**INCIDENT REPORT: BN-19002-Offensive-Access-Secured-Document**

**Date: 6/28/2024**

**Executive Summary:**

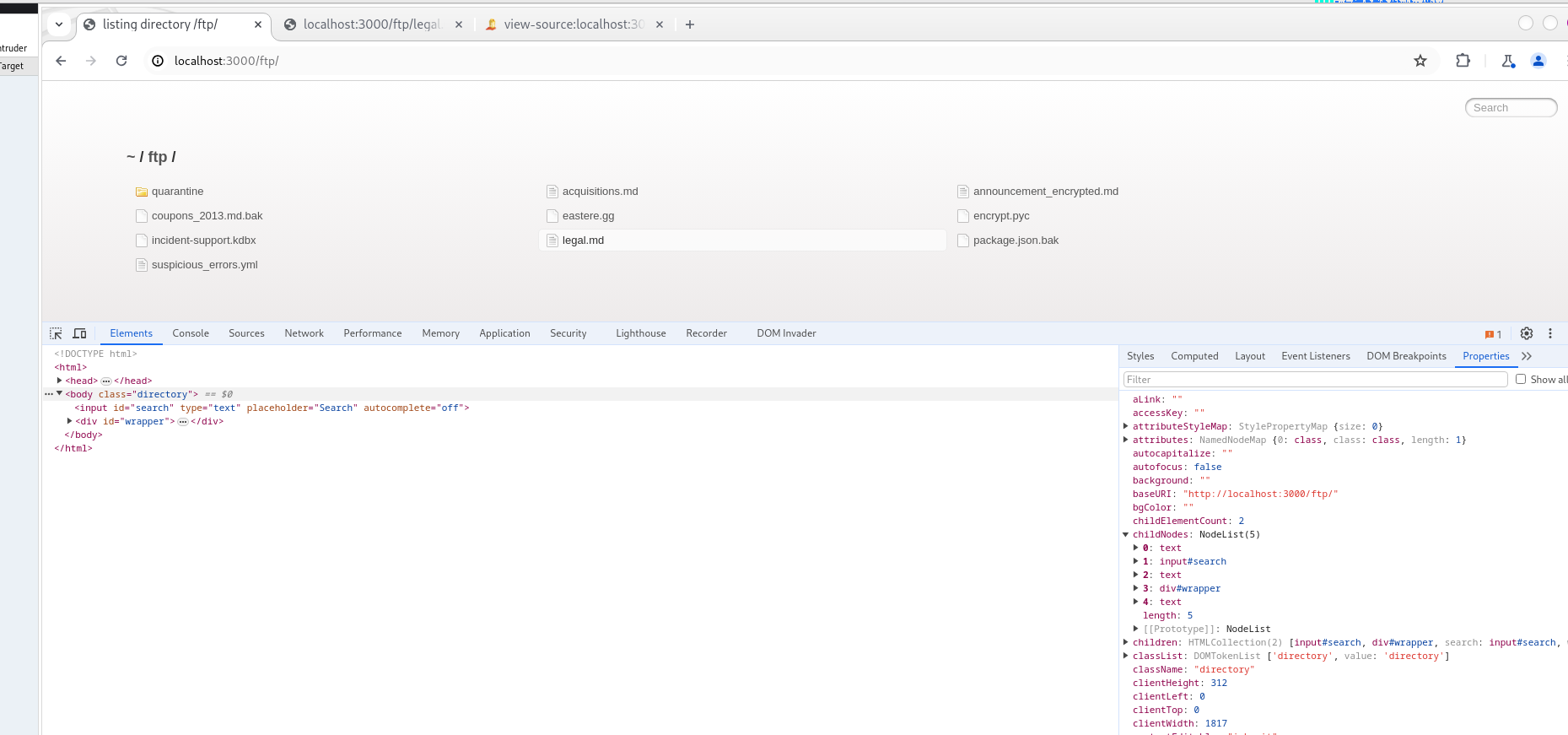
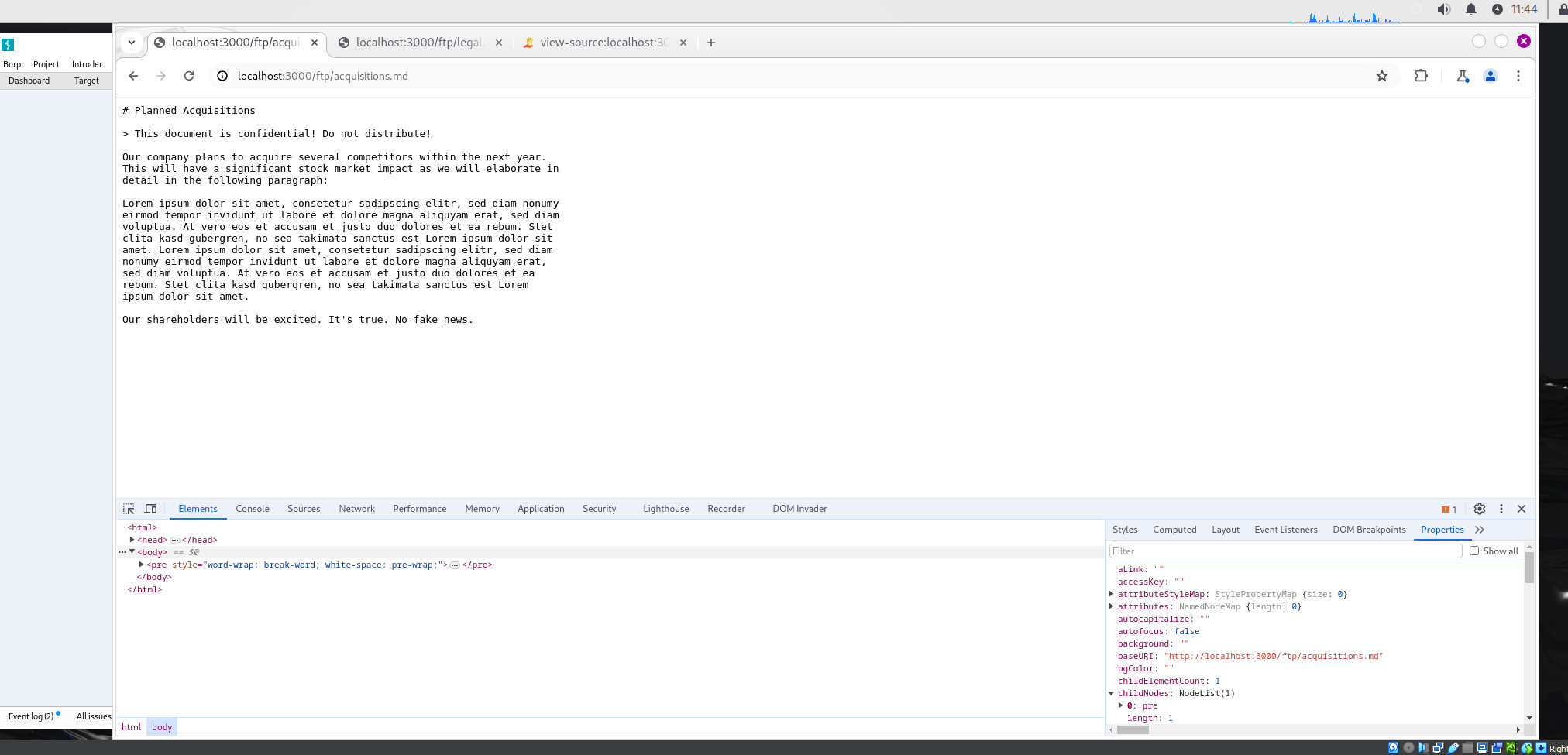
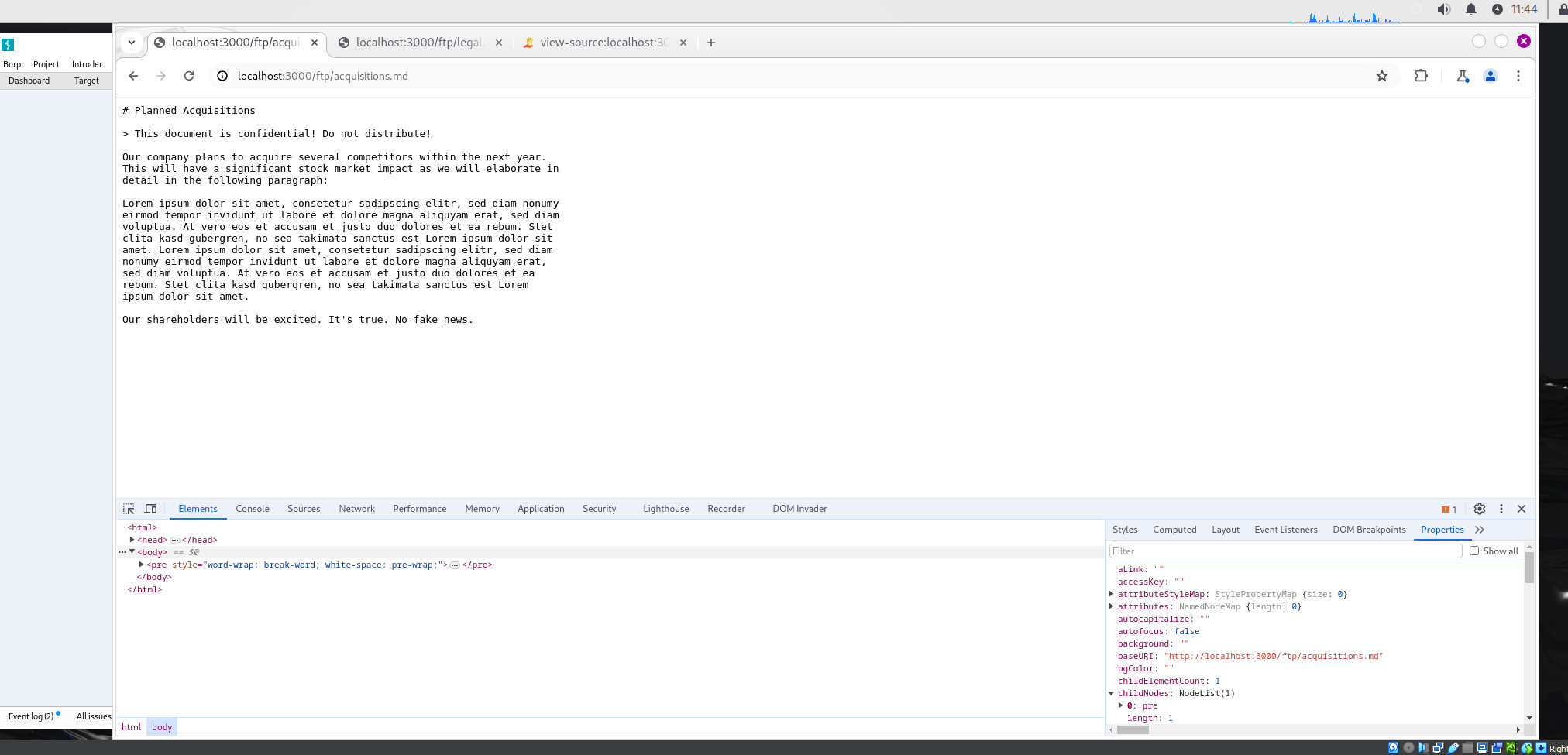
During security testing, the sensitive "acquisitions.md" file was discovered within the OWASP Juice Shop application's file structure. This file was accessible due to inadequate access controls on the /ftp directory.

