UJAR TECH SOLUTION

NAME: Rithik varma

INTERN ID: UTS1103

TASK 3

Analyze Website Security Headers Using Online Tools:

Understand and practically analyze the security headers of a website and understand how they protect users from common attacks like XSS, clickjacking, and content sniffing.

PRACTICAL DESCRIPTION

Problem:- *Explore Web browser Free online tools: o securityheaders.com and analyze missing headers such as: X-Frame-Options , Content-Security-Policy , Strict-Transport-Security , X-XSS-Protection.*

Website Security Headers:

When you open a website, your browser requests the page from the server.
*Along with the webpage, the server sends **HTTP Response Headers**.*
*Some of these are **security headers** that tell your browser how to handle the content safely.*

They protect against:

- ***XSS (Cross-Site Scripting)***
- ***Clickjacking***
- ***Content sniffing attacks***
- ***Unsecured connections (HTTP vs HTTPS)***

Common Security Headers are:-

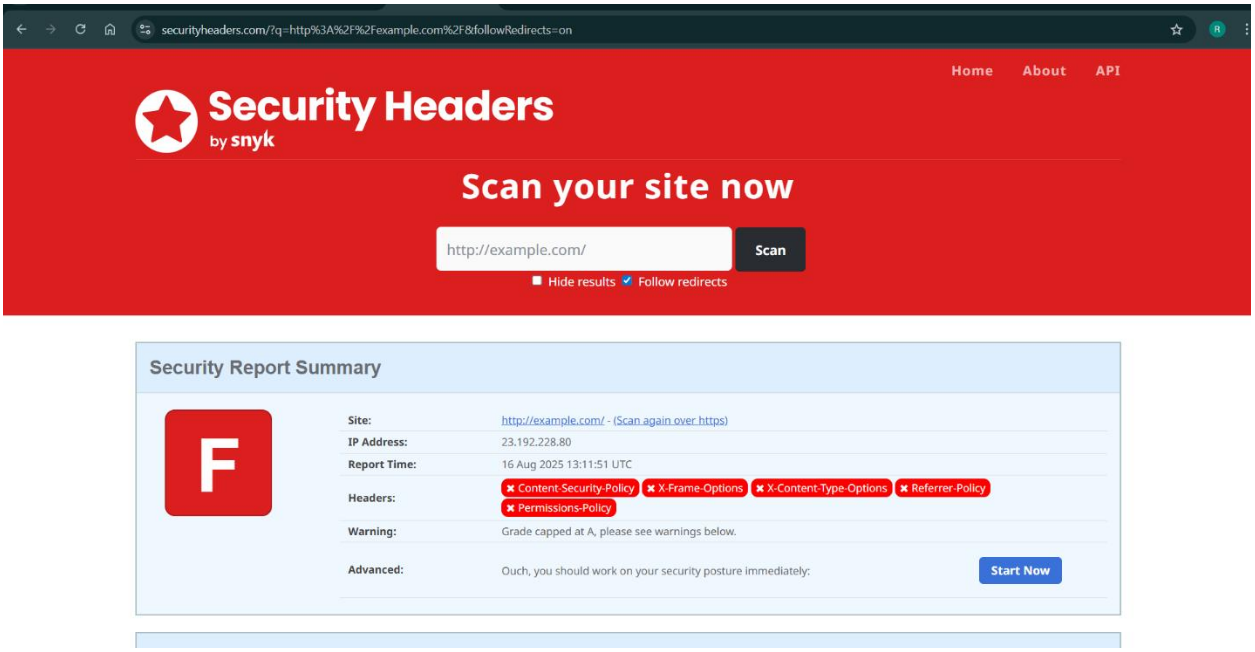
1. ***Strict-Transport-Security (HSTS)***
   - *Forces browsers to use HTTPS only.*
   - *Protects against downgrade attacks.*
2. ***Content-Security-Policy (CSP)***

- *Controls which scripts, images, and resources can load.*
- *Strong defense against **XSS attacks**.*

