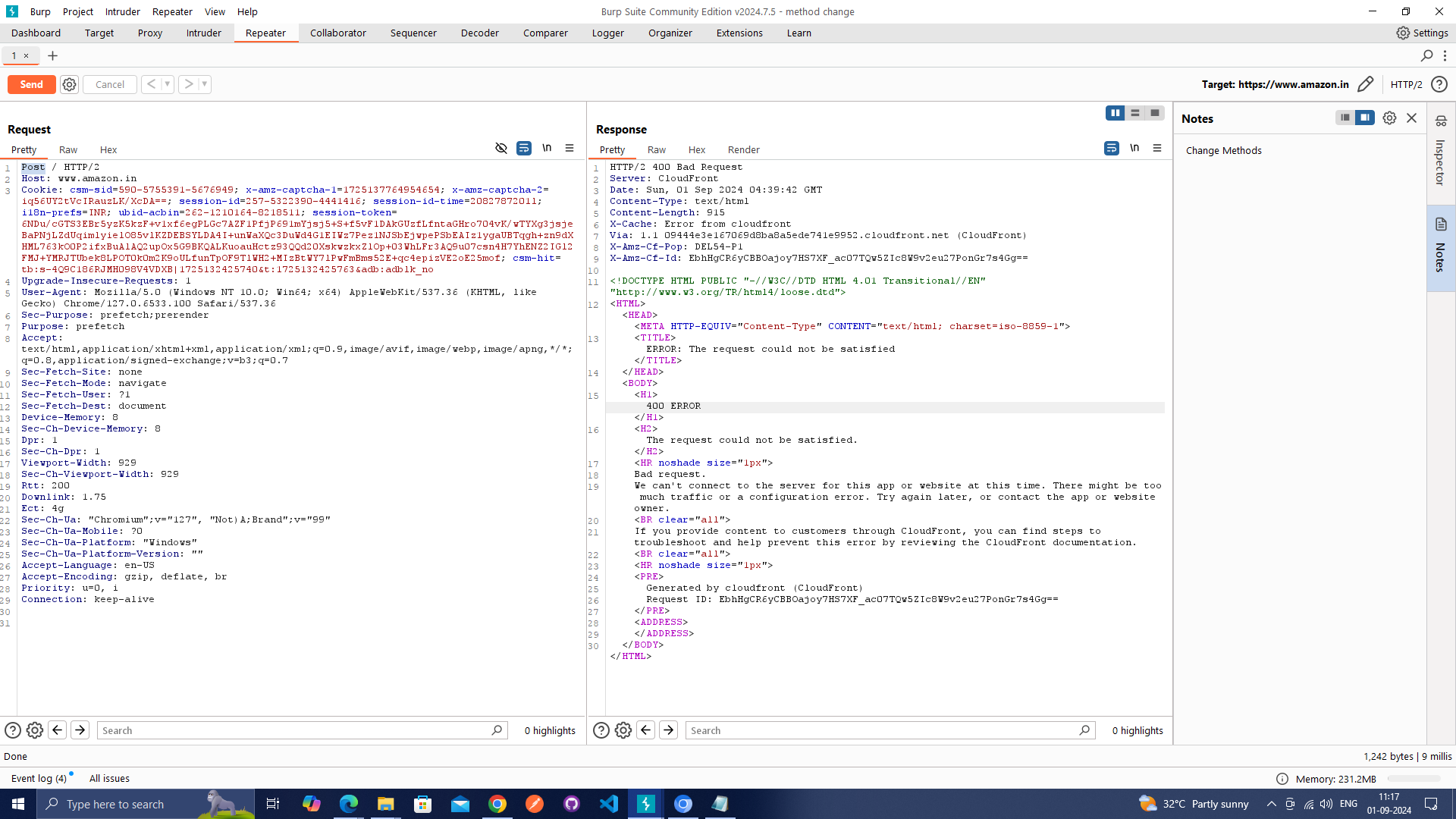
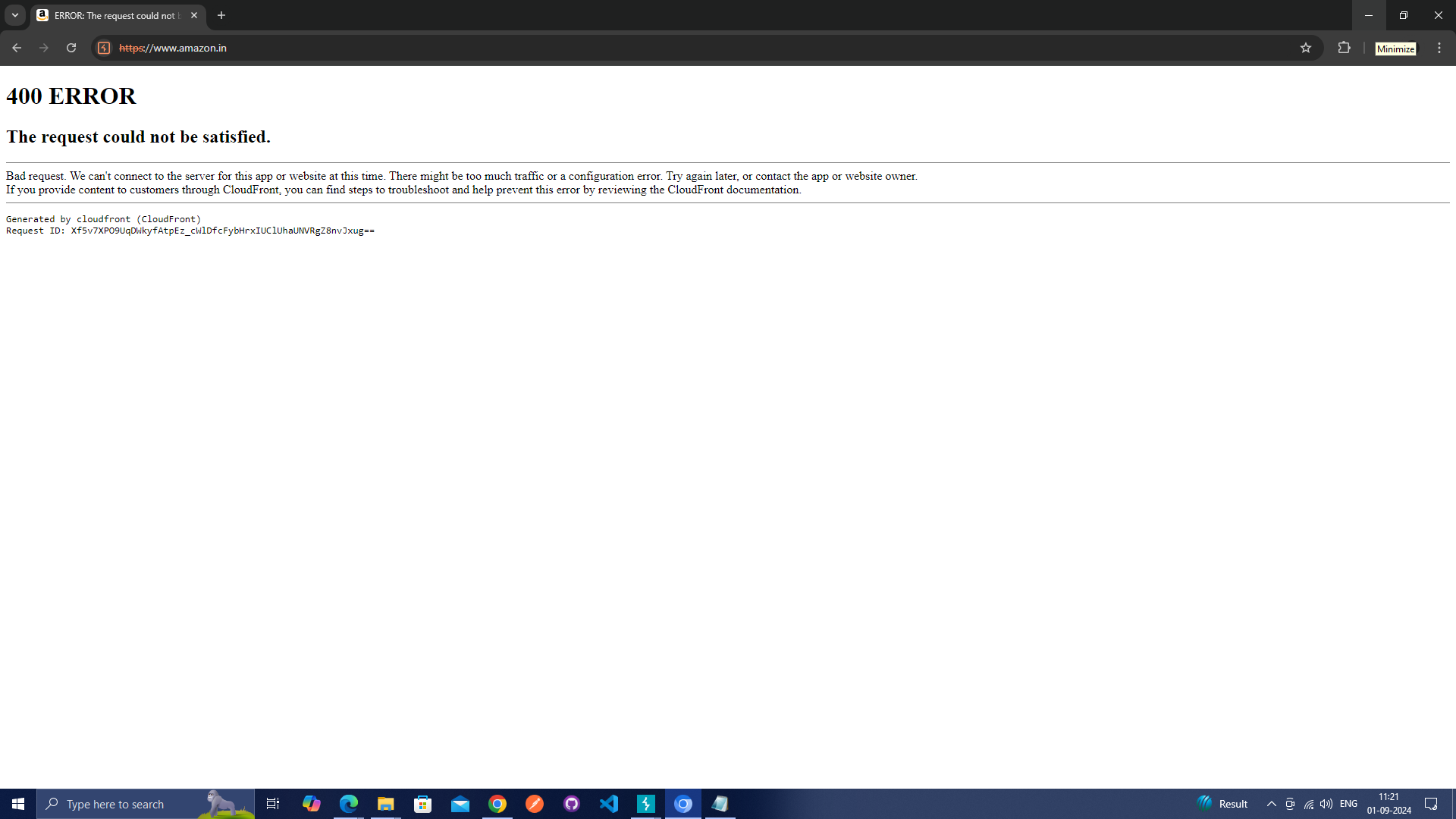
**1.CSRF (Cross-Site Request Forgery) Protection:**

