**ANALYSING WEBSITE SECURITY HEADERS USING ONLINE TOOLS**

**-SWASTHIK C SHETTY**

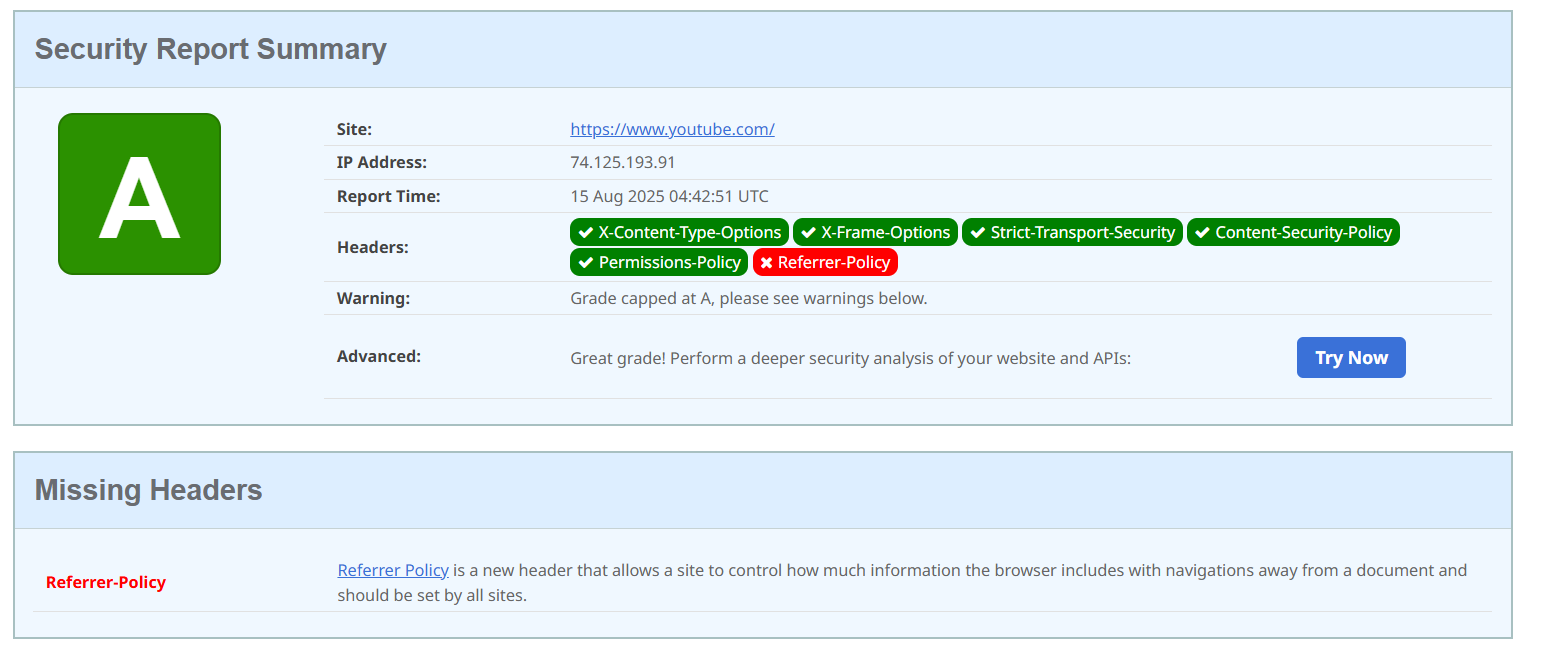
**DATE:15 AUGUST 2025**

**Introduction**

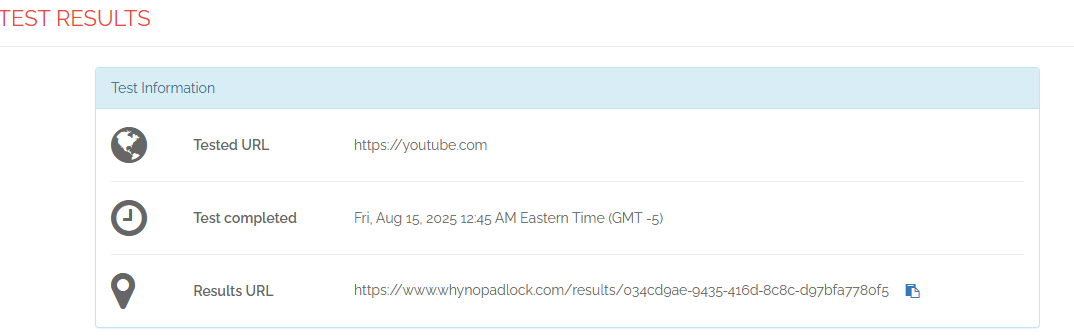
Security headers are HTTP response settings that tell browsers how to handle website content securely. They help protect against attacks like XSS, Clickjacking, and Content Sniffing. In this task, we used SecurityHeaders.com and WhyNoPadlock.com to scan websites, identify missing or misconfigured headers, and suggest improvements based on best practices.