3. *X-Frame-Options*** **
   - *Stops your website from being embedded in another site's iframe.*
   - *Prevents **clickjacking**.*
4. ***X-Content-Type-Options***
   - *Prevents browsers from guessing file types incorrectly.*
   - *Stops **content sniffing attacks**.*
5. ***X-XSS-Protection** (older browsers only)*
   - *Blocks reflected XSS attacks.*
6. ***Referrer-Policy***
   - *Controls how much referrer info is shared when a user clicks a link.*
7. ***Permissions-Policy (Feature-Policy)***
   - *Controls browser features like camera, microphone, geolocation.*

Analyzing Website Security Headers:-

1. Example.com -



securityheaders.com/?q=http%3A%2F%2Fexample.com%2F&followRedirects=on
Home
About
API
Security Headers
by snyk
Scan your site now
http://example.com/
Scan
☐ Hide results ☑ Follow redirects
F
Start Now

Security Report Summary

Site:	http://example.com/ - (Scan again over https)
IP Address:	23.192.228.80
Report Time:	16 Aug 2025 13:11:51 UTC
Headers:	✖ Content-Security-Policy ✖ X-Frame-Options ✖ X-Content-Type-Options ✖ Referrer-Policy ✖ Permissions-Policy
Warning:	Grade capped at A, please see warnings below.
Advanced:	Ouch, you should work on your security posture immediately:

*We have scanned the website with the **url-example.com** in **Security Headers** platform and gained the result (**F**) as u can see in image above .*

headers were missing are :-

1. Content-Security-Policy (CSP)

- ***Protects Against:***
  - *Cross-Site Scripting (XSS) attacks, where malicious scripts run on your site.*

    - *Data injection attacks (e.g., loading scripts/images from untrusted sources).*
- ***How it Helps:***
    - *Lets you specify trusted sources for scripts, images, CSS, etc.*
    - *Example: only allow scripts from yourdomain.com.*
- ***Improvement:***

  *Add a strict CSP like**:***

  (Content-Security-Policy: default-src 'self'; script-src 'self')

2. X-Frame-Options

- ***Protects Against:***
    - *Clickjacking (where attackers embed your site in a hidden frame and trick users into clicking).*
- ***How it Helps:***
    - *Blocks your site from being loaded inside an iframe unless allowed.*
- ***Improvement:***
    - *Add:*

      (X-Frame-Options: SAMEORIGIN)

3. X-Content-Type-Options

- ***Protects Against:***
  - ***MIME type sniffing*** *attacks (where browsers guess file type and execute malicious content).*
- ***How it Helps:***
  - *Forces browser to follow declared content type.*
- ***Improvement:***
  - *Add:*

  (X-Content-Type-Options: nosniff)

Referrer-Policy

- ***Protects Against:***
  - ***Information leakage*** *through HTTP referrer headers (like leaking full URLs, query strings, or session IDs to external sites).*
- ***How it Helps:***
  - *Controls how much referrer info is shared when navigating to another site.*
- ***Improvement:***

  Use a restrictive policy, e.g.:

(Referrer-Policy: no-referrer-when-downgrade)

