# Task 1

## Perform a Vulnerability Assessment of a Sample Web Application

### Vulnerability Assessment Report : -

---

### Tool Used : OWASP ZAP

### 1. Introduction : -

- **Objective**: -
- The purpose of this assessment is to identify potential security vulnerabilities within the target web application - **OWASP Juice Shop.**
- The assessment was conducted using **OWASP ZAP**, and this report provides a summary of the **identified vulnerabilities, their associated risks, and recommendations to mitigate them.**

---

### 2. Methodology : -

- **Testing Phases :**
  1. **Spidering**: Mapping the structure of the application.
  2. **Active Scanning**: Identifying vulnerabilities based on the automated scans.

---

### 3. Vulnerabilities Identified : -

- Found **7 Alerts** out of which **: -**
- **3** of them were **Medium** Level of Risk
- **2** were **Low** level of Risk
- **2** were **Informational** Level alerts

| Alert No. | Vulnerability Name | Risk Level | Remediation |
|---|---|---|---|
| 1. | Content Security Policy (CSP) Header Not Set (9) | Medium | Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header. |
| 2. | Cross-Domain Misconfiguration (20) | Medium | Ensure that sensitive data is not available in an unauthenticated manner (using IP address whitelisting<br><br>Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, |
| 3. | Hidden File Found(4 ) | Medium | Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc. |
| 4. | Cross-Domain JavaScript Source File Inclusion(4) | Low | Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be |

| | | | |
|---|---|---|---|
| | | | controlled by end users of |
| 5. | Timestamp Disclosure - Unix | Low | Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns. |
| 6. | Information Disclosure - Suspicious Comments | Informational | Remove all comments that return information that may help an attacker and fix any underlying problems they refer to. |
| 7. | Modern Web Application | Informational | This is an informational alert and so no changes are required. |

---

## 4. Vulnerabilities Description : -

▢ **Content Security Policy (CSP) : -**

- 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.
- CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page.
- Covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

---

▢ **Cross-Domain Misconfiguration : -**

- Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**Evidence : -**

**Access-Control-Allow-Origin: ***

---

▢ **Hidden File Found : -**

- **A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.**

**Evidence : -**

**HTTP/1.1 200 OK**

---

▢ **Cross-Domain JavaScript Source File Inclusion : -**

- **The page includes one or more script files from a third-party domain.**

**Evidence : -**

**<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>**

---

▢ **Timestamp Disclosure - Unix : -**

- **A timestamp was disclosed by the application/web server. - Unix**

**Evidence : -**

**1734944650**

---

## 5. Conclusion : -

**In conclusion, the vulnerabilities identified during the assessment pose significant risks to the confidentiality, integrity, and availability of the web application. Immediate action should be taken to mitigate the high and medium severity vulnerabilities, Implementing the recommended solutions will greatly enhance the security posture of the application.**

