Incident Report

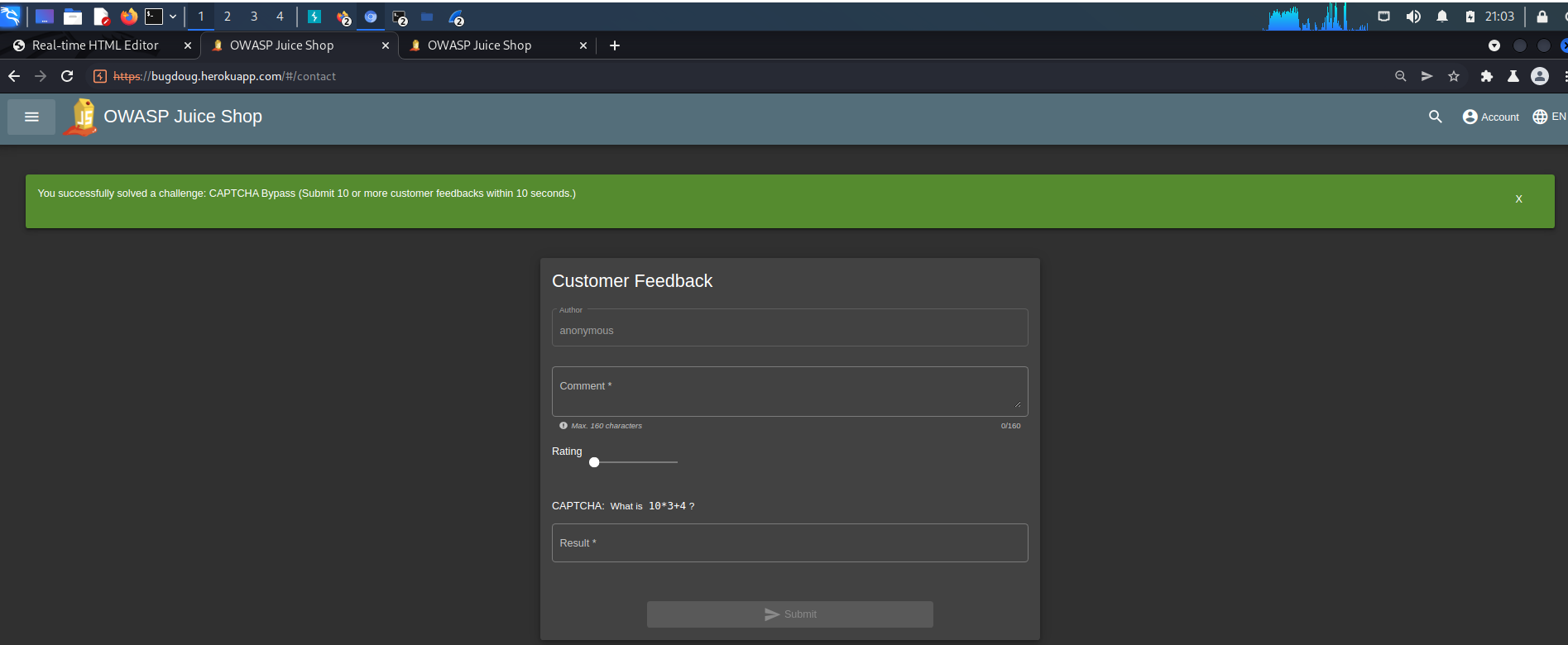
13145 Offensive: CAPTCHA Exploit

Date: 5-27-2022 (DS)

# Executive Summary:

ProsperSec was contacted by The Tech Academy to conduct brute force testing on the customer feedback page. The main goal is to see if it withstands a penetration test.

**Results**:



**Application Details:**

Application URL: bugdoug.herokuapp.com/#/contact

User Account: Any

**Attack Narrative (Steps):**

* I first captured the page using the proxy intercept tab on Burp.
* I then sent the post request to the repeater.
* I then tried sending the request again, which lead to a success (even though there was no new captcha entered.
* I then sent this over to the intruder, where I was able to load 10 random pieces of data in the payload section and set off the attack, which was successful.

Upon trying the brute force attack, I found that I could send unlimited feedback responses no matter what the captcha was.

**Conclusion:**

ProsperSec was contracted to find vulnerabilities on this page, the result was that the Captcha implemented is not secure and is vulnerable to brute force attacks which allow a bypass of the Captcha criteria.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_