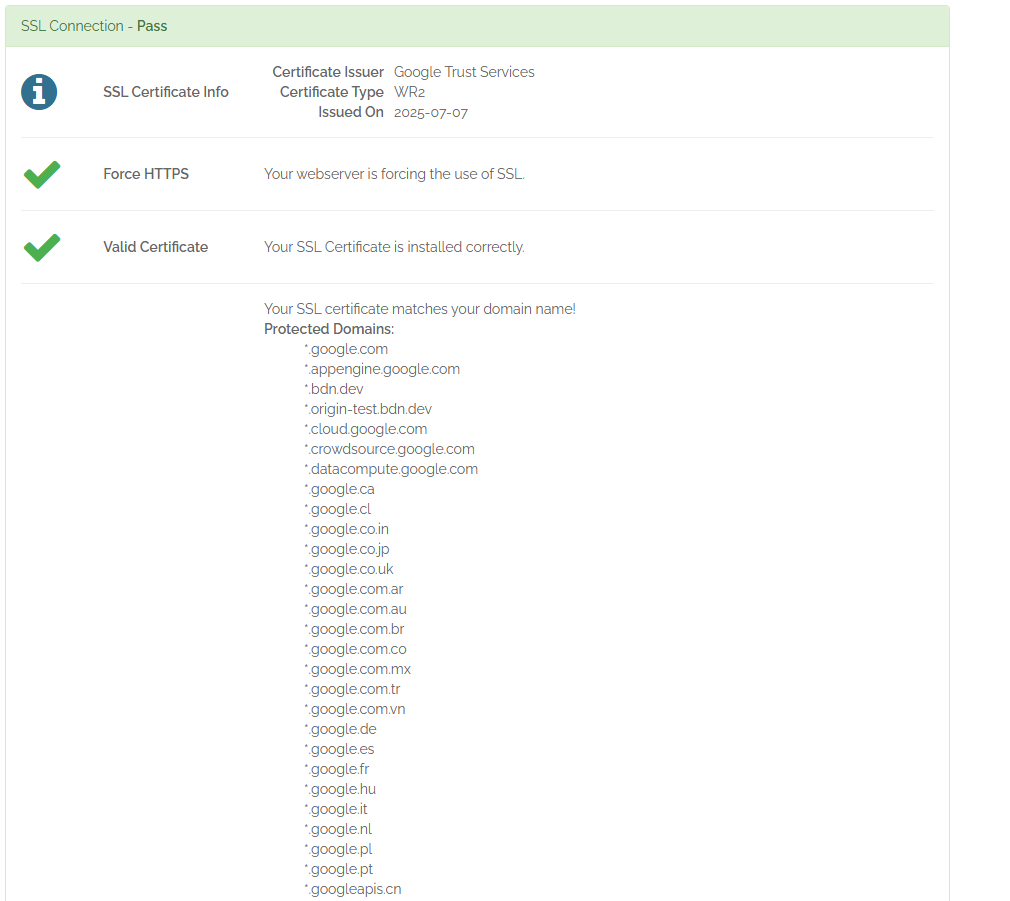
**Results**

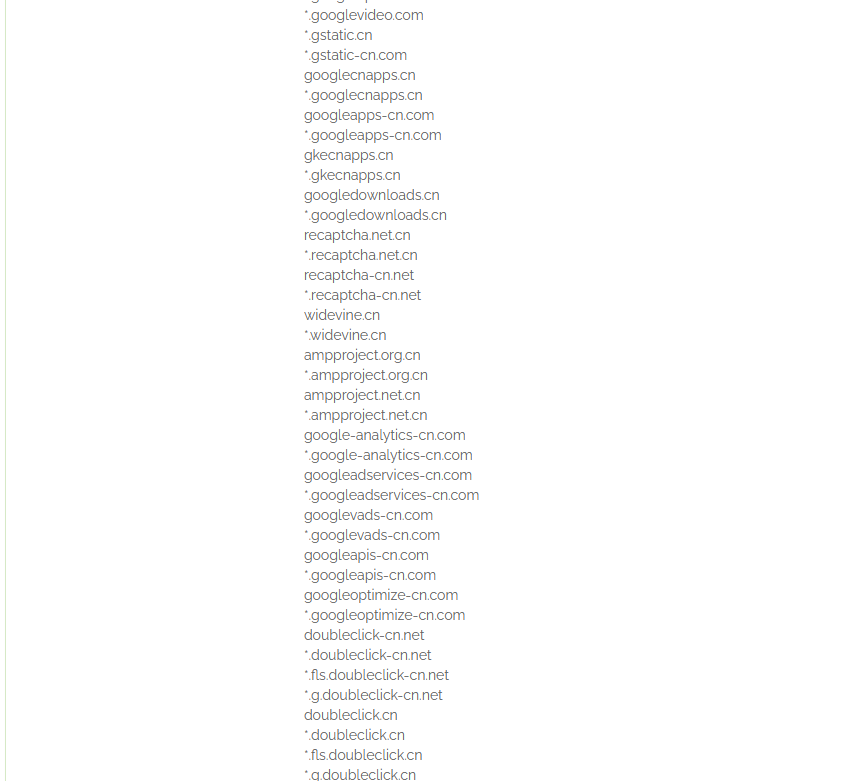
Youtube.com

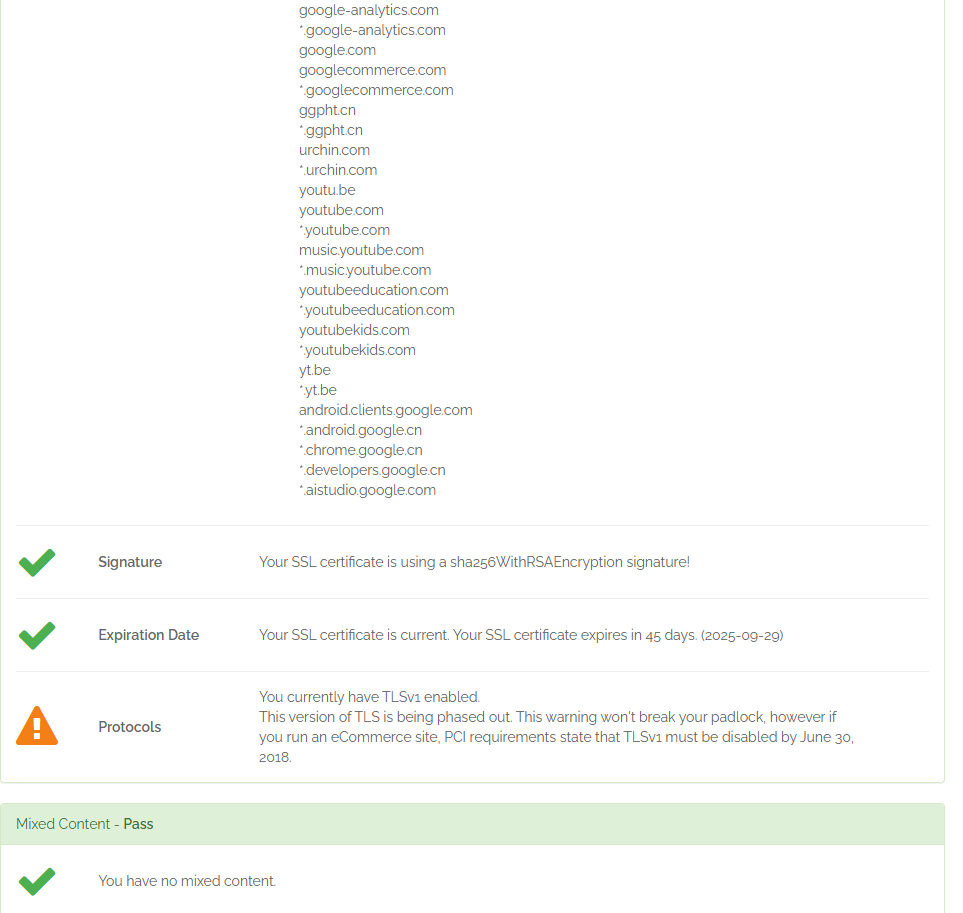


Img 1.1



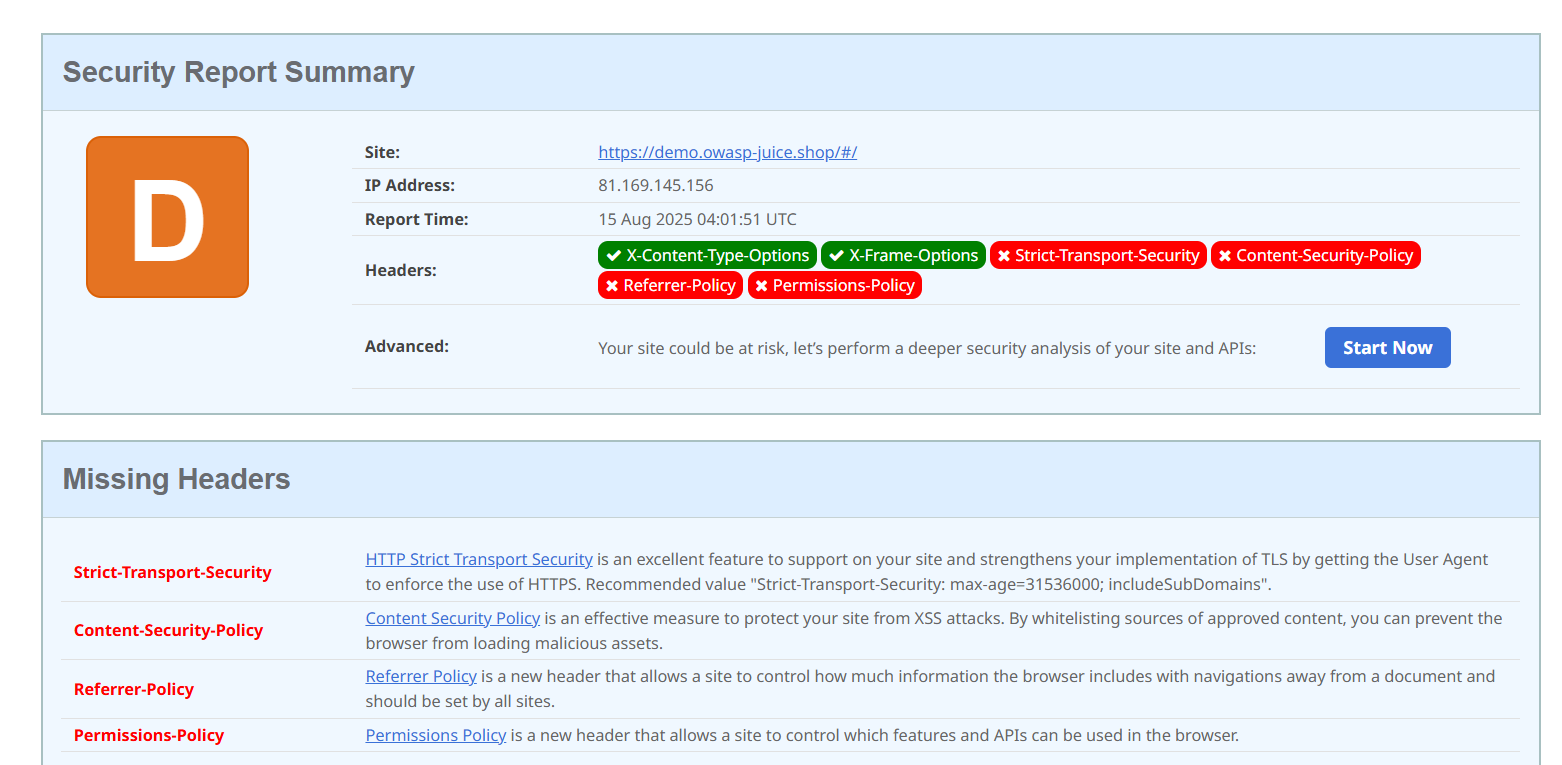


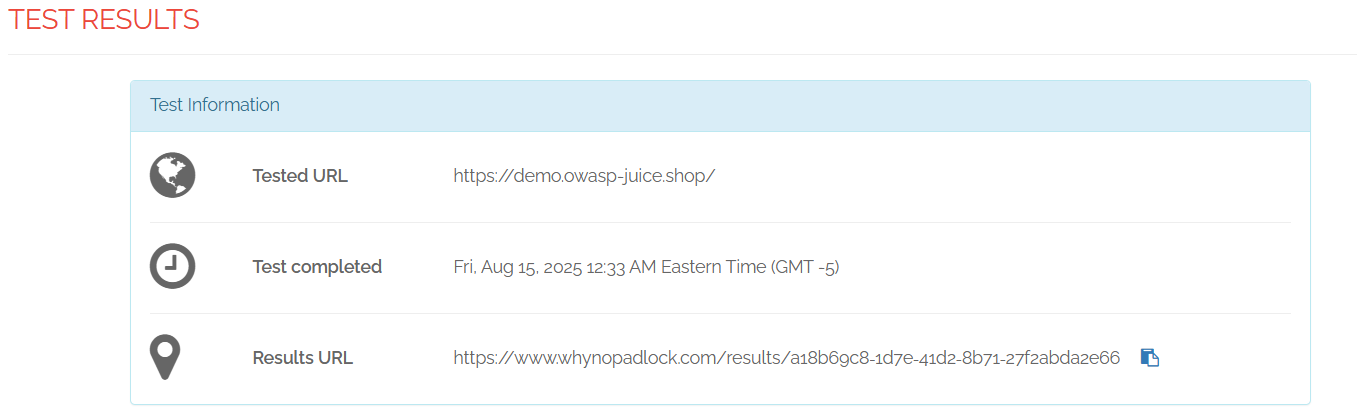


