**Incident Report: KG-19108-Offensive:-CAPTCHA-Exploit  
Date:** 09-12-2024

### **Executive Summary**

In this task, I exploited a weak CAPTCHA mechanism in the customer feedback section of OWASP Juice Shop by flooding it with multiple HTTP requests using Burp Suite. The goal was to send 10+ CAPTCHA submissions simultaneously to bypass the CAPTCHA’s security and trigger a completion flag.

### **Methodology**

To complete this task, I followed these steps:

1. **Captured the CAPTCHA HTTP Request:**I navigated to the customer feedback section on the Juice Shop site, filled out a feedback form, and captured the HTTP request using Burp Suite’s proxy feature.
2. **Configured Burp Suite’s Intruder Tool:**After capturing the initial CAPTCHA request, I sent the request to Burp Suite’s Intruder tool. In Intruder, I configured the tool to send the same feedback request repeatedly, adjusting the payload values to mimic multiple submissions.
3. **Executed the CAPTCHA Flood Attack:**Using Burp Suite’s Intruder feature, I sent 10+ requests at once, overwhelming the CAPTCHA’s intended security measure and bypassing the validation process.
4. **Completion Confirmation:**After successfully flooding the CAPTCHA, I took a screenshot of the task completed modal and a screenshot of Burp Suite showing the 10+ requests sent.

### **Findings/Solutions**

The CAPTCHA flooding attack was successful, demonstrating the vulnerability of weak CAPTCHA implementations. To prevent this type of attack, CAPTCHA systems should implement rate limiting, stronger CAPTCHA algorithms, or other mechanisms like reCAPTCHA to limit the effectiveness of brute-force attacks.

**Project Description**

For this story, we will be using Burp suite to send HTTP requests.

The customer feedback area has a very unusual CAPTCHA than what is normally used.

We can exploit this CAPTCHA by flooding it with many requests in a short timeframe. Send 10+ CAPTCHAS all at once to complete this story.

Take a screen shot of the task completed modal and of Burp Suite with the 10+ sent CAPTCHAS. Include these two screenshots with your incident report.