**Findings:**

**Sensitive Data Exposure:** The "acquisitions.md" file, containing confidential information about planned acquisitions, was found within the publicly accessible /ftp directory.

**Inadequate Access Controls:** The lack of restrictions on the /ftp directory allowed unauthorized users to browse and download sensitive files.

**Evidence:**



**Application Details:**

* Burp Suite Community Edition: v2024.4.4.5
* OWASP Juice Shop: Latest version (running on Docker)

**Attack Narrative:**

1. Explored the Juice Shop's "About Us" page.
2. Noticed a link to /ftp/legal.md.
3. Accessed the /ftp directory by removing "legal.md" from the URL.
4. Discovered and accessed the "acquisitions.md" file.

**Consequences:**

**The exposure of the "acquisitions.md" file poses severe risks, including:**

* **Competitive Disadvantage:** Competitors could exploit the information for their gain, potentially disrupting the company's strategic plans.
* **Financial Loss:** Premature disclosure of acquisition targets could lead to increased costs or failed deals.
* **Legal Issues:** Unauthorized disclosure of sensitive financial information could violate securities regulations or other legal requirements.

**Prevention Strategies:**

**To mitigate this vulnerability, the following actions are recommended:**

* **Implement Strict Access Controls:** Restrict access to the /ftp directory and all sensitive files to authorized personnel only.
* **Review File Permissions:** Ensure that files containing sensitive data have appropriate permissions to prevent unauthorized access.
* **Regular Security Audits:** Conduct routine security assessments to identify and address potential vulnerabilities in file structures and access controls.