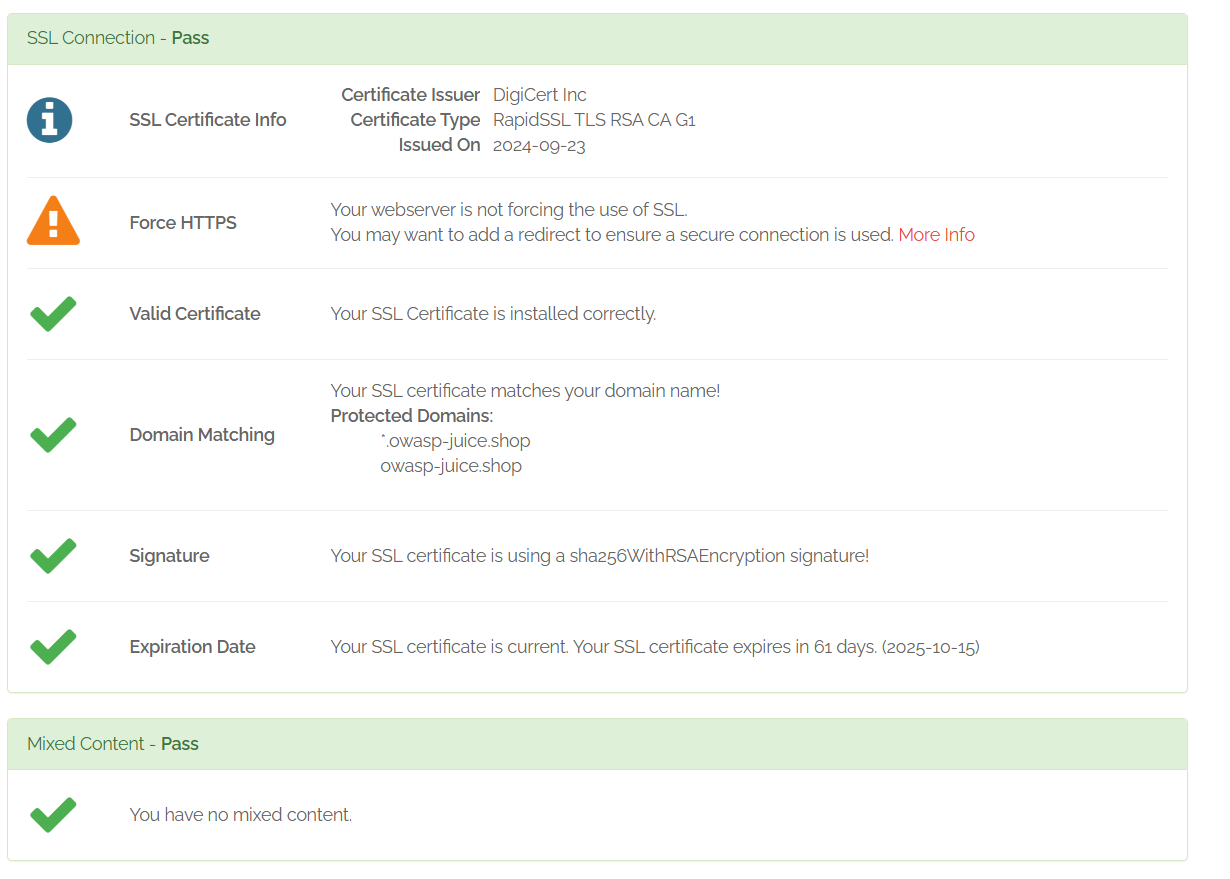


* In the above security report we can see that youtube.com is the Grade A website all the headers are there except “Referrer-Policy” which is the new header this helps to protect user privacy and reduces information exposure.
* In the above test result we can see that all the connections are encrypted and the certificates are valid several other goggle sub domains are protected.SSl uses sha256 with RSA Enscryption signature which expires in 45 days.Protocol supports an outdated TLSv1.

