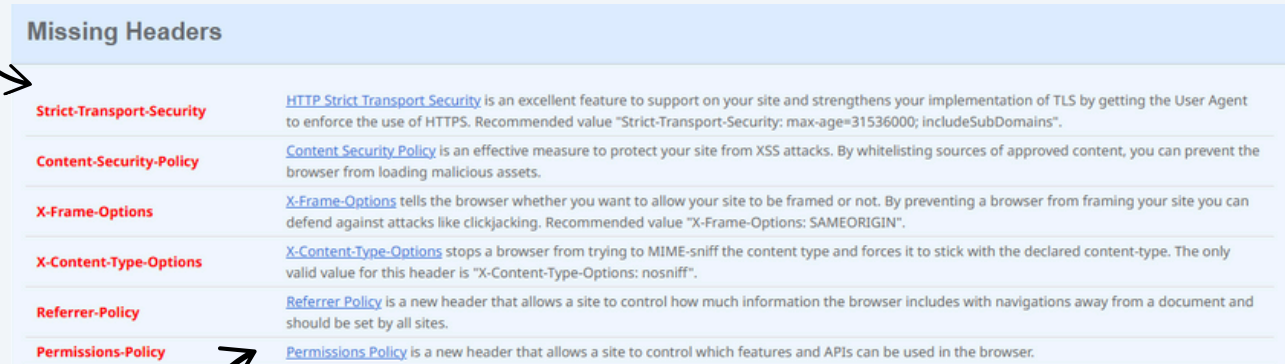


The screenshot shows a 'Security Report Summary' with a large red 'F' grade icon. The report details the following information:

- Site:** [Redacted]
- IP Address:** [Redacted]
- Report Time:** 26 Nov 2024 19:04:34 UTC
- Headers:** A list of missing headers: Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, and Permissions-Policy. Each header name is enclosed in a red box with a white 'X' on the left.
- Advanced:** Ouch, you should work on your security posture immediately. [Start Now button]

These missing headers (like 'Strict-Transport-Security') help protect against attacks—this is a security risk.

These missing security features protect your site from attacks like hacking and phishing.



The screenshot shows a 'Missing Headers' table with the following entries:

Header Name	Description
Strict-Transport-Security	HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS. Recommended value "Strict-Transport-Security: max-age=31536000; includeSubDomains".
Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

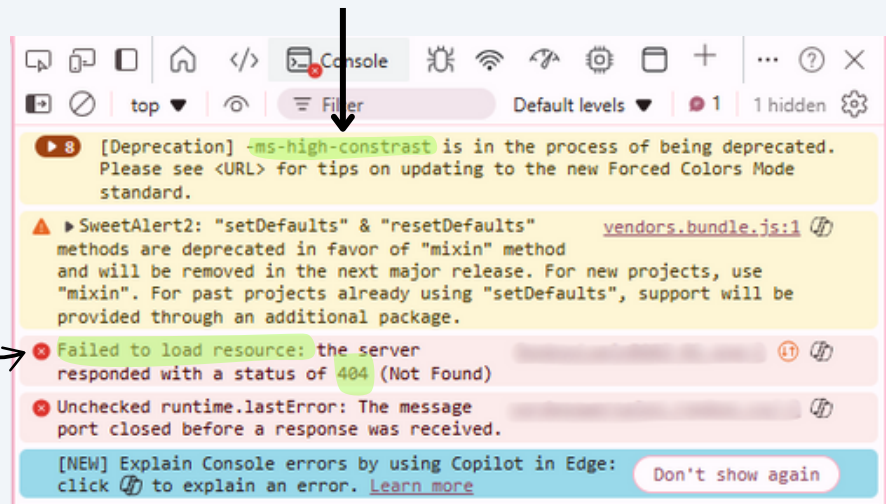
Content-Security-Policy helps block harmful scripts (small programs that run on websites) from being used by hackers.

