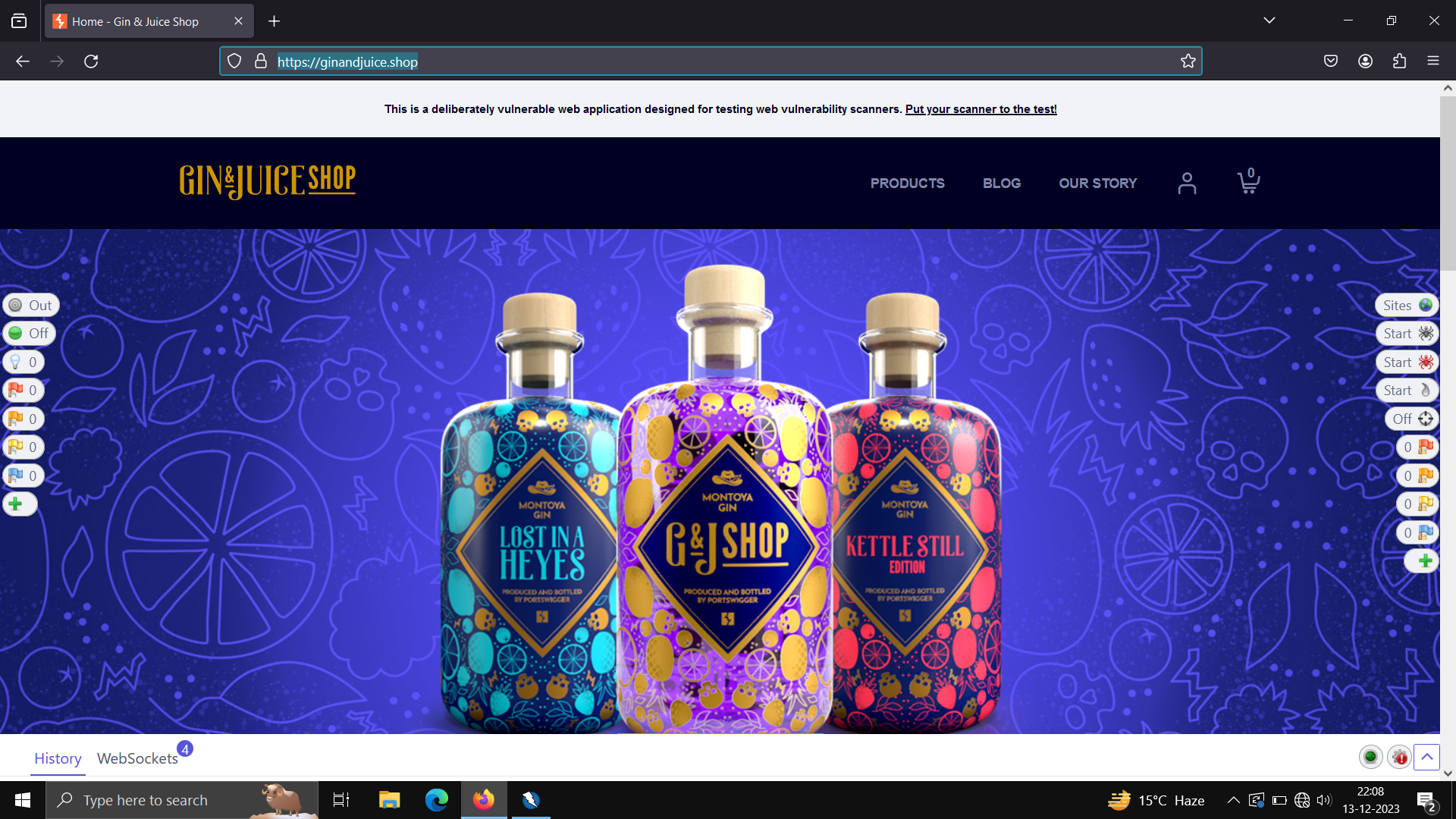
**USING AJAX SPIDER, TRADITIONAL SPIDER AND ACTIVE SCAN**

