FUTURE INTERNS

CYBER SECURITY - TASK 1

NAME: Akshaya Raj

CIN ID: FIT/JAN26/CS5590

- **Website Name:** Wikipedia
- **URL:** https://www.wikipedia.org
- **Assessment Type:** Passive Security Review (Read-Only)
- **Date:** 15th January 2026

SCOPE & ETHICS STATEMENT:

IN SCOPE

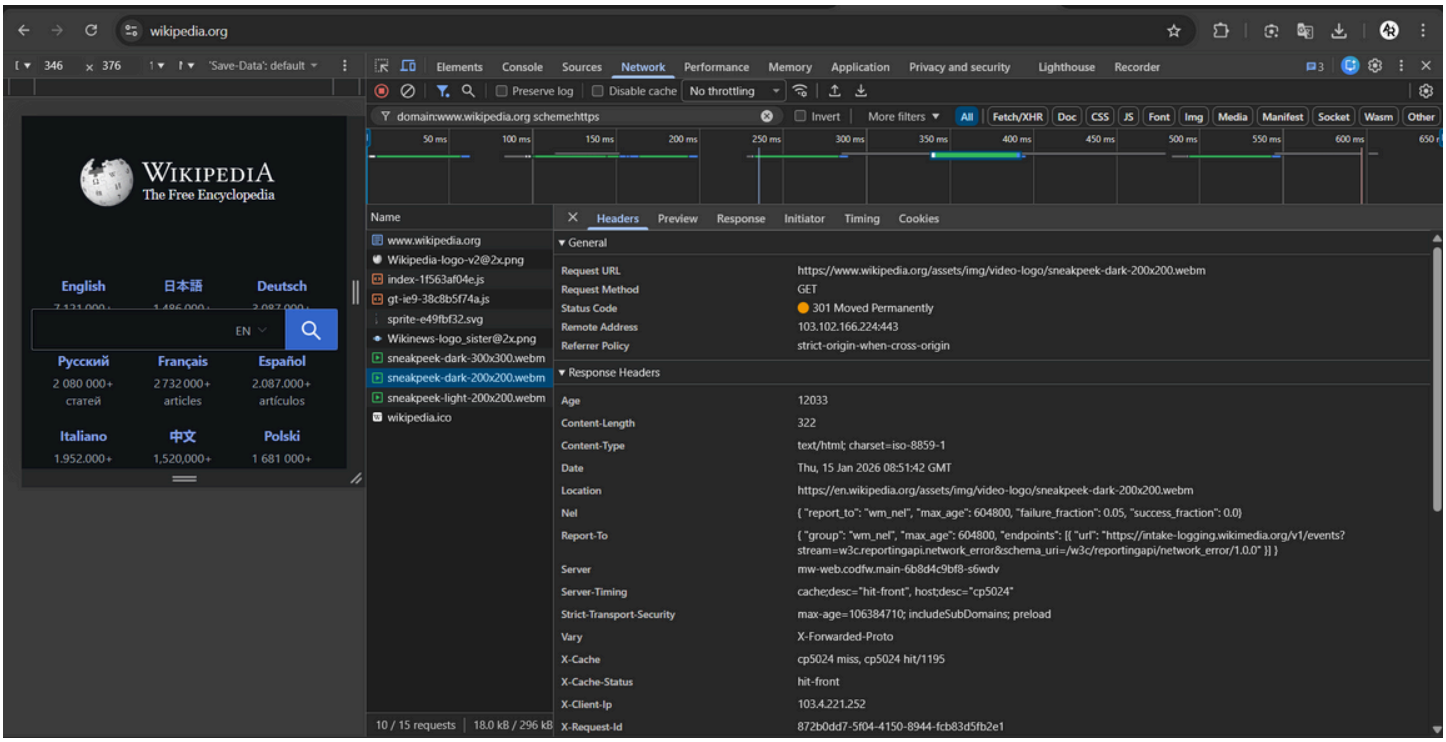
- Public-facing pages only
- Passive header and configuration analysis
- Browser-based inspection