Test 3: Browser Errors

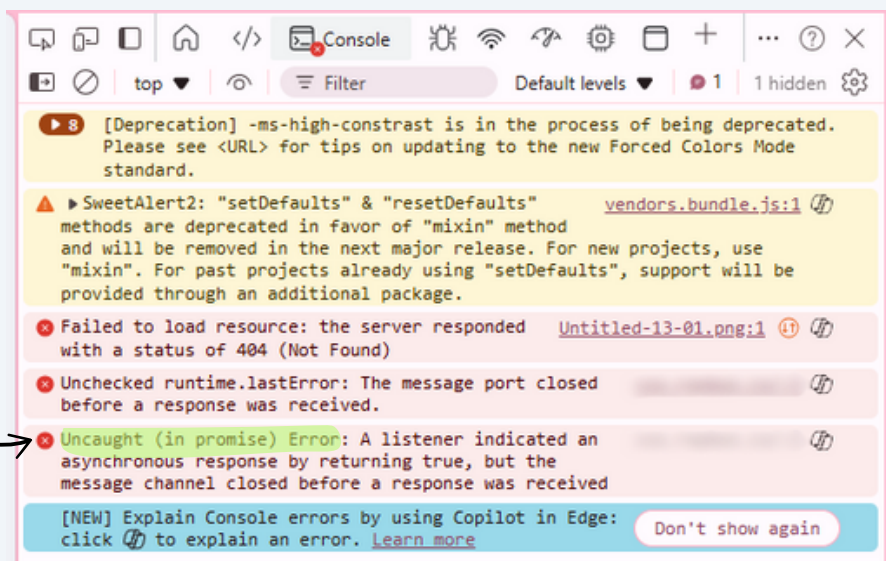
Inspect Browser Console for Errors – Open your browser's developer tools (usually F12 or right-click > Inspect) and check the console for errors. If you see deprecated technology or vulnerable JavaScript libraries, your system might run on outdated code, leaving you open to attack.

This feature is outdated and may stop working in future browser updates.

A file is missing, which could break part of the page.



A coding issue could cause the page not to work.



Test Four: Password Practices

Test Password Practices—Try setting a weak password to see if the system enforces password complexity. Strong systems should require at least eight characters, a mix of uppercase and lowercase letters, numbers, and special characters. Anything less can make your system vulnerable to brute-force attacks.

What Makes a Good Password

- Long: At least 8-12 characters. The longer, the better.
 - Example: "Z3bRa\$Ro@d56"
- Mix of Characters: Include uppercase and lowercase letters, numbers, and special symbols (e.g., @, #, \$, !).
- Unique: Use a different password for each account (e.g., Facebook, email, banking).
- Unpredictable: Avoid real words or common phrases. Combine random characters.
 - Example: "Z3bRa\$Ro@d56" is better than "Password123."

