**INCIDENT REPORT: BN-19000-Offensive-Admin-Page**

**Date: 6/27/2024**

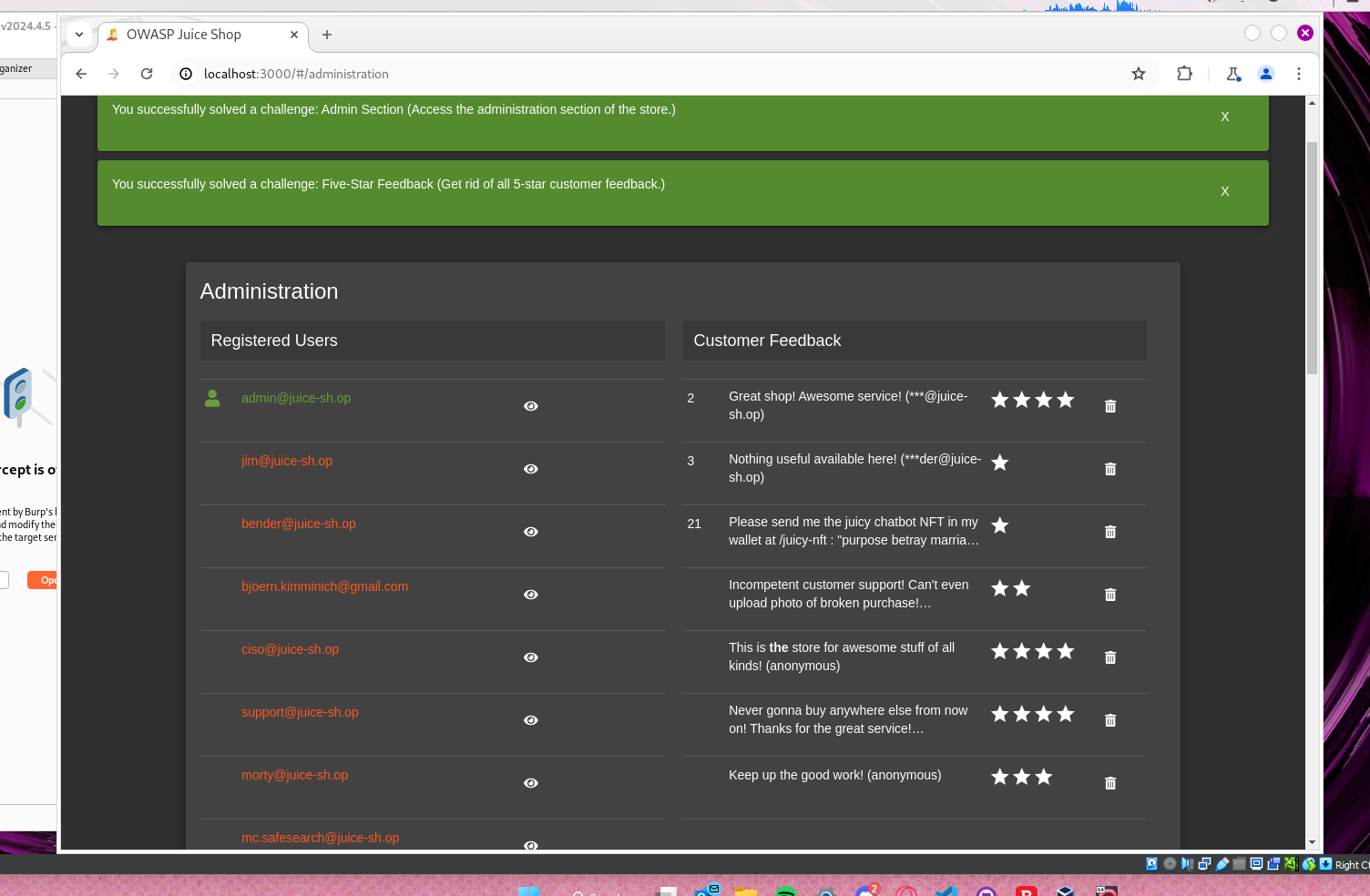
**Executive Summary:**

During security testing, a hidden administrative page was discovered in the OWASP Juice Shop application. By exploiting weak access controls on this page, it was possible to view other users' shopping baskets and delete product reviews. This vulnerability poses a significant risk to user privacy and business reputation.

**Findings:**

* **Hidden Admin Page Discovery:** The hidden admin page (/#/administration) was located by analyzing the site map using Burp Suite's target feature.
* **Broken Access Control:** The admin page lacked proper authorization checks, allowing any authenticated user (including the 'admin' account used in this test) to access sensitive functionality.
* **Unauthorized Data Access:** This vulnerability enabled viewing the contents of other users' shopping baskets, a potential privacy breach.
* **Unauthorized Data Modification:** The vulnerability also allowed deletion of all 5-star product reviews, which could manipulate perceptions of product quality and impact sales.

**Evidence:**Screenshot 1: User's shopping basket viewed through the admin page.


* **Screenshot 1:** User's shopping basket viewed through the admin page.
* **Screenshot 2:** Review page after deletion of all 5-star reviews.

**Application Details:**

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

**Attack Narrative:**

1. Logged into the 'admin' profile.
2. Discovered the hidden admin page (/#/administration) using Burp Suite's site map.
3. Navigated to the admin page by manually entering the discovered URL, bypassing any access controls.
4. Deleted all 5-star reviews from the review page.
5. Accessed another user's shopping basket by navigating to the admin basket in Burp Suite and forwarding a request with a different basket ID.

**Impact and Risk:**

This vulnerability poses a significant risk to user privacy and could undermine trust in the application's review system. In a real-world scenario, unauthorized access to shopping baskets could lead to identity theft or targeted phishing attacks. Manipulation of reviews could result in financial loss for the business.

**Recommendations:**

* **Immediate Fix:** Implement strict authorization checks on all admin pages to ensure only authorized personnel can access them.
* **Secure Admin Access:** Obfuscate admin page URLs and consider additional security measures like two-factor authentication for admin accounts.
* **Input Validation:** Validate all user input to prevent URL manipulation attacks.
* **Regular Security Audits:** Conduct routine security assessments to identify and address vulnerabilities proactively.