**MANUALLY CRAWLING COMPONENETS OF WEBSITE and then -ajax scan , spider scan and last active scan**

**TARGET WEBSITE -** [**https://ginandjuice.shop**](https://ginandjuice.shop)



**Vulnerabilities - >**

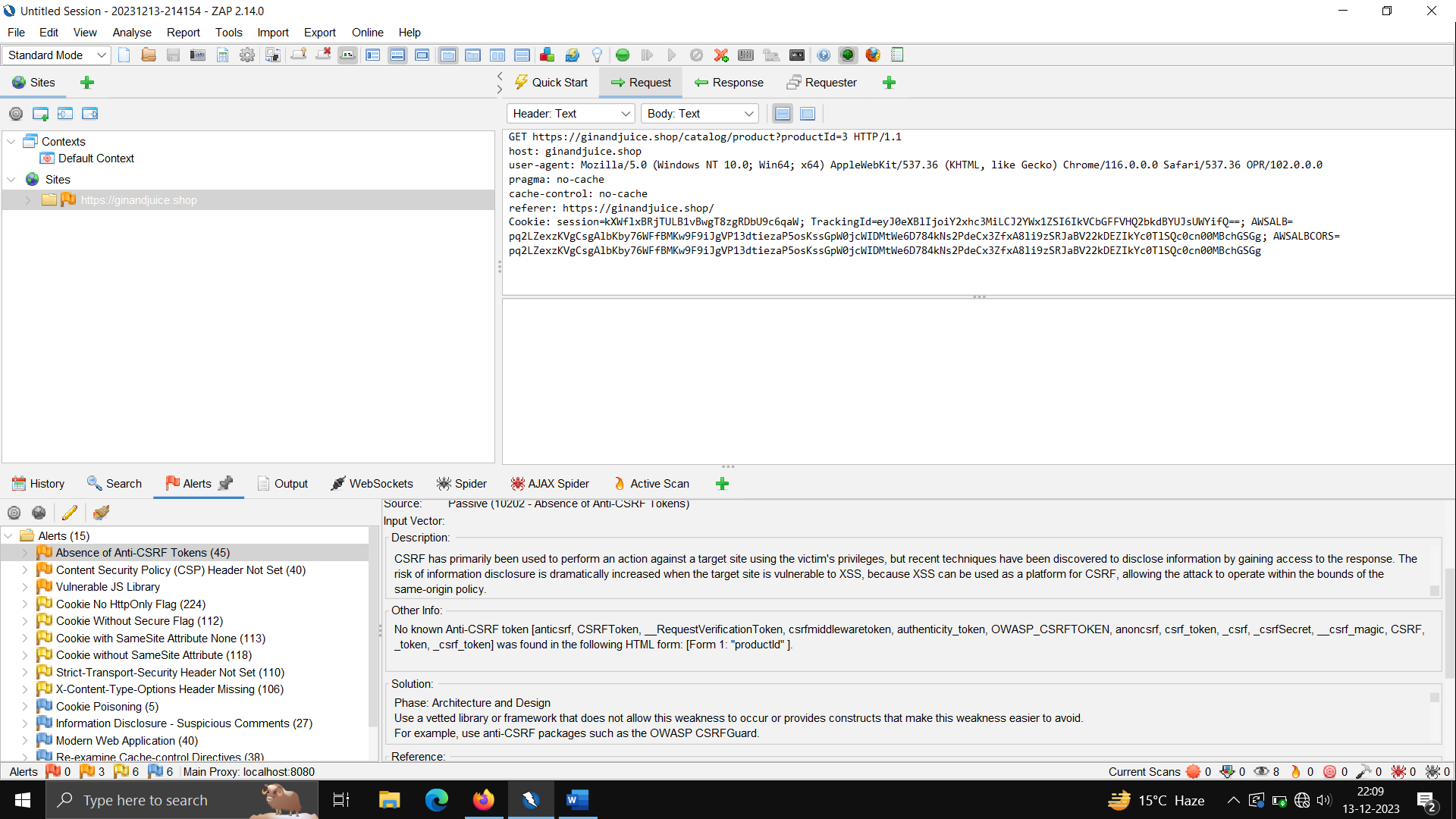
**Severity: MEDIUM**

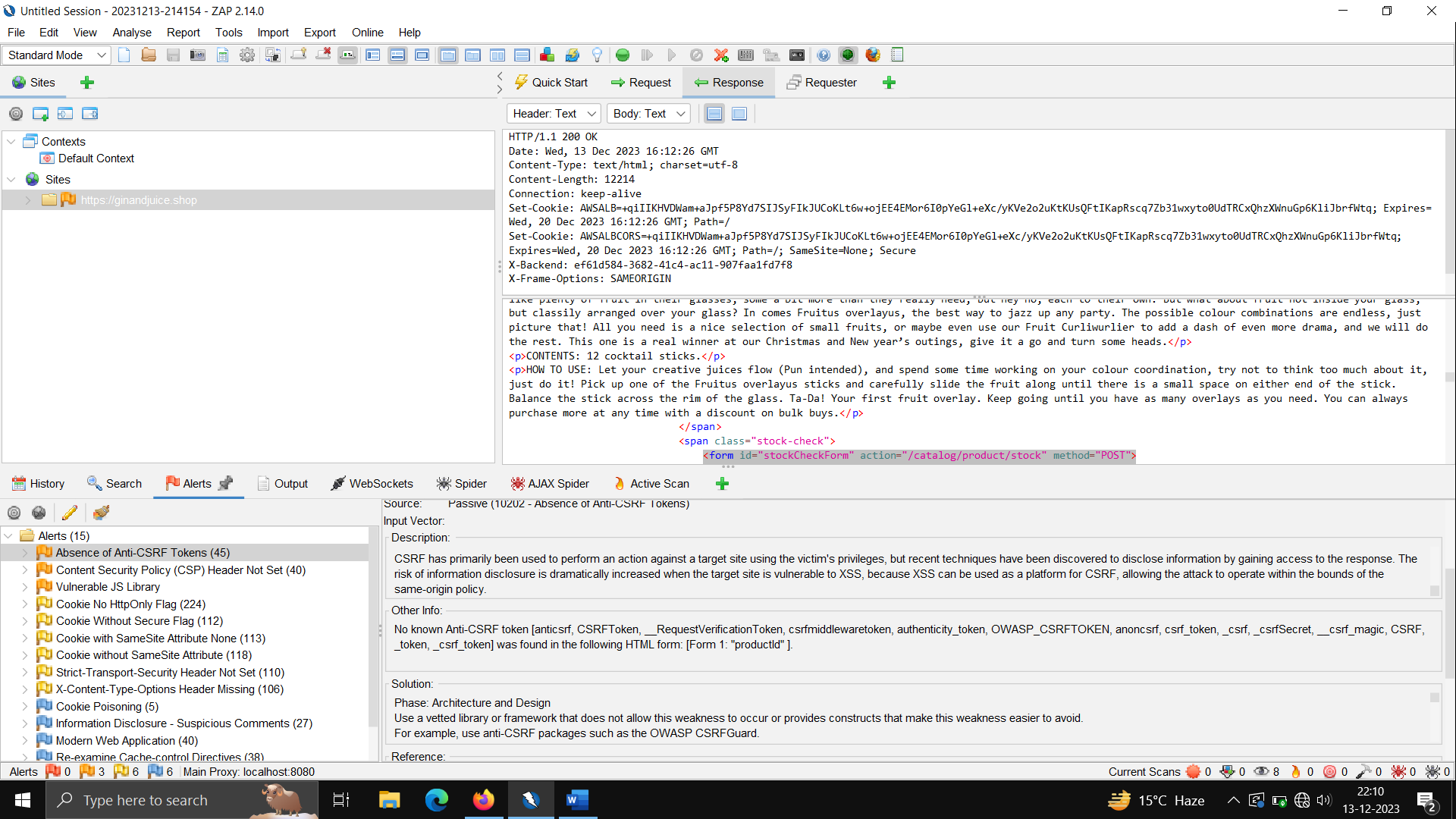