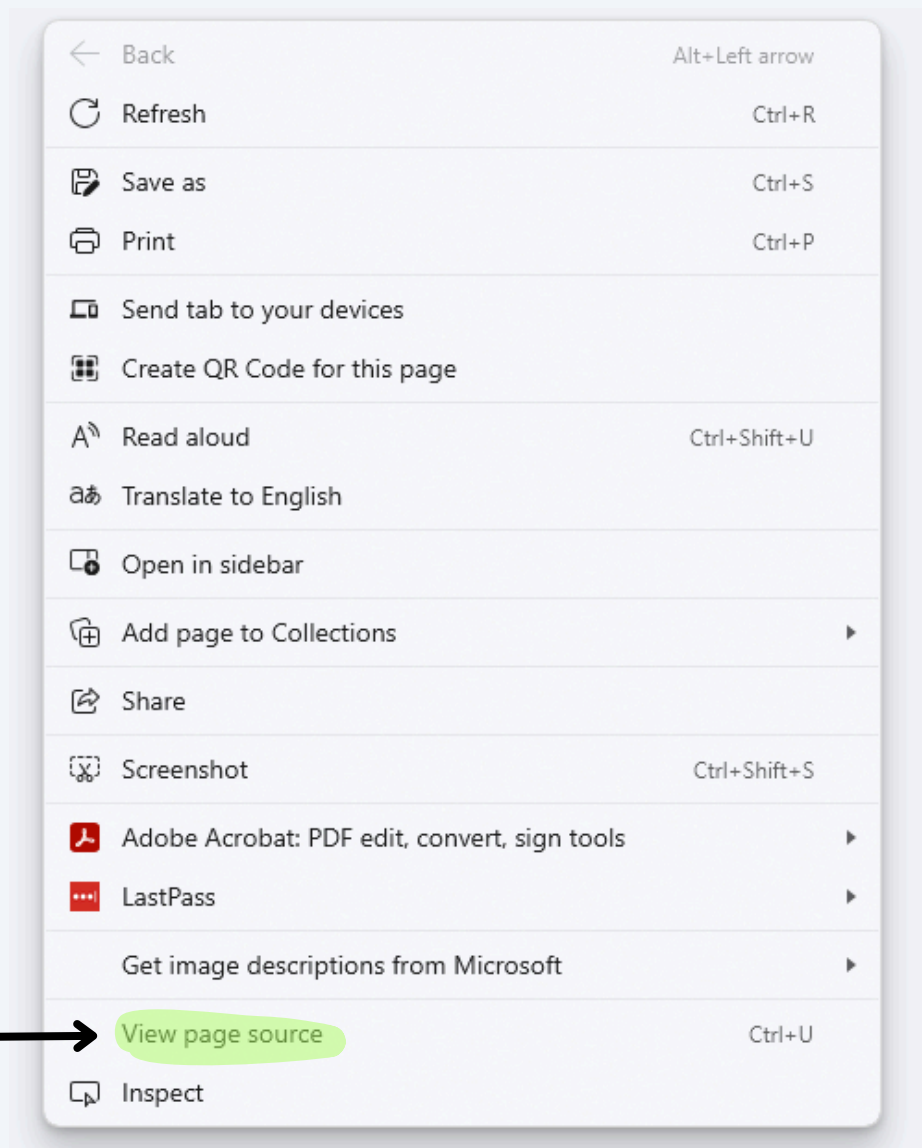
What Makes a Bad Password

- Short: Less than 8 characters (e.g., "12345" or "abc123").
- Predictable: Passwords like "password", "123456", or "qwerty" are too easy to guess.
- Personal Info: Avoid names, birthdays, or pets (e.g., "John1985").
- Common Phrases: Don't use phrases like "iloveyou" or "letmein."
- Reused Passwords: Never use the same password across different sites—one breach can compromise all your accounts.

Test 5: Credentials Exposure

You can perform a basic search in the page's source code (right-click > View Source) for any hard-coded database credentials or sensitive information. If you can see any credential-related information, your system exposes a massive security hole.

Right-click, then choose 'View Source' or something similar (depends on your browser).



Test 6: Publicly Known Vulnerabilities

Use tools like [Snyk](#), [OWASP](#), or [ImmuniWeb](#) to see if your system uses third-party libraries with known vulnerabilities. An up-to-date system should have patched these vulnerabilities immediately.

Outdated software found—update immediately to fix known security issues.

Web Software Security Test

Web Software Found	Web Software Outdated	Web Software Vulnerabilities
20	15	13

Fingerprinted CMS & Vulnerabilities ⓘ

No CMS were fingerprinted on the website. [Information](#)

Fingerprinted CMS Components & Vulnerabilities ⓘ

jQuery 1.12.4

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities. Urgently update to the most recent version **3.7.1**.

CVSSv3.1 Score	Vulnerability CVE-ID CVE	Vulnerability Type
5.5 Medium	CVE-2020-11022	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2015-9251	CWE-79 - Cross-site scripting
4.8 Medium	CVE-2019-11358	CWE-1321 - Prototype pollution
4.1 Medium	CVE-2020-11023	CWE-79 - Cross-site scripting

Critical vulnerabilities detected in third-party components—patching is essential to protect user data.

Conclusions

If you made it through all six tests, congratulations—you're already ahead of most in your industry. You've identified key vulnerabilities and know exactly where you stand. But don't stop here. Data security isn't a "set it and forget it" deal. It's a constant process of evaluating, updating, and staying ahead of threats.

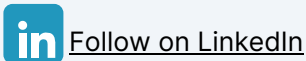
The truth is, bad actors don't take breaks, and neither should your commitment to security. By tackling these self-tests regularly and addressing any gaps, you're building a foundation of trust with your customers and partners. That trust? It's your most valuable asset in today's market.

Don't wait for a breach to wake you up. Take charge, fix what's broken, and invest in tools and processes to stay one step ahead. Your business, your clients, and your reputation will thank you for it.

About the Authors



James Thomas
CTO, Flow RMS



James Thomas is the CTO and co-founder of Flow RMS, specializing in data security, artificial intelligence, and scalable enterprise-grade software. Previously, he built secure, data-driven technologies for United Health Group, addressing the complex needs of a global market. He also co-founded Data Crunch, a Fortune 5000 data consultancy, and helped lead it to a successful acquisition in 2023. With a passion for innovation, James drives Flow RMS's vision for AI-powered transformation across industries.

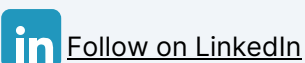
[Work with James](#)

Get a demo of Flow: FlowRMS.com

Subscribe to the Flowing Sales podcast: FlowingSales.com



Curtis Seare
CEO, Flow RMS



Curtis Seare is the CEO and founder of Flow RMS, a company building the AI-First ERP for manufacturers, reps, and distributors. He co-founded Data Crunch, a Fortune 5000 data consulting firm acquired in 2023, and hosted the Popular Data Crunch Podcast, where he explored AI and data science in business innovation. With a focus on efficiency, Curtis leads AI-powered transformation in industrial sectors.

[Work with Curtis](#)

Get a demo of Flow: FlowRMS.com

Subscribe to the Flowing Sales podcast: FlowingSales.com