5. Permissions-Policy (formerly Feature-Policy)

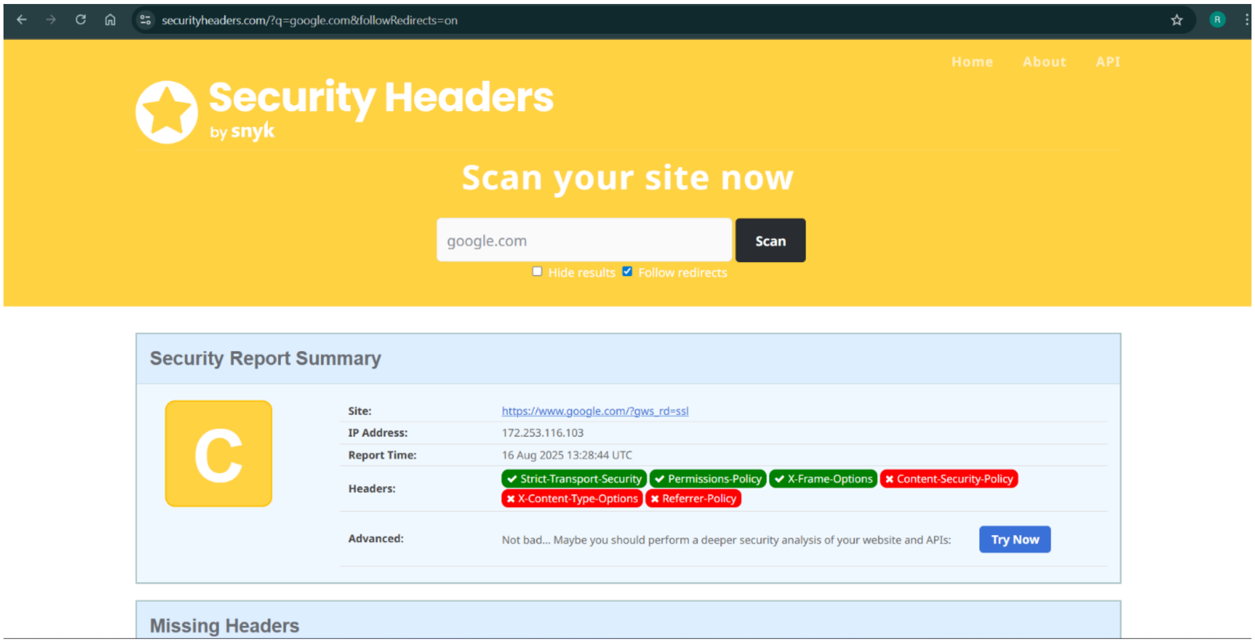
- ***Protects Against:***
  - *Abuse of **browser features** like camera, microphone, location, fullscreen, etc.*
- ***How it Helps:***
  - *Restricts access to powerful APIs unless explicitly allowed.*
- ***Improvement:***
  - *Example:*

(Permissions-Policy: geolocation=(), microphone=(), camera=())

How Websites(example.com) Can Improve:-

- *Add missing headers → If a scan shows they are absent, configure them in your web server (Apache, Nginx, IIS).*
- *Keep policies strict → Don't use overly permissive CSP or Referrer-Policy.*
- *Test after applying → Sometimes headers can block legitimate content if misconfigured.*
- *Combine with TLS (HTTPS) → Headers work best when traffic is encrypted.*

2. Google.com –


securityheaders.com/?q=google.com&followRedirects=on
Home
About
API
Security Headers
by snyk
Scan your site now
google.com
Scan
□ Hide results ☑ Follow redirects