---

## 6. Screenshots : -

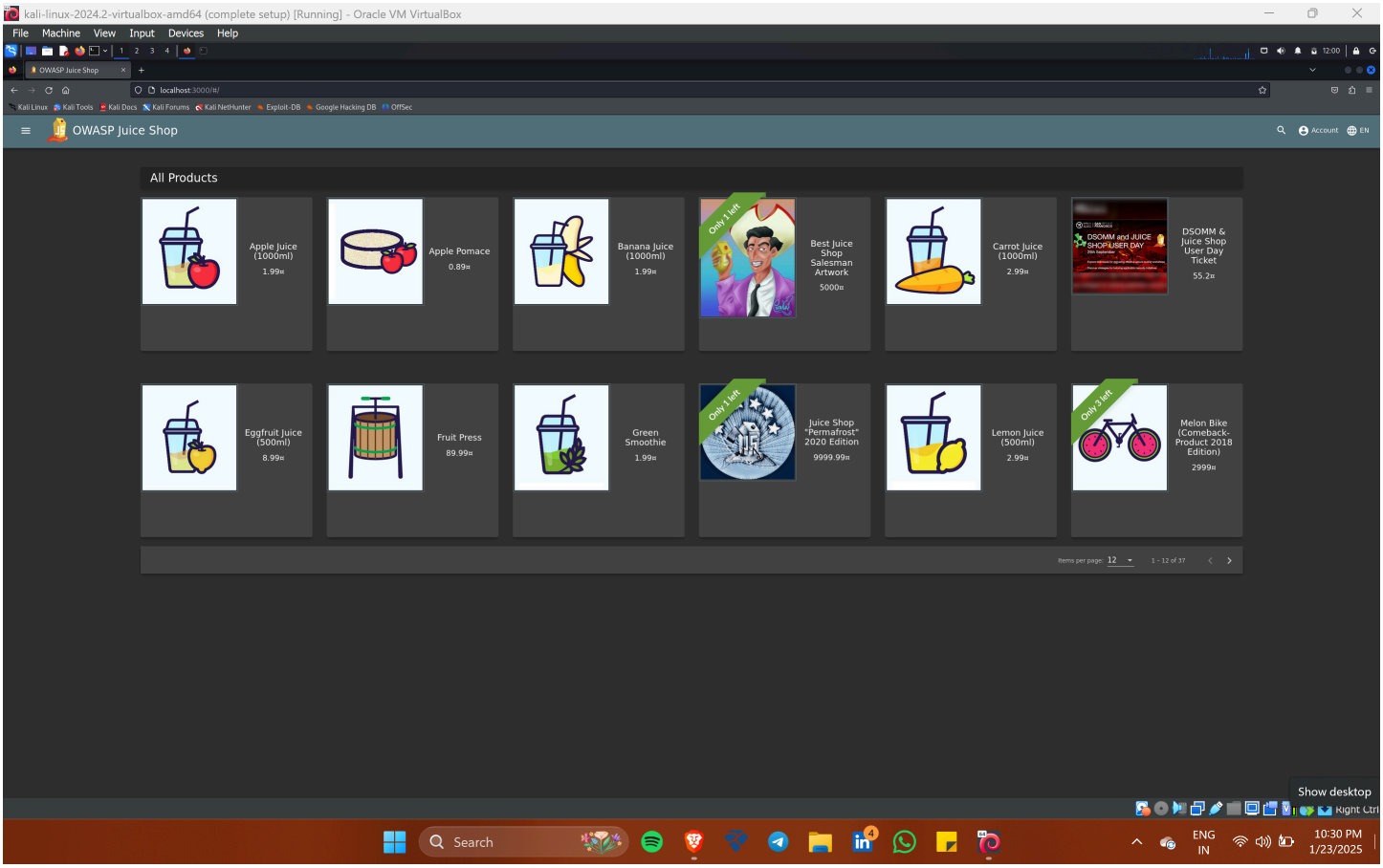


**Figure - 1 : OWASP JUICE SHOP**