Owasp-juice.shop

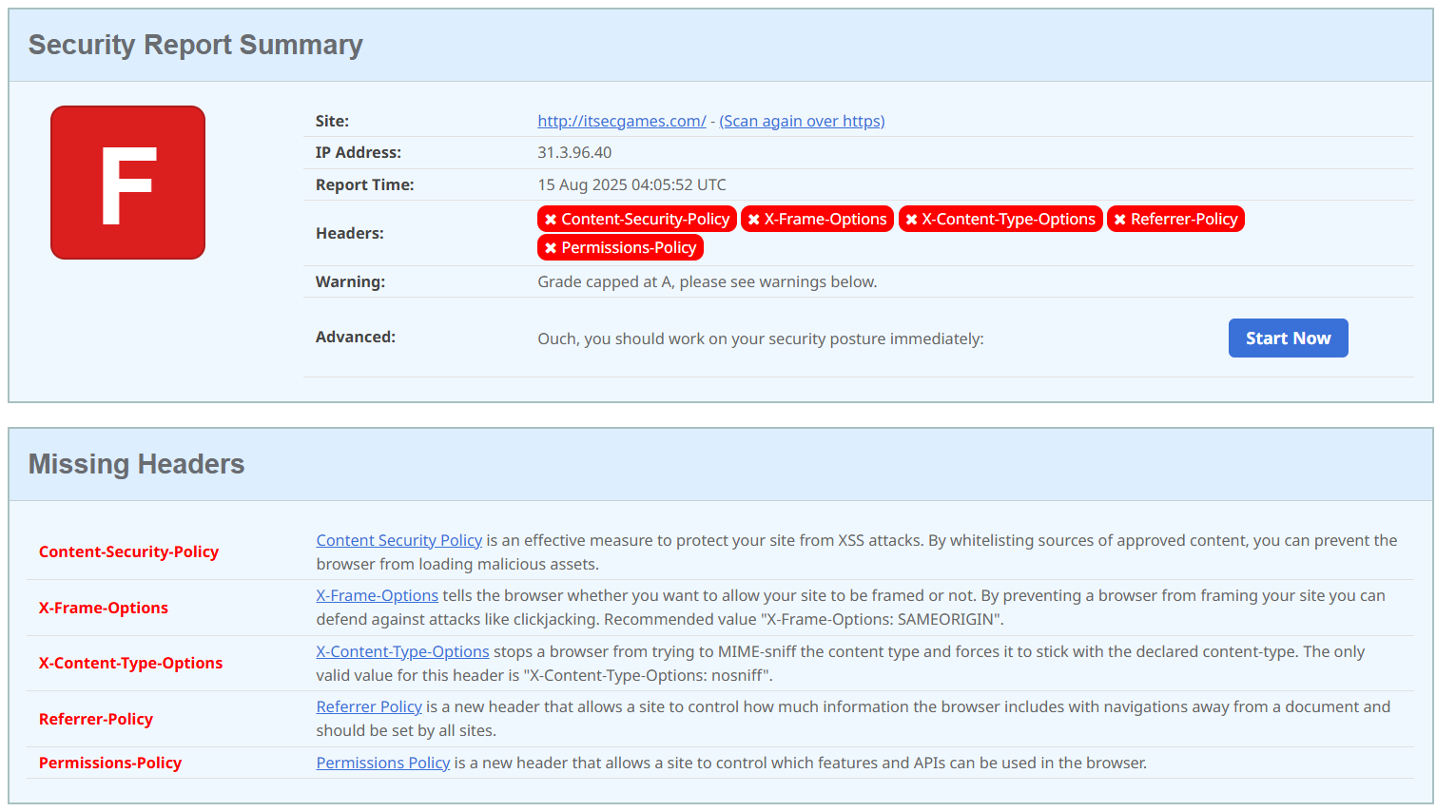


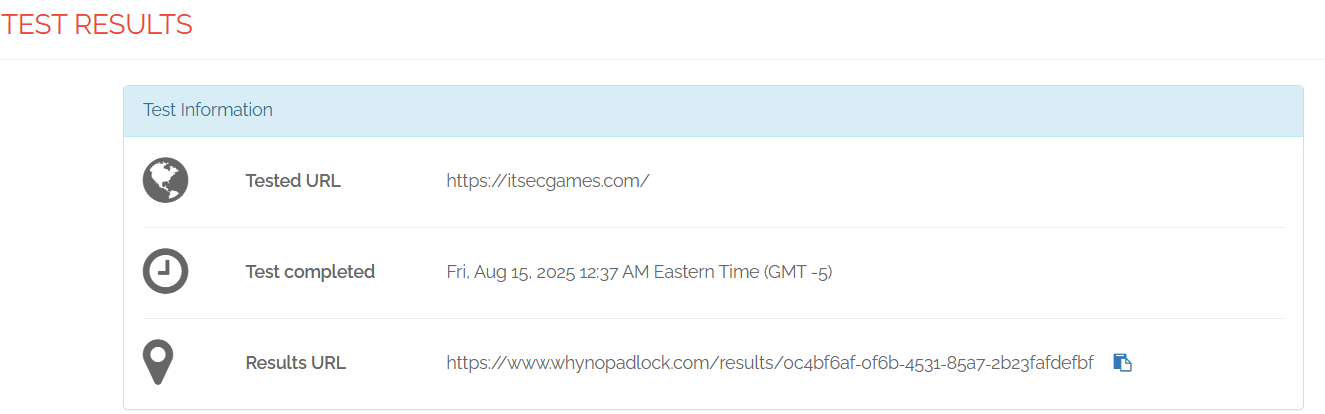


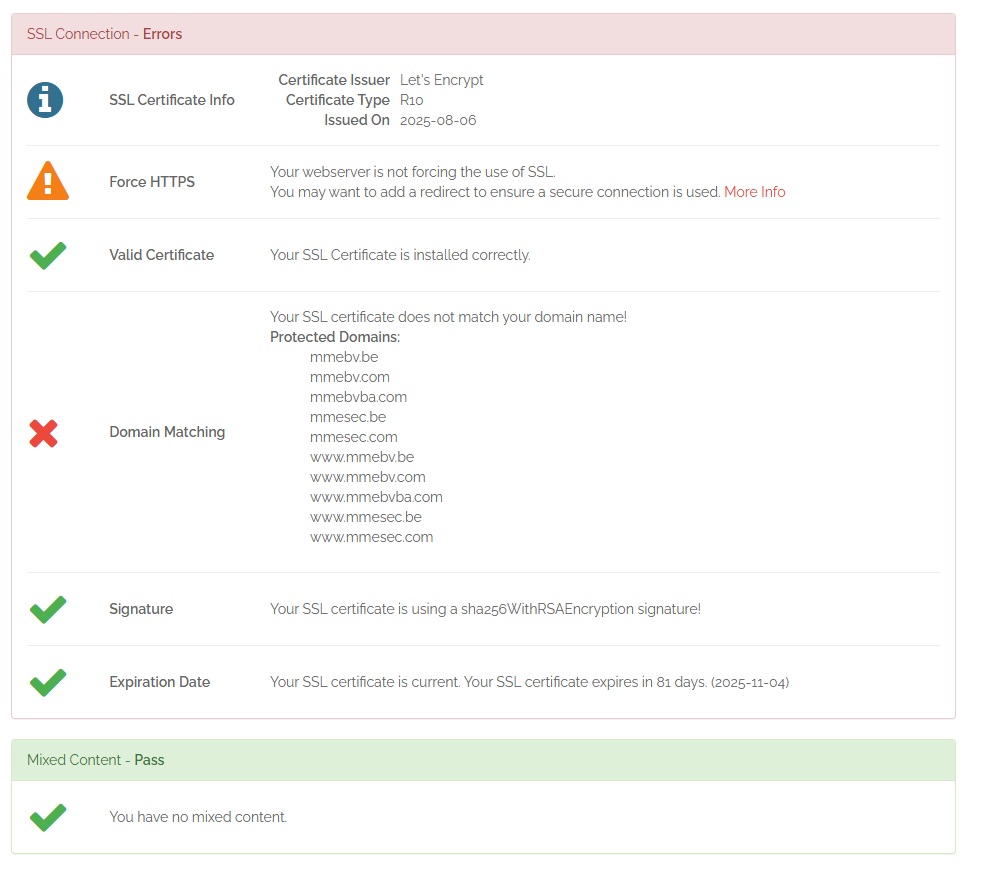


* In the above security report we can see that owasp-juice.com is the Grade D website which is missing headers like
  + **Strict-Transport-Security :** It forces browsers to connect to a website only over HTTPS, preventing insecure HTTP connections and protecting against SSL stripping attacks.
  + **Content-Security-Policy (CSP):** It limits what content a browser can load for a website. It helps prevent Cross-Site Scripting (XSS) and data injection attacks by only allowing resources from trusted sources.
  + **Referrer-Policy:** It controls how much referrer information the browser sends when navigating to another site. It protects user privacy and prevents leaking sensitive data in URLs.
  + **Permissions-Policy:** It controls which browser features (like camera, microphone) a site or its iframes can use. It helps reduce the attack surface by disabling unused or risky features.
* In the above test results OWASP Juice Shop uses a valid SSL certificate issued by DigiCert (RapidSSL TLS RSA CA G1) with domain matching and SHA256WithRSAEncryption. The certificate is valid until 15 October 2025, and no mixed content was detected. However, the site does not enforce HTTPS, allowing access over unsecured HTTP.

