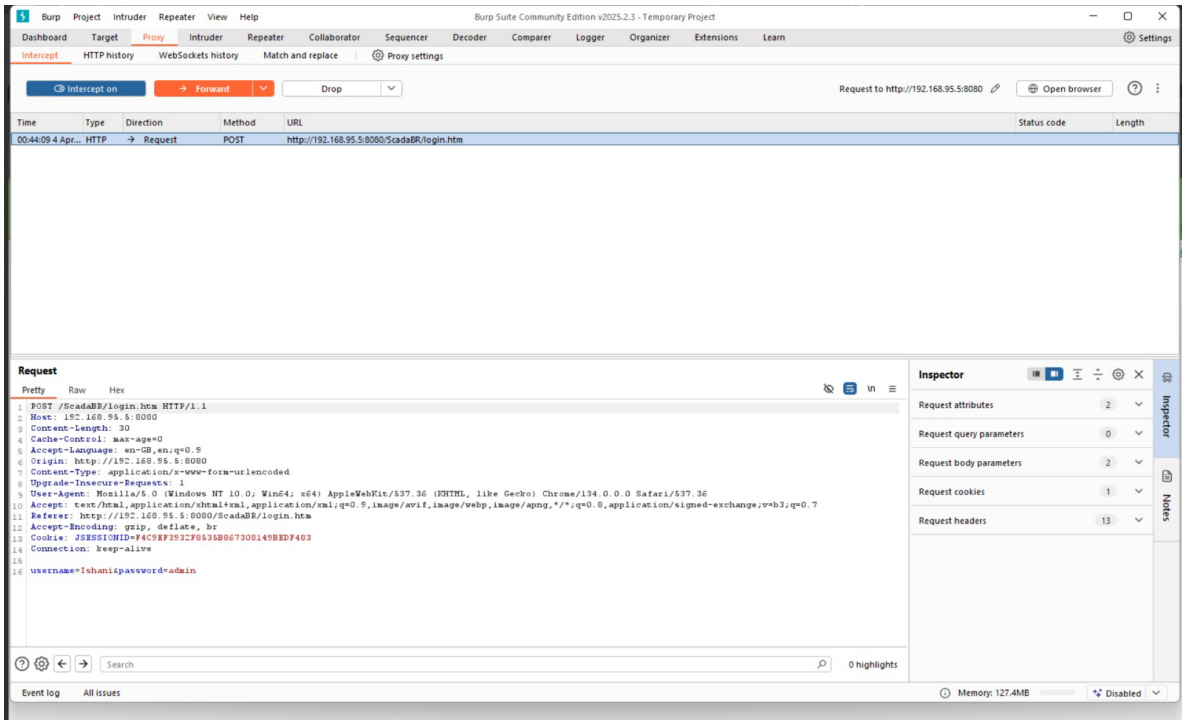
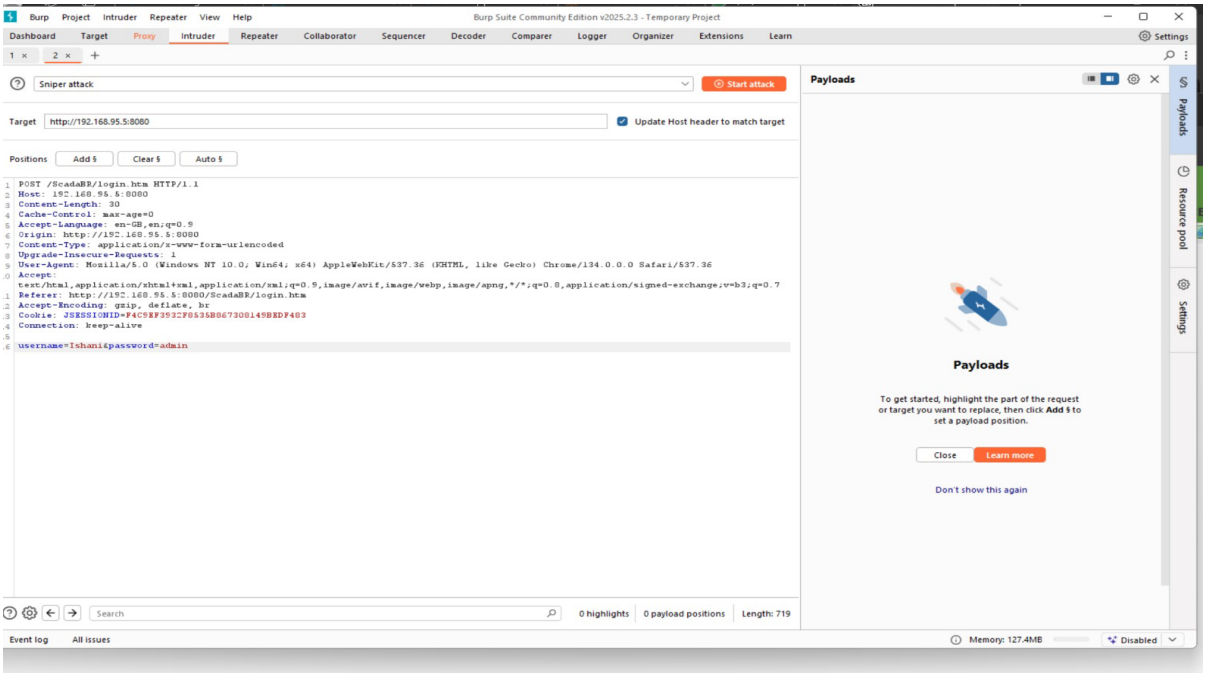
Step1: Download burpsuite. Burp Suite is designed specifically for web application security assessments, making it an ideal tool for analyzing HMI web interfaces. Using burpsuite's default settings I started my project.