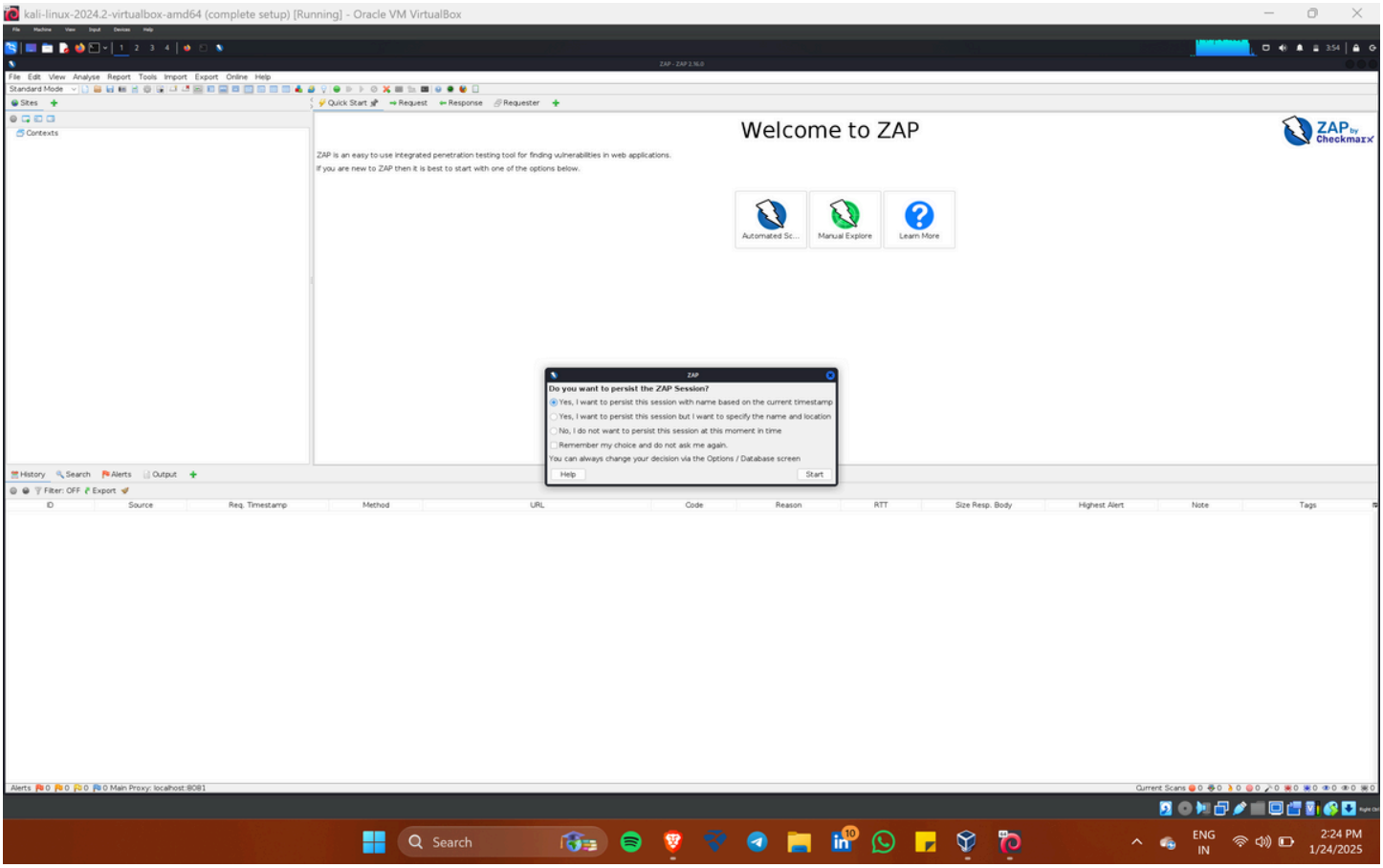


**Figure - 2 : OWASP ZAP**

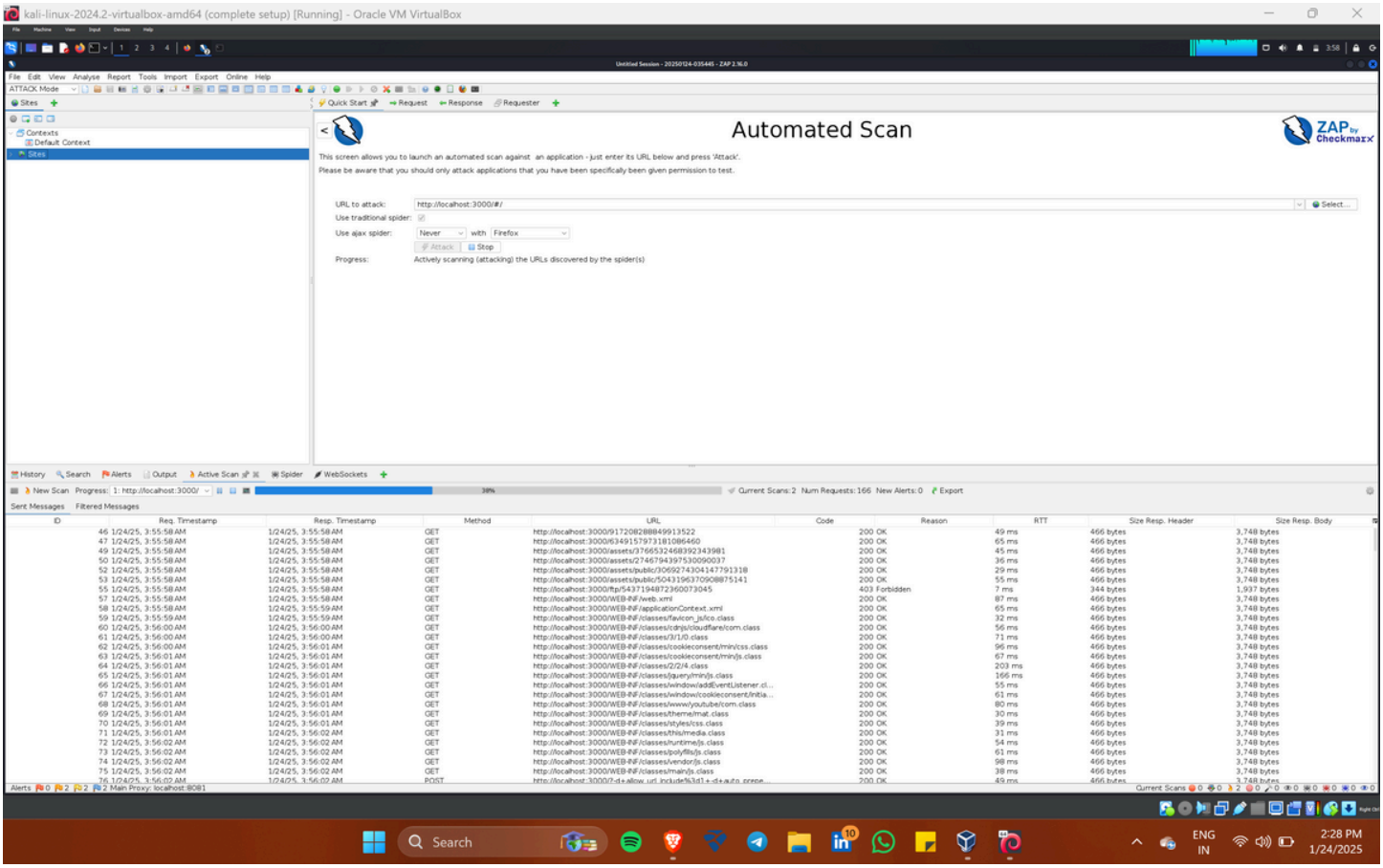