Itsecgames.com

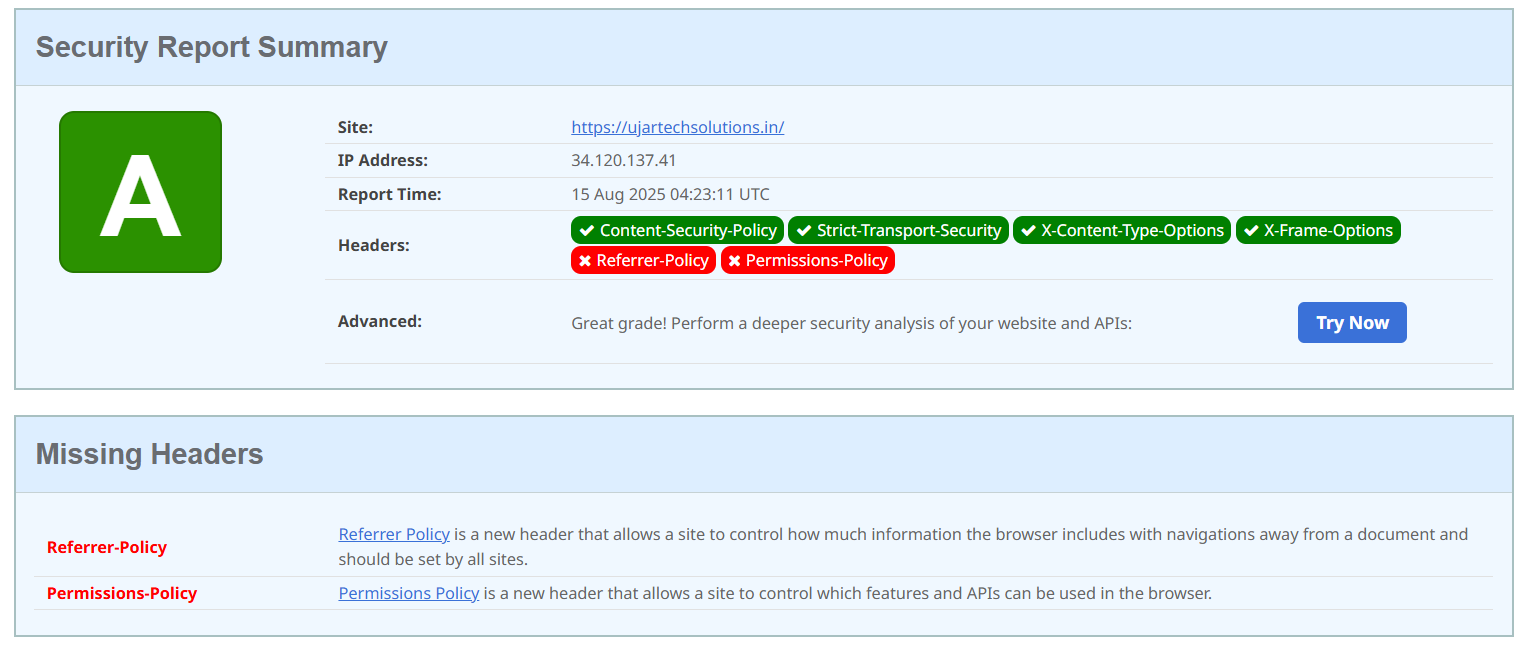


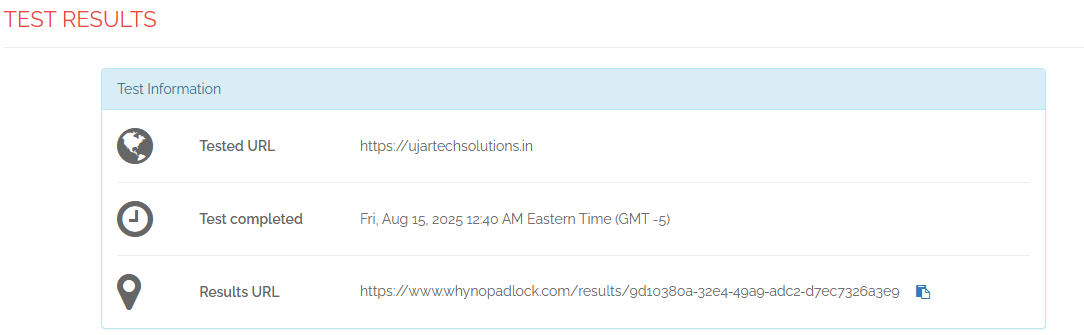


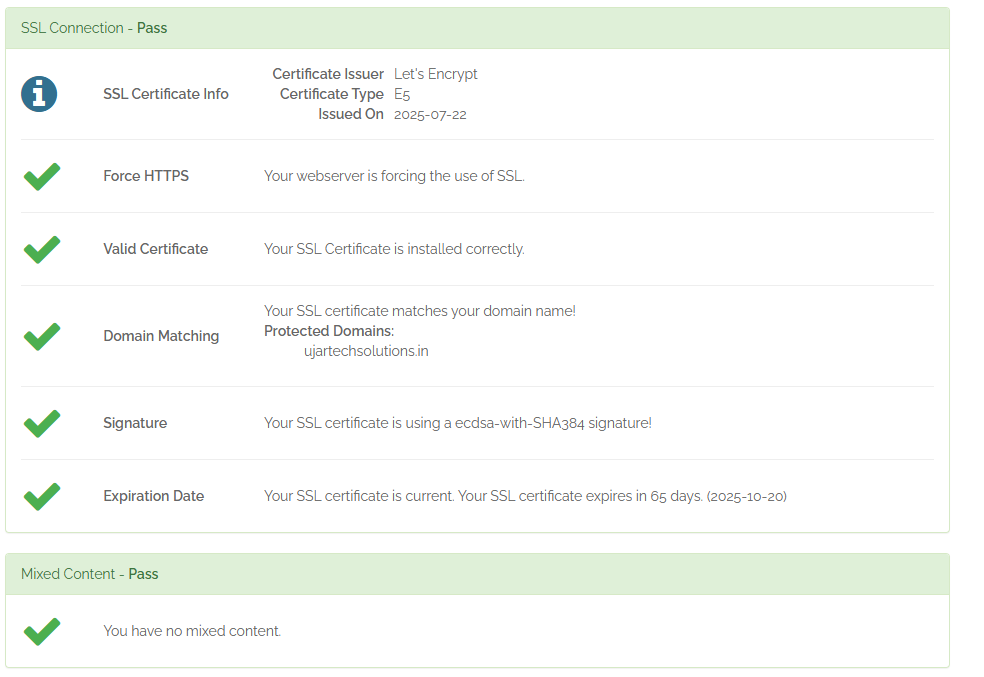


* In the above security report we can see that it’s a Grade F website which has missing headers like
  + **Content-Security-Policy (CSP):** It limits what content a browser can load for a website. It helps prevent Cross-Site Scripting (XSS) and data injection attacks by only allowing resources from trusted sources.
  + **X-Frame-Options:** This header helps prevent clickjacking attacks by controlling whether a web page can be displayed inside an <iframe>. If set to DENY, it blocks all framing;
  + **X-Content-Type-Options** header prevents browsers from MIME-sniffing a file’s type and forces them to use the declared Content-Type. Setting it to nosniff helps mitigate attacks like drive-by downloads or script execution of non-JavaScript files.
* In the above SSL test shows issues for this site: while the certificate is valid, uses a secure SHA256 signature, and has no mixed content, there are critical problems. HTTPS is not enforced, and the certificate’s domain names do not match the site’s domain, which can cause security warnings for visitors. The certificate expires in 81 days.

Ujartechsolutions.in







* In the above security report we can see that Ujartechsolutions.in is the Grade A website all the headers are there except “Referrer-Policy” which is the new header this helps to protect user privacy and reduces information exposure and “Permissions-Policy” controls which browser features (like camera, microphone) a site or its iframes can use. It helps reduce the attack surface by disabling unused or risky features.
* The SSL test shows that ujartechsolutions.in passed all tests. HTTPS is enforced, the certificate is valid and matches the domain, uses a secure ECDSA-with-SHA384 signature, has no mixed content, and will expire in 65 days

**Conclusion**  
the above research shows that grade A sites like YouTube and Ujartechsolutions.in have strong security implementations but still lack modern headers . In contrast, OWASP Juice Shop and Itsecgames.com have critical missing headers and HTTPS enforcement gaps, making them more vulnerable to common web-based attacks. Adopting complete security header configurations and enforcing HTTPS across all sites is essential for robust web security.