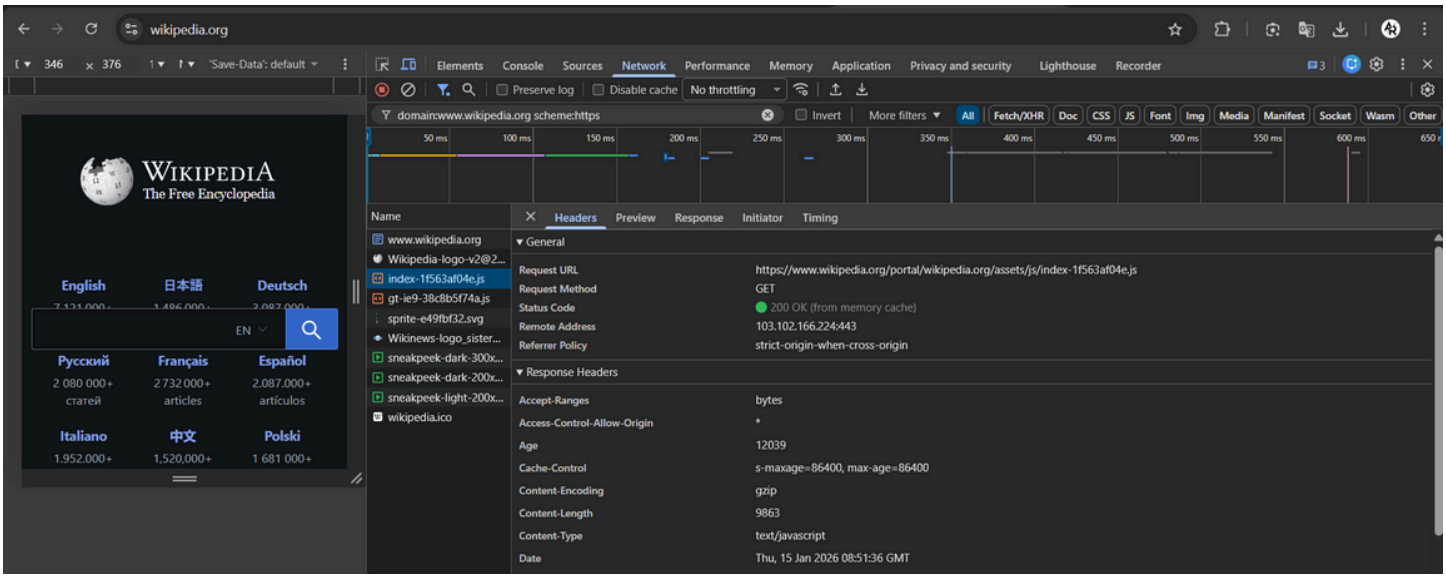
OUT OF SCOPE

- Login areas
- Exploitation attempts
- Brute force, DoS, or bypass techniques

TOOLS USED:

TOOL	PURPOSE
Browser Developer Tools	Inspect headers, cookies, HTTPS
OWASP ZAP (Passive Mode)	Identify misconfigurations
Online Header Inspection	Validate HTTP response headers
Manual Observation	Detect visible components





VULNERABILITY FINDINGS

Finding #1: Inconsistent Security Headers

- **Risk Level:** Medium
- **Tool Used:** Browser DevTools, OWASP ZAP (Passive)

What is the issue?

Some standard HTTP security headers, such as X-Frame-Options and X-Content-Type-Options, are not consistently visible across all public pages.

Why does it matter?

Security headers instruct browsers to block unsafe behaviours. Missing headers can increase exposure to:

- Clickjacking
- MIME-type sniffing attacks

Business Impact

Users could be tricked into interacting with embedded or manipulated content, affecting trust and brand reputation.

Recommended Remediation

- Enforce consistent security headers at the CDN or server level
- Use a standardised security header policy across all pages

Finding #2: Cookies Not Uniformly Scoped

- **Risk Level:** Low
- **Tool Used:** Browser DevTools (Application → Cookies)

What is the issue?

While most cookies use secure attributes, not all cookies consistently apply SameSite restrictions.

Why does it matter?

Improper cookie scoping may increase exposure to cross-site request forgery (CSRF) risks.

Business Impact

Low likelihood impact, but could affect authenticated users in edge cases.

Recommended Remediation

- Apply Secure, HttpOnly, and SameSite=Strict where applicable
- Review cookies during feature changes

Finding #3: No Public Security Policy Link on Landing Page

- **Risk Level:** Low
- **Tool Used:** Manual Review

What is the issue?

A clear security disclosure or vulnerability reporting link is not prominently visible on the landing page.

Why does it matter?

Researchers may not know how to responsibly report issues.

Business Impact

Delays in responsible disclosure could increase the exposure window.

Recommended Remediation

- Add a visible “Security” or “Report a Vulnerability” link
- Encourage responsible disclosure practices

RISK CLASSIFICATION SUMMARY

FINDINGS	RISK
Inconsistent Security Headers	Medium
Cookie Scope Consistency	Low
Security Policy Visibility	Low

EXECUTIVE SUMMARY (NON-TECHNICAL LANGUAGE)

- The website demonstrates a strong overall security foundation, including HTTPS enforcement and minimal server information exposure.
- One medium-risk improvement was identified related to browser security controls and client-side dependency management.
- No critical vulnerabilities were discovered during this passive assessment.