**Figure - 3 : Active and Spider Scan**

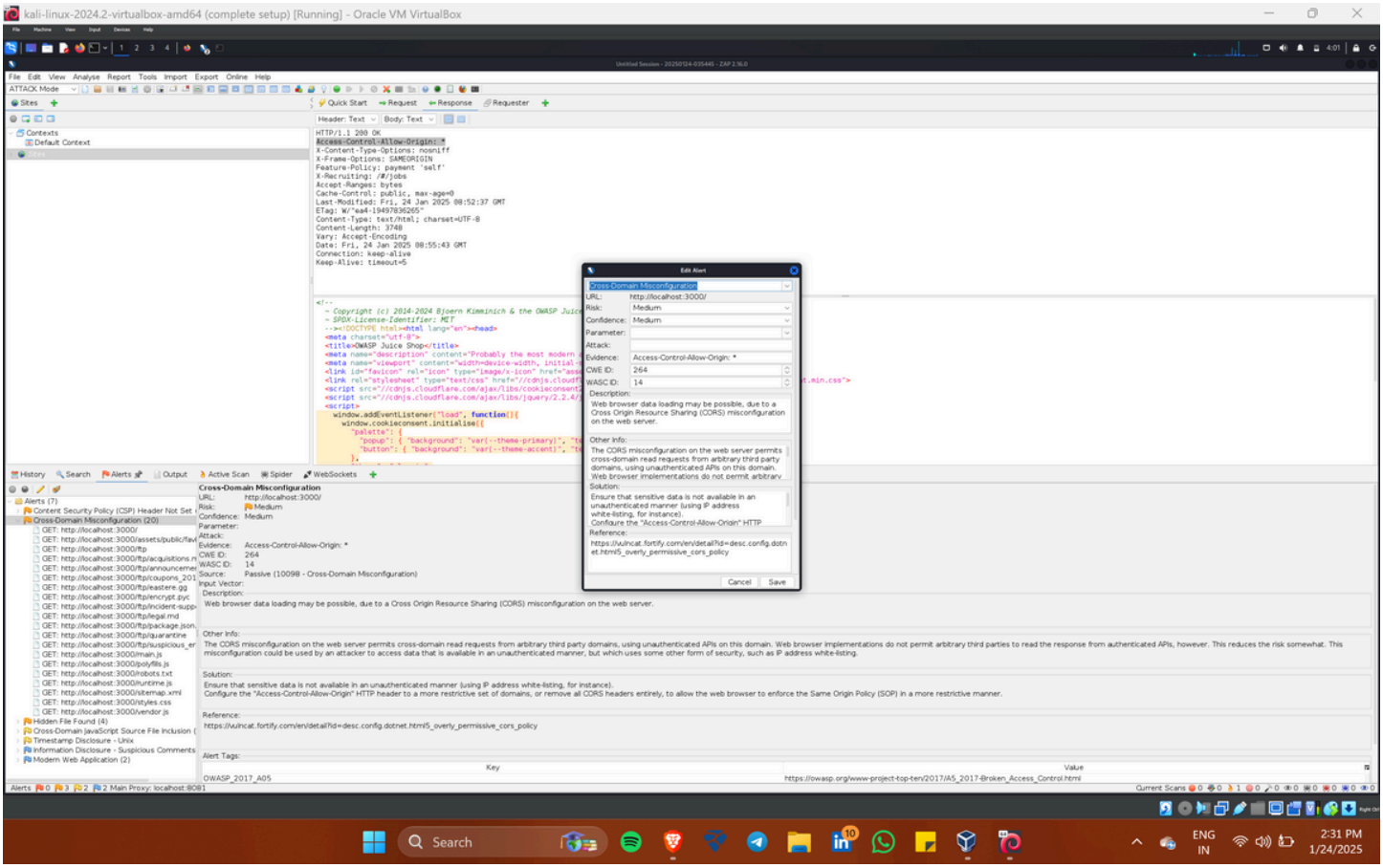


**Figure - 4 : Alerts Tab featuring the