**Changing a method from GET to POST is a crucial consideration in various vulnerability testing**



**Conclusion :** Showing bad request (As expected)

**Response:**

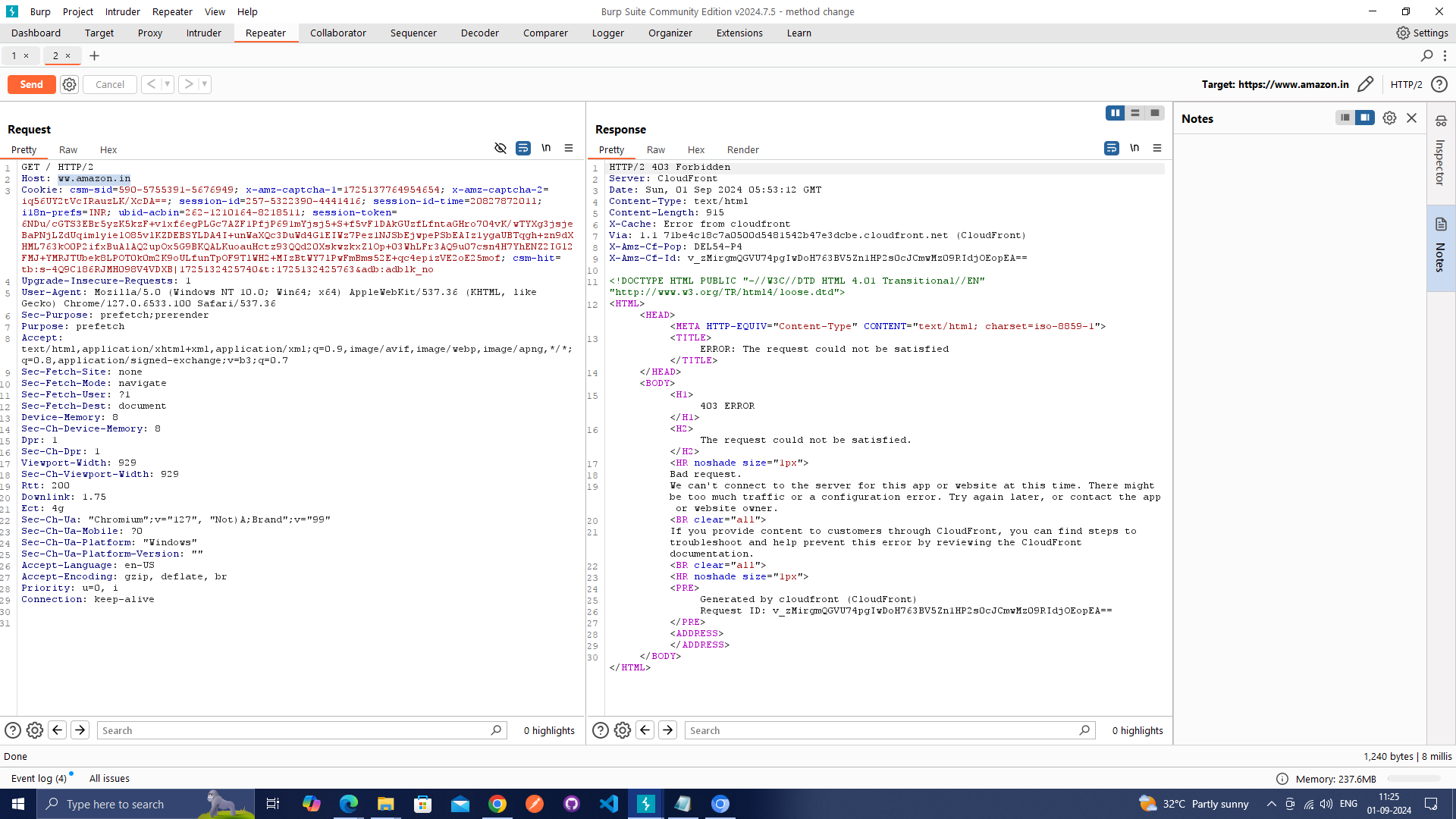


**2.Host Header Injection**

Request:

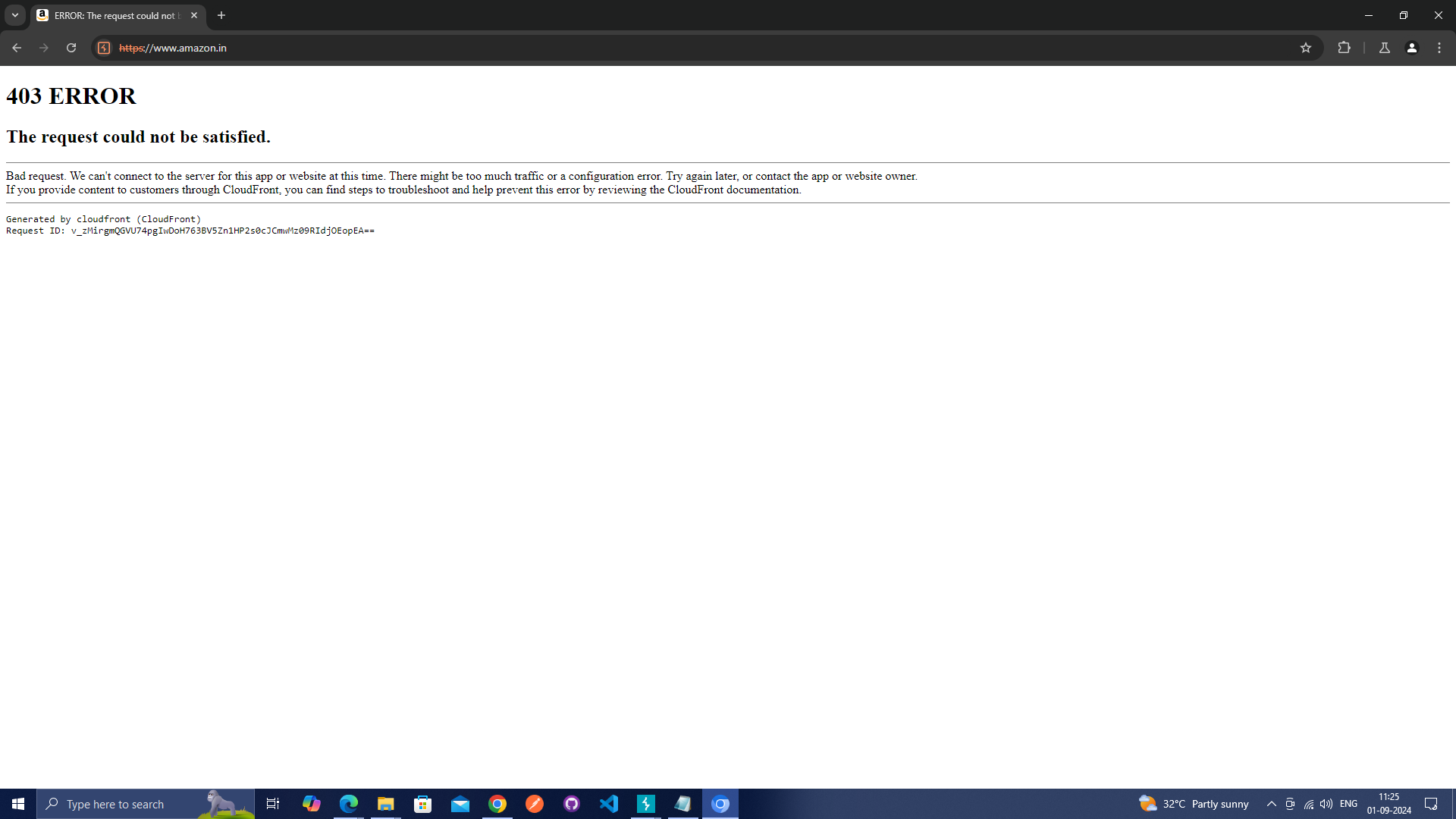
Host Header Injection occurs when an application improperly trusts or uses the Host header in HTTP requests. This can lead to a range of security issues if the application doesn’t properly validate or sanitize this header.

Changing Host from [www.amazon.in](http://www.amazon.in) to ww.amazon.in to check the critical vulnerability



**Conclusion :** Showing bad request (As expected)

**Response:**



**3. SQL Injection Price Manipulation Vulnerabilities**

Price manipulation occurs when a user can alter the price of a product or service through client-side or server-side modifications.