Step2: Click on the proxy tab, make sure the intercept is off. Open a burpsuite browser and search for http://192.168.95.5:8080/ScadaBR. Trying logging in with random credentials on the ScadaBR page.

Step3: Manually I tried a few credentials on ScadaBR. For my last try I entered random credentials again and before clicking on the login button I went back to burpsuite and turned on intercept. The **Intercept** feature in Burp Suite allows you to capture, modify, and forward HTTP/S requests and responses between your browser and the target web server in real-time.



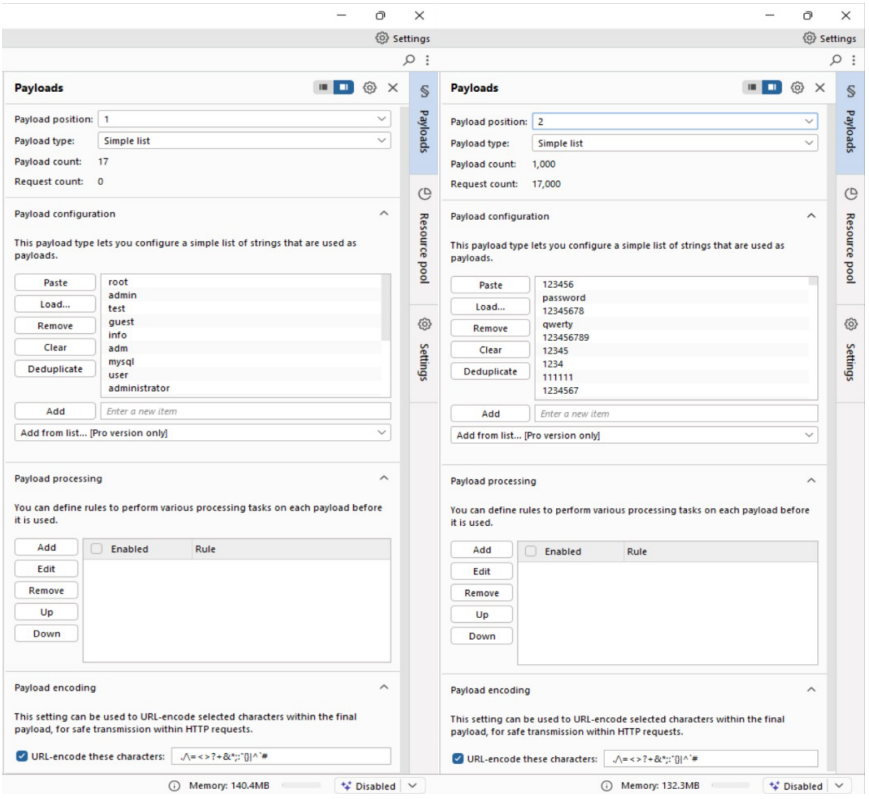
Step4: I then went on to the request tab sent it to the Intruder tab. The **Intruder** tool in Burp Suite automates attacks by sending multiple payloads to a target, helping identify vulnerabilities like weak authentication, injection flaws, and rate-limiting issues.