**Absence of Anti-CSRF Tokens-**

**No Anti-CSRF tokens were found in a HTML submission form.**

**A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim.**

**Request/Response-**





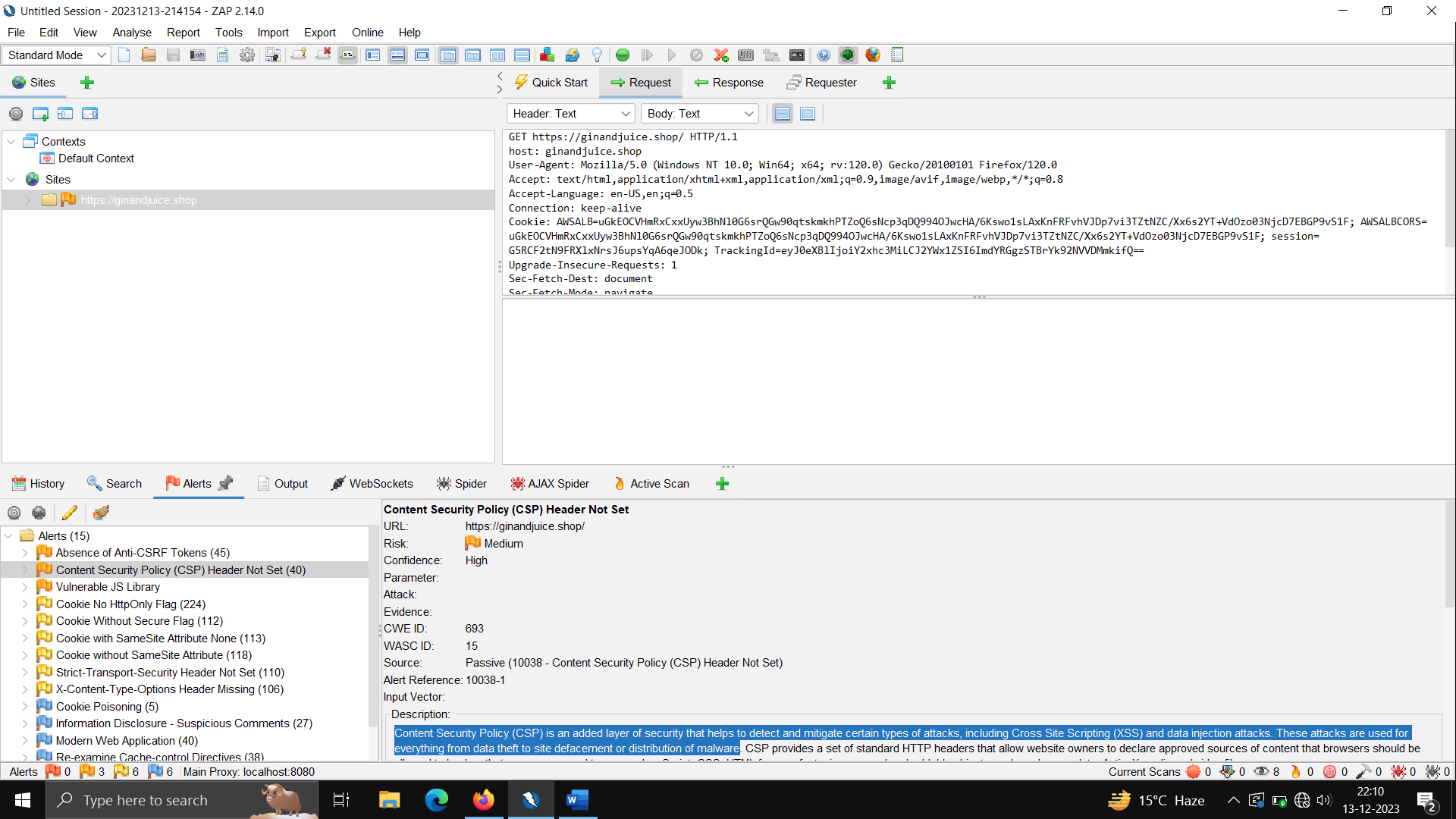
**Use CRSF token encryption at client and decryption at server side for token verification – that is unique to every user.**