descriptions and solutions for remediation**

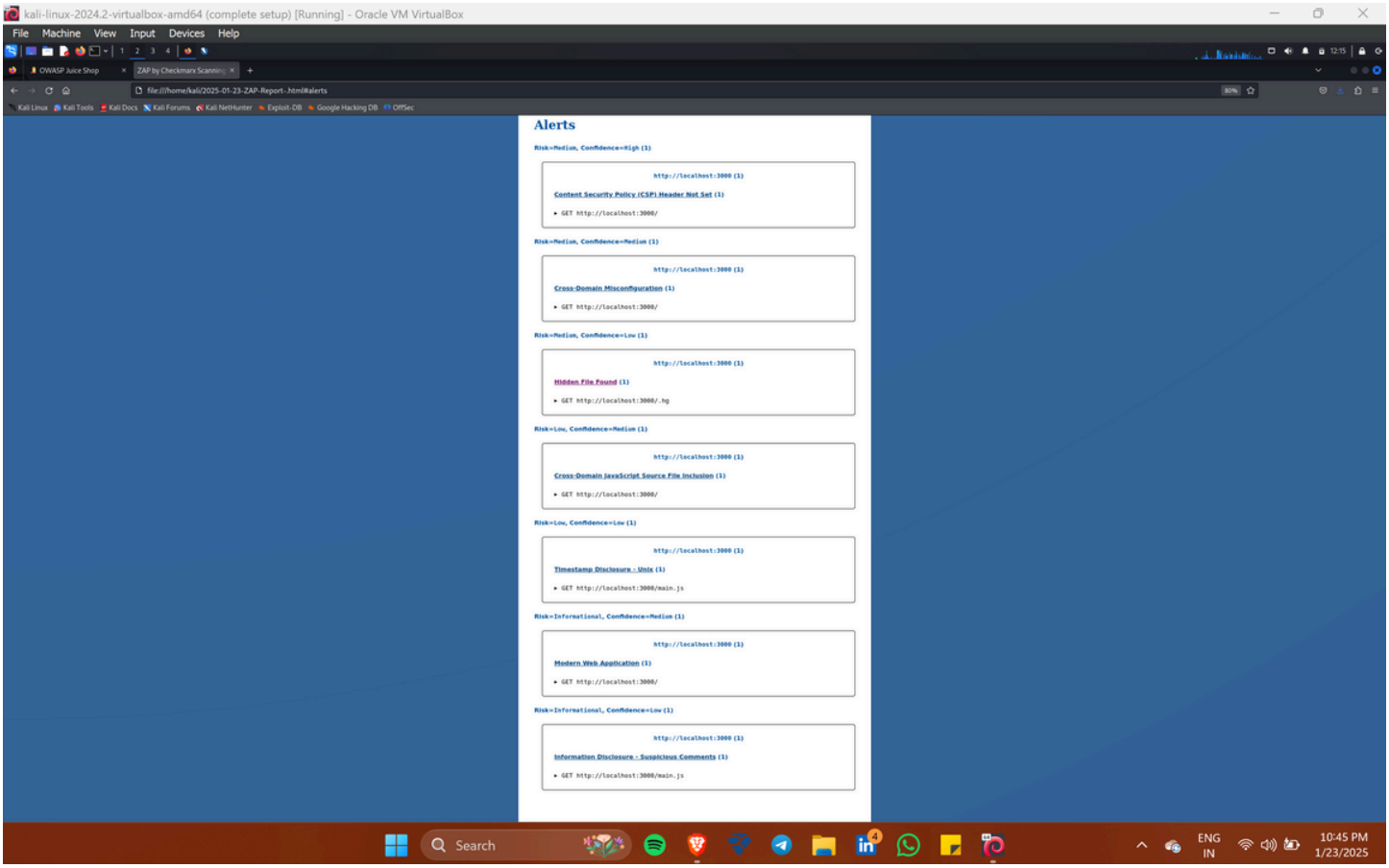


**Figure - 5 : OWASP ZAP REPORT**