Security Report Summary

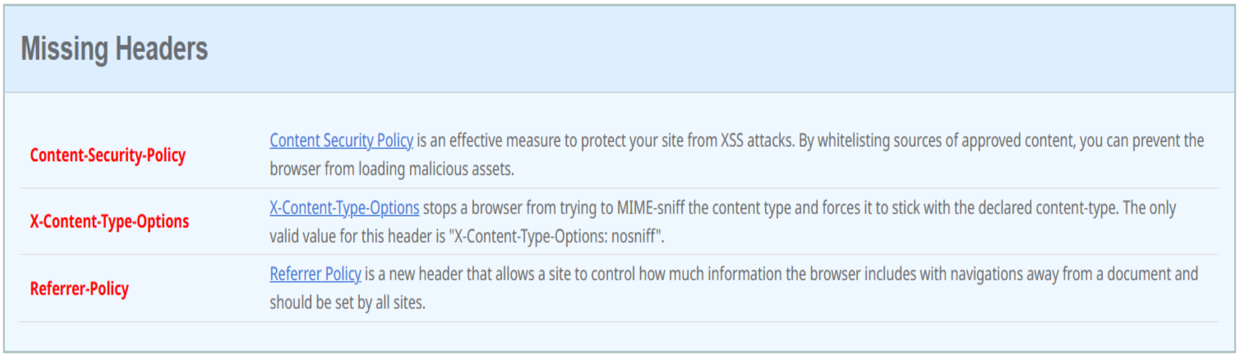
C

Site:	https://www.google.com/?gws_rd=ssl
IP Address:	172.253.116.103
Report Time:	16 Aug 2025 13:28:44 UTC
Headers:	✓ Strict-Transport-Security ✓ Permissions-Policy ✓ X-Frame-Options ✗ Content-Security-Policy ✗ X-Content-Type-Options ✗ Referrer-Policy
Advanced:	Not bad... Maybe you should perform a deeper security analysis of your website and APIs: Try Now

Missing Headers

We have scanned the website with the ***url-google.com*** *in* ***Security Headers*** *platform and gained the result (**C**) as u can see in image above .*

headers were missing are :-



Missing Headers

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-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.

How the Website Could Improve in case of (CSP):

- *Define a strict CSP to control what resources can load.*
- *Example:*

  (Content-Security-Policy: default-src 'self'; script-src 'self' https://trusted.cdn.com; object-src 'none')

  This blocks malicious scripts and allows only trusted resources.

How the Website Could Improvein case of (X-Content-Type-Options):

- *How the Website Could Improve:*
  - *Always set to nosniff.*
  - *Example:*

    (X-Content-Type-Options: nosniff).

  Ensures browsers only execute files with the correct declared type.

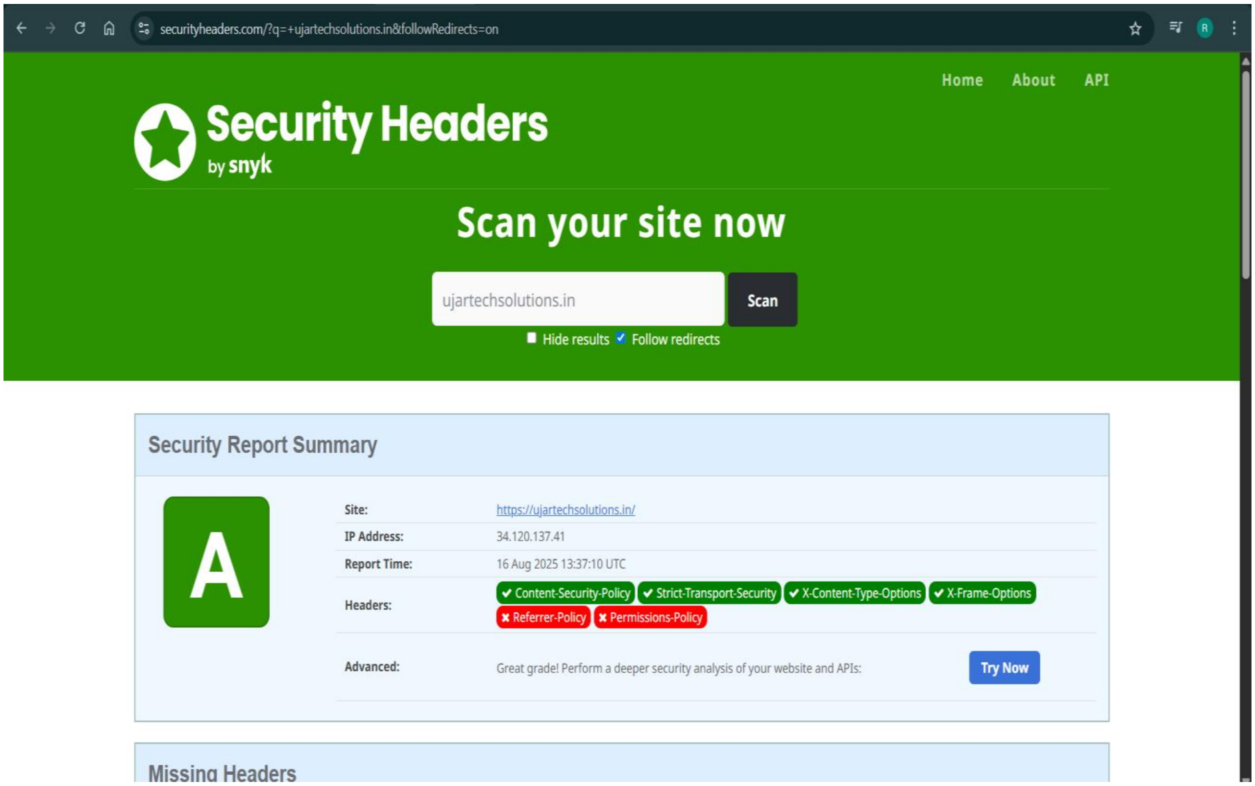
How the Website Could Improvein case of (Referrer-Policy):