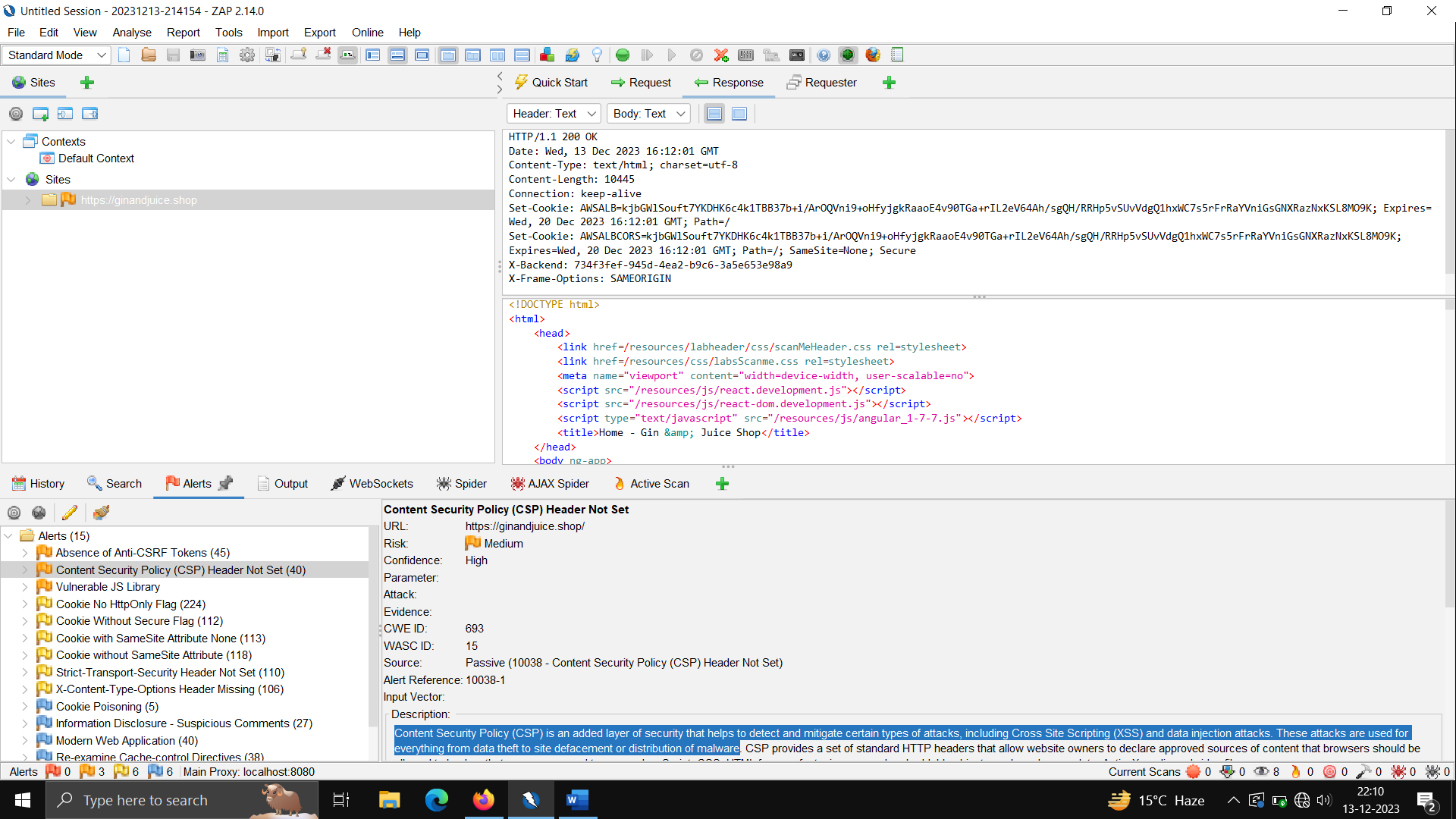
**Content Security Policy (CSP) Header Not Set**

