**INCIDENT REPORT: BN-18984-Admin-Password-Reset**

**Date: 6/19/2024**

**Executive Summary:** I was tasked with discovering the administrator's password in OWASP Juice Shop and changing it, demonstrating the risk of weak passwords and unauthorized access.

**Results**

* **Exploit Successful:** Successfully brute-forced the admin password and changed it.
* **Old Password:** admin123
* **New Password:** brandon

**Application Details:**

* OWASP Juice Shop: Latest version
* Burp Suite Community Edition: v2024.4.4.5

**Attack Narrative:**

1. **Intercepted Login Request:** Used Burp Suite to capture the HTTP POST request for the admin login page.
2. **Configured Intruder Attack:**
   * **Attack Type:** Sniper
   * **Payload Position:** Password field
   * **Payload List:** best1050.txt wordlist
3. **Launched Attack:** Initiated the Intruder attack to systematically test passwords from the wordlist.
4. **Identified Successful Payload:** Observed a successful login attempt when the payload "admin123" was used as the password.
5. **Logged in as Admin:** Entered the discovered password ("admin123") in the intercepted login request and forwarded it to successfully log in as the administrator.
6. **Changed Password:** Navigated to the account settings page and changed the admin password to "brandon."

**Conclusion:**

This exercise demonstrates the risks associated with using weak or easily guessable passwords, especially for privileged accounts. A successful brute-force attack can lead to unauthorized access, data breaches, and potential system compromise. Implementing strong password policies, encouraging the use of password managers, and enabling MFA are crucial steps to mitigate this risk

.