**INCIDENT REPORT: BN-18985-CAPTCHA-Exploit**

**Date: 6/20/2024**

**Executive Summary:** I was tasked with exploiting a broken CAPTCHA mechanism in OWASP Juice Shop by sending multiple requests in rapid succession using Burp Suite's Intruder tool. This exercise demonstrates how inadequate anti-automation measures can leave web applications vulnerable to abuse.

**Results**

* Successfully sent 13 CAPTCHA responses through the customer feedback form.
* Successfully sent 50 CAPTCHA responses, incrementing the customer rating to 500.

**Application Details:**

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

**Attack Narrative:**

1. **Intercepted Request:** Captured the POST request to the /api/Feedbacks endpoint using Burp Suite.
2. **Analyzed Request:** Examined the request in Repeater and determined that no modifications were needed for a successful submission.
3. **Configured Intruder Attack (Comments):**
   * **Attack Type:** Sniper
   * **Payload Position:** Appended a number to the end of the comment field.
   * **Payload Type:** Number
   * **Payloads:** 1, 2, 3... 13
4. **Launched Attack (Comments):** Successfully sent 13 modified feedback requests.
5. **Configured Intruder Attack (Ratings):**
   * **Attack Type:** Sniper
   * **Payload Position:** Incremented the rating parameter by 10.
   * **Payload Type:** Number
   * **Payloads:** 10, 20, 30... 500
6. **Launched Attack (Ratings):** Successfully sent 50 modified feedback requests with inflated ratings.

**Conclusion:**

This exercise demonstrates the importance of implementing robust anti-automation measures in web applications. The broken CAPTCHA in Juice Shop allowed for the submission of multiple requests within a short timeframe, which could be leveraged for malicious purposes like flooding the server with fake feedback, manipulating ratings, or potentially causing a denial-of-service (DoS) attack. Properly implemented CAPTCHA mechanisms, rate limiting, and other safeguards can help mitigate such risks.



