Vulnerability Assessment Report for a Live Website

Task: Cyber Security – Task 1
Website Tested: www.verisign.com
Website found through: Bugcrowd (Bug Bounty hunting platform)
Assessment Type: Web Application Security Testing

- ## Introduction

  Web application security is a critical component of cybersecurity, as live web applications handle sensitive data and support essential online services. Vulnerabilities in such systems can lead to unauthorized access, data exposure, and operational risks.

  This assessment focuses on basic security testing of a live web application selected from a Bugcrowd-managed vulnerability disclosure program. The target application, **www.verisign.com**, was explicitly listed as in scope, and all testing was conducted in accordance with the program's authorization, scope limitations, and responsible disclosure guidelines.

- ## Objective

  To perform authorized basic assessment on a live web application in order to identify common vulnerabilities and assess their potential impact using automated and manual techniques.

- ## Tools Used
  - **OWASP ZAP** – Automated web application security scanner
  - **Nmap** – Network scanning tool used to identify exposed services and open ports
  - **Web Browser** – Used for manual testing

- # Vulnerability Assessment Performed
  - ## Nmap Scanning

    A limited network reconnaissance scan was conducted using Nmap to identify exposed network services within the authorized scope.

    The scan identified the following open ports on the target system:
    - **80/tcp** – HTTP
    - **443/tcp** – HTTPS

    Observation:
    The presence of only standard web service ports indicates a minimal external attack surface, with no additional unnecessary services exposed.

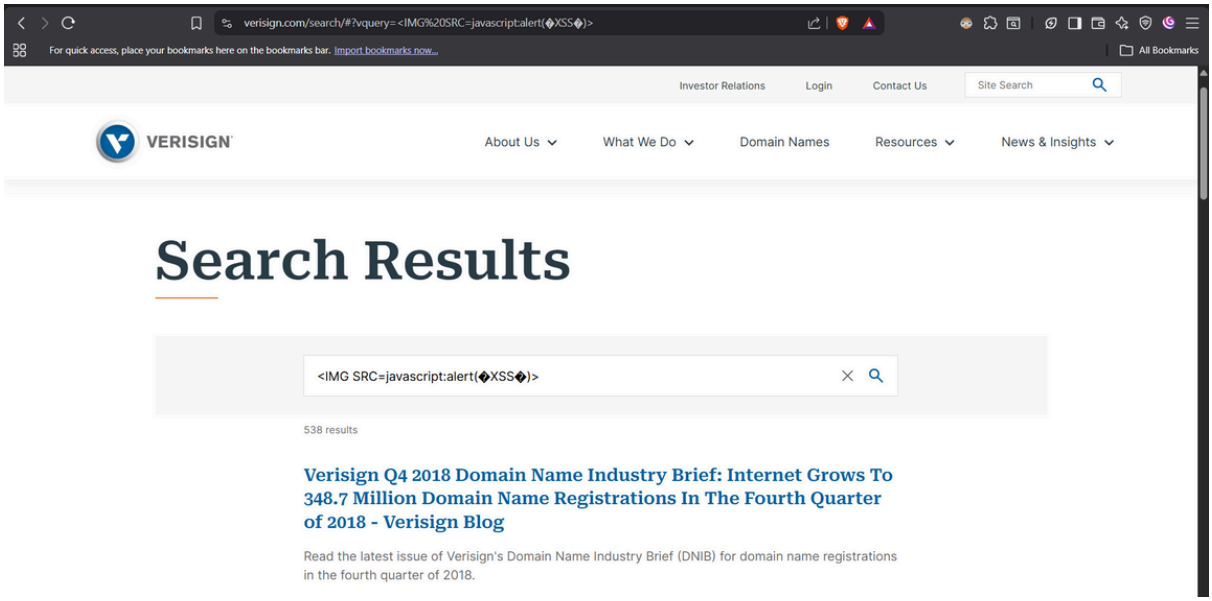
```
┌──(kali㉿kali)-[~]
└─$ nmap www.verisign.com -p- -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-18 15:32
Nmap scan report for www.verisign.com (72.13.63.40)
Not shown: 64345 filtered tcp ports (no-response), 1188 filtered tcp ports (net-unreach)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

  - ## XSS Testing

    Description:
    Cross-Site Scripting (XSS) testing was performed by injecting common script-based payloads into input fields to assess the application's handling of untrusted input and output encoding.

    Observation:
    The application successfully blocked or neutralized the injected scripts, and no script execution or unexpected client-side behavior was observed.

    Impact:
    If proper input sanitization and output encoding were not enforced, an attacker could exploit XSS vulnerabilities to execute malicious scripts in a user's browser, potentially leading to session hijacking, data theft, or unauthorized actions performed on behalf of the user.

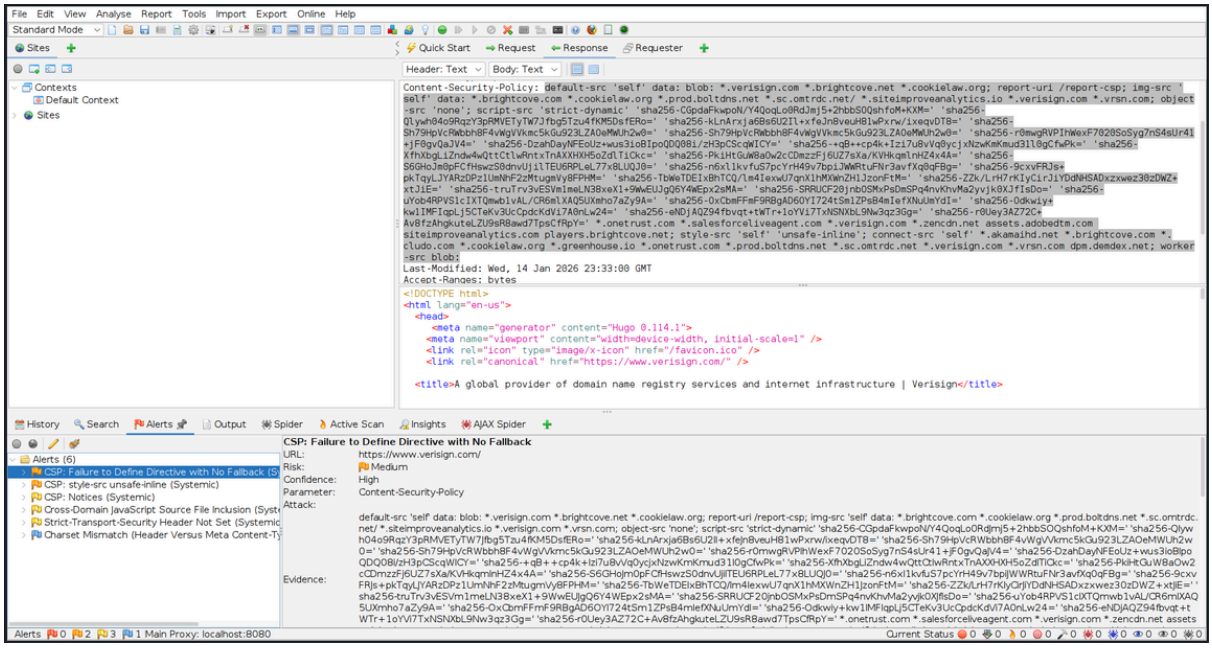


- **Automated Security Scan (OWASP ZAP)**
  An automated security scan was conducted using **OWASP ZAP** against the website

  Findings:
  The scan identified the following issues:

  - CSP: Failure to Define Directive with No Fallback [medium]
  - CSP: style-src unsafe-inline [medium]
  - CSP: Notices [low]
  - Cross-Domain JavaScript Source File Inclusion [low]
  - Strict-Transport-Security Header Not Set [low]
  - Charset Mismatch (Header Versus Meta Content-Type Charset) [informational]

  These findings primarily indicate misconfigured security headers rather than direct exploitation vulnerabilities.



- # Screenshots and Evidences

  Screenshots and tool outputs were taken during each phase of the assessment, including:

  - XSS testing
  - Nmap scanning
  - OWASP ZAP alert details

  These screenshots and outputs serve as evidence of the assessment activities and findings.

- # Disclaimer

  This assessment was conducted strictly for educational purposes on a live web application selected from a Bugcrowd-managed vulnerability disclosure program. The target was explicitly listed as in scope, and all testing was performed within authorized boundaries, following responsible and ethical assessment practices. No unauthorized or destructive testing was carried out.