- *Set a strict referrer policy to limit what information is shared.*
- *Example:*

(Referrer-Policy: strict-origin-when-cross-origin)

This way, only the domain is shared across sites (not the full path/query), reducing privacy and data leakage risks.

3. ujartechsolutions.in—



securityheaders.com/?q=+ujartechsolutions.in&followRedirects=on

ujartechsolutions.in

☐ Hide results ☑ Follow redirects

Security Report Summary

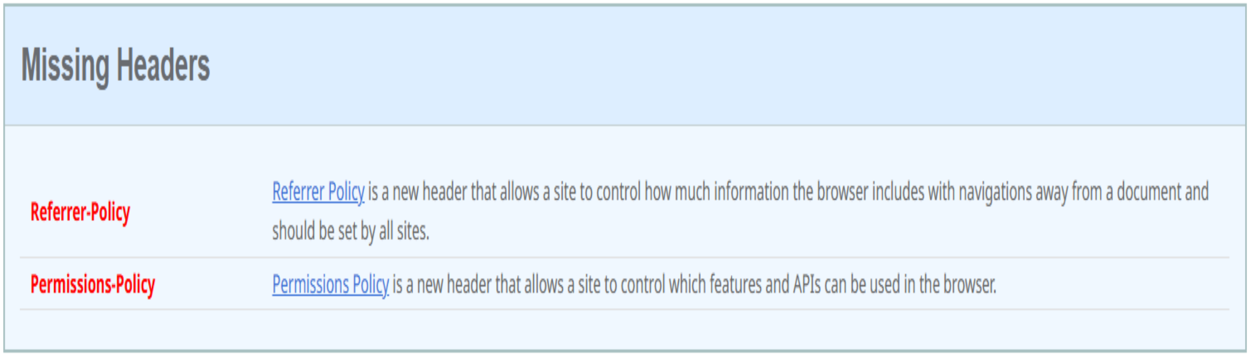
A

Site:	https://ujartechsolutions.in/
IP Address:	34.120.137.41
Report Time:	16 Aug 2025 13:37:10 UTC
Headers:	✓ Content-Security-Policy ✓ Strict-Transport-Security ✓ X-Content-Type-Options ✓ X-Frame-Options ✗ Referrer-Policy ✗ Permissions-Policy
Advanced:	Great grade! Perform a deeper security analysis of your website and APIs:

Missing Headers

We have scanned the website with the ***url-google.com*** *in* ***Security Headers*** *platform and gained the result (****A****) as u can see in image above, but as we can see missing Headers policy which can be fixed to Maximise the secure .*

headers were missing are :-



Missing Headers

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.

Header	***Protects Against***	***How to Improve***
Referrer-Policy	*Info leakage via Referer header (URLs, tokens, query params)*	*Use strict-origin-when-cross-origin for a balanced privacy + functionality*
Permissions-Policy	*Abuse of browser features (camera, mic, location, autoplay)*	*Disable unused features; explicitly allow only trusted origins*