**Severity: MEDIUM**

**Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware**

**Request/Response-**





**Set header content policy – in html ->**

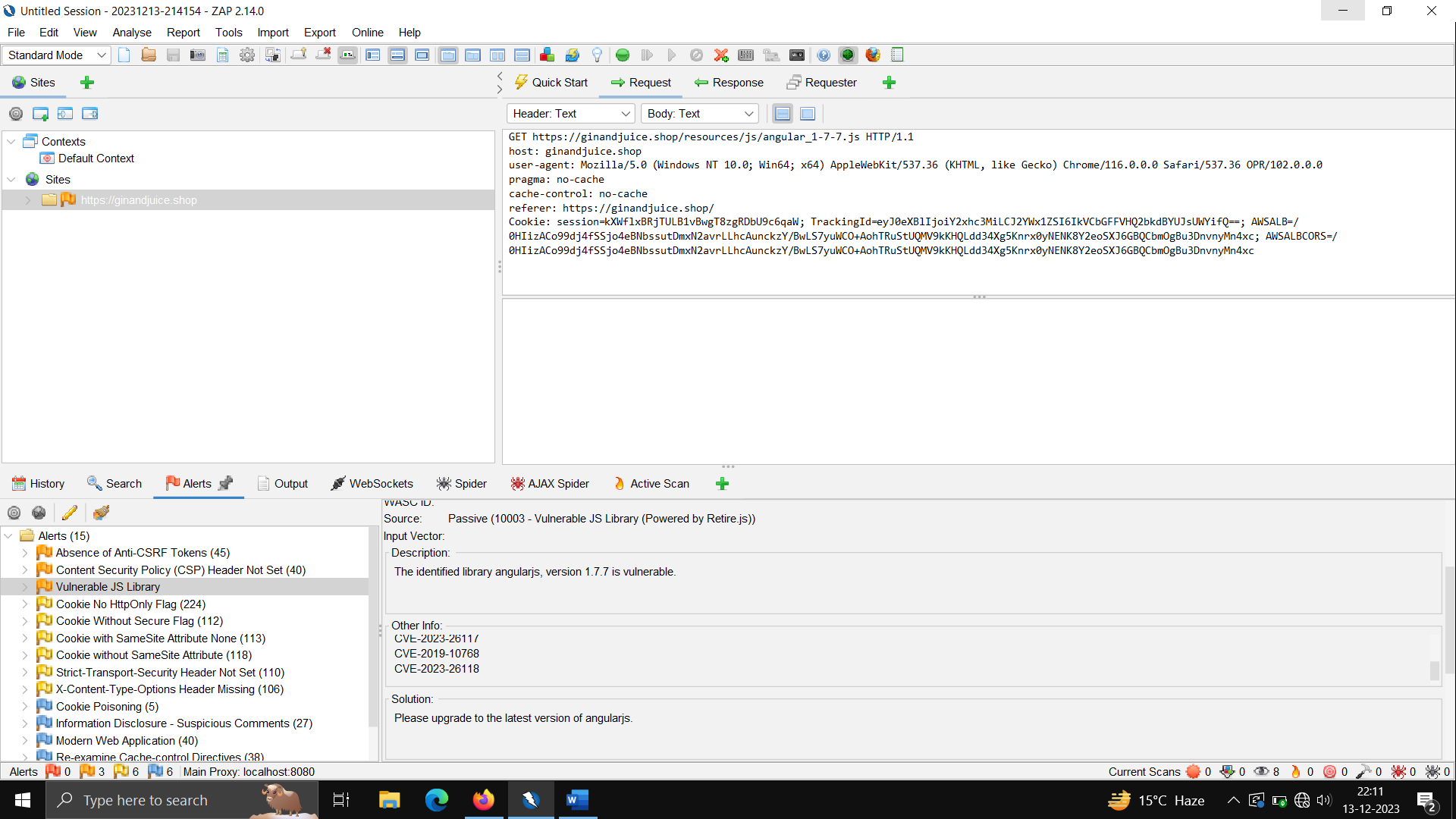
<meta content = "default-src 'none';" http-equiv = "Content-Security-Policy" />

**Vulnerable JS Library**

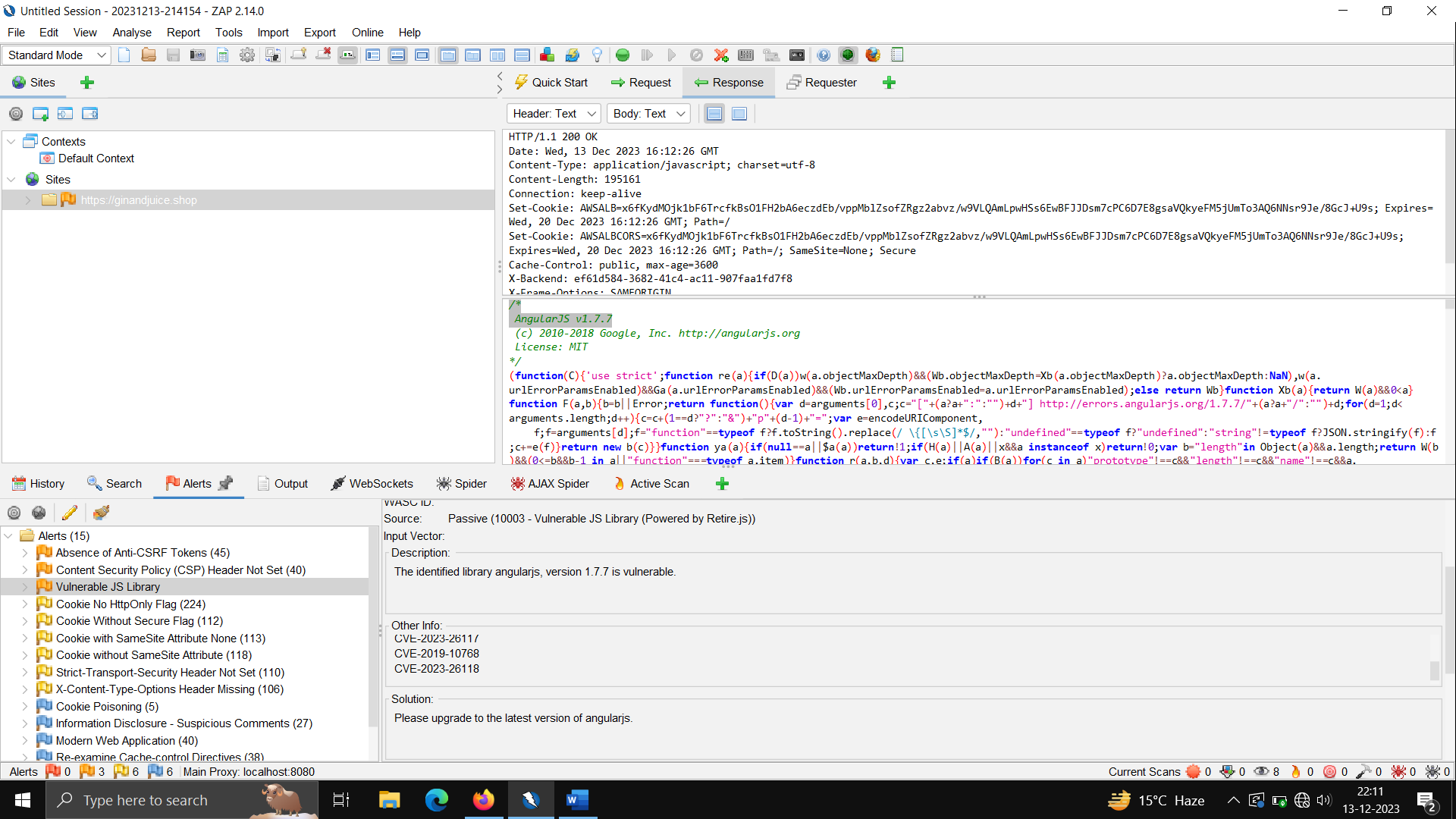
**Severity: MEDIUM**

**The identified library angularjs, version 1.7.7 is vulnerable.**

**Request/Response-**



**Remediation – Regular updates/Patching**

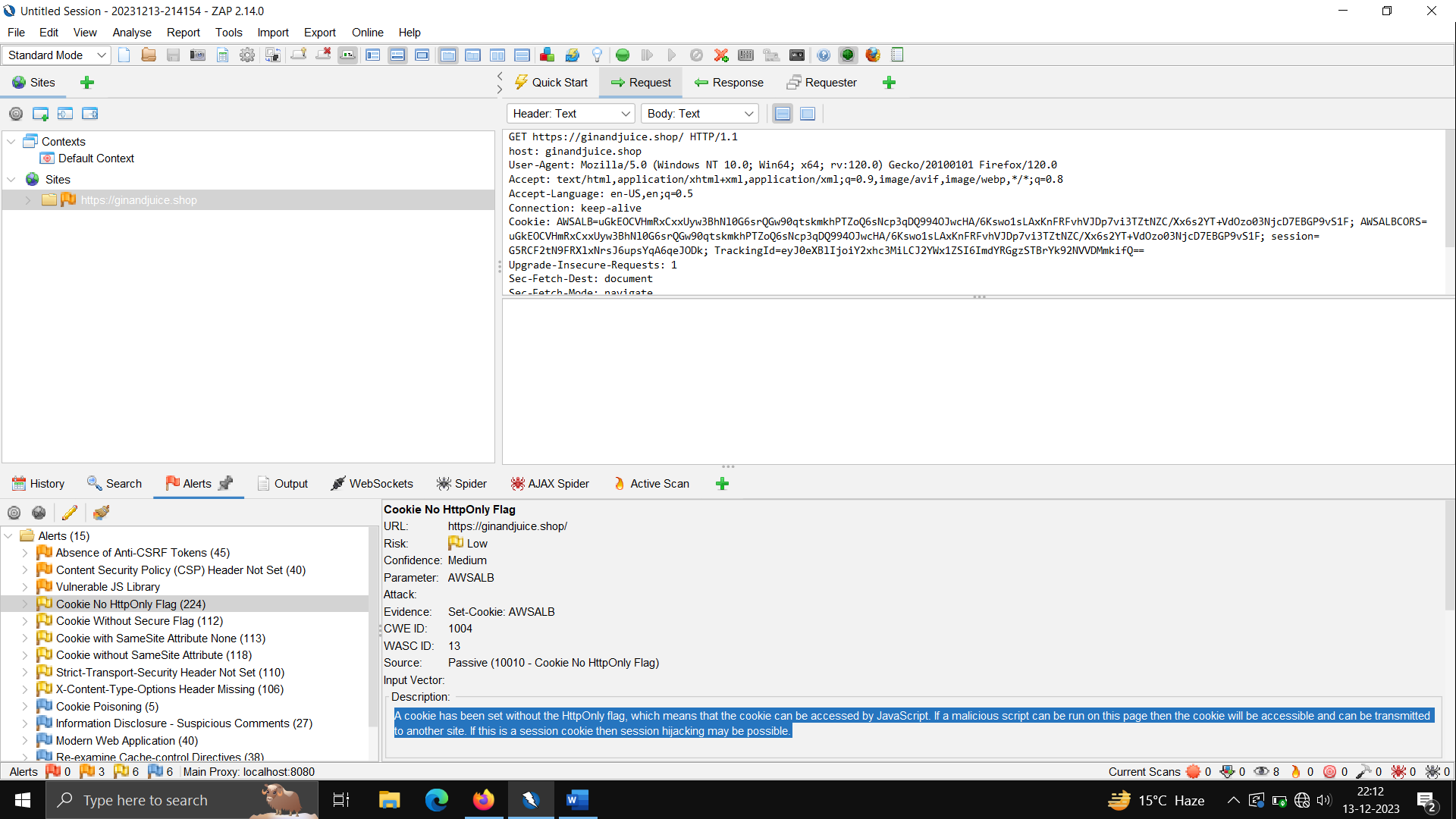


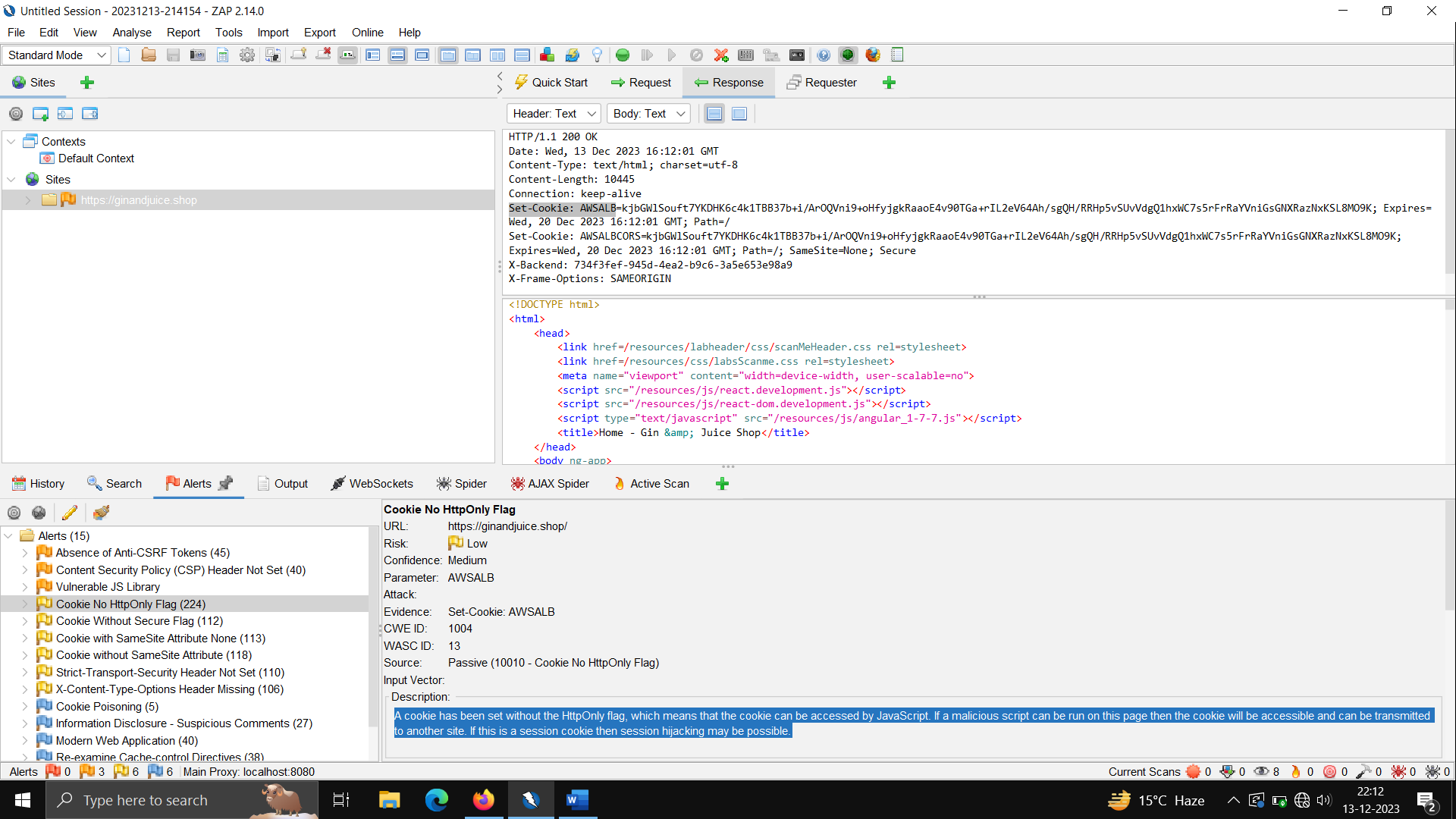
**Cookie No HTTP Only Flag**

**Severity: LOW**

**A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.**

**Request/Response-**





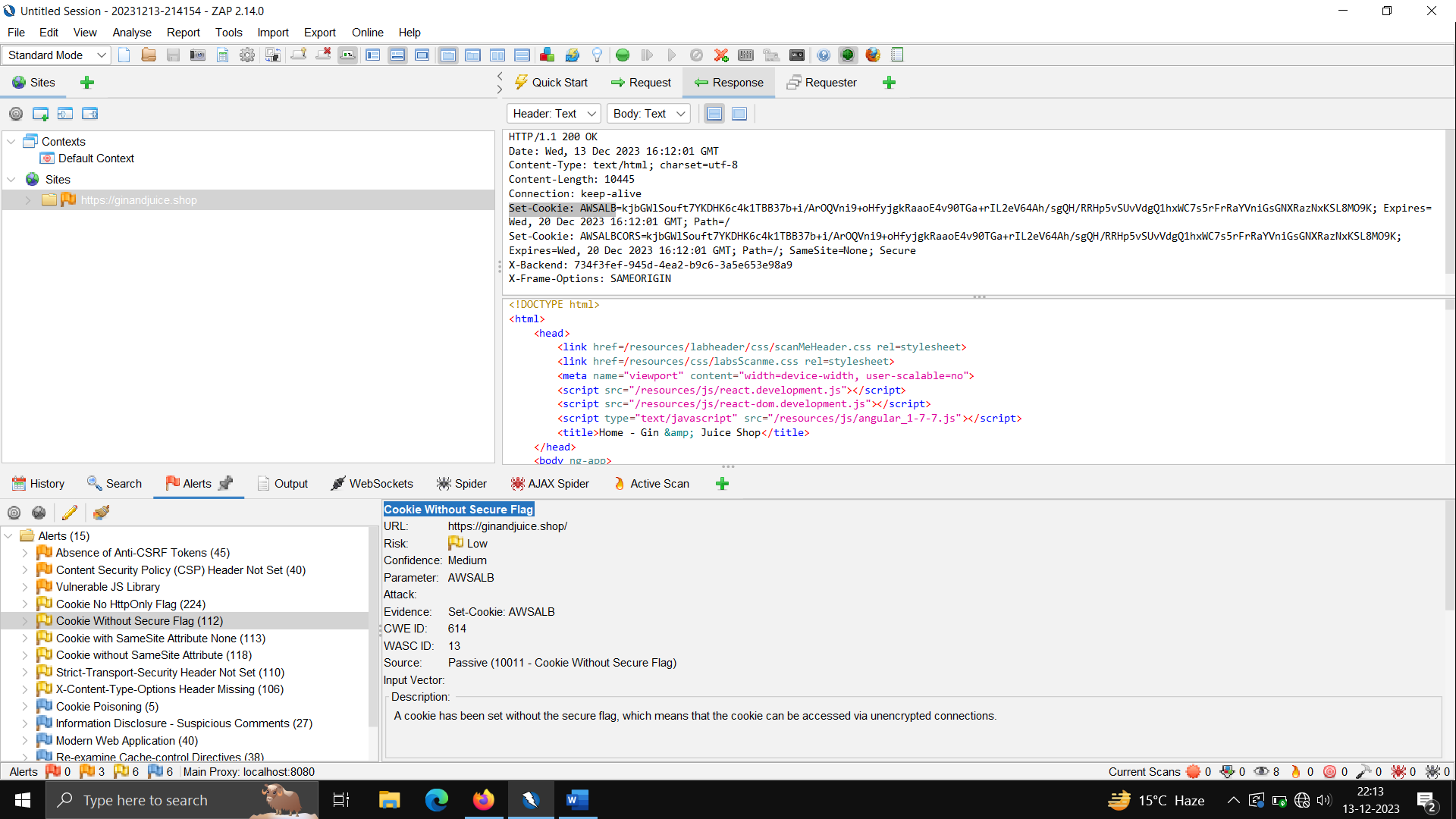
**Cookie Without Secure Flag**

**Severity: LOW**

**A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.**

**Request/Response-**





**X-Content-Type-Options Header Missing**

**The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.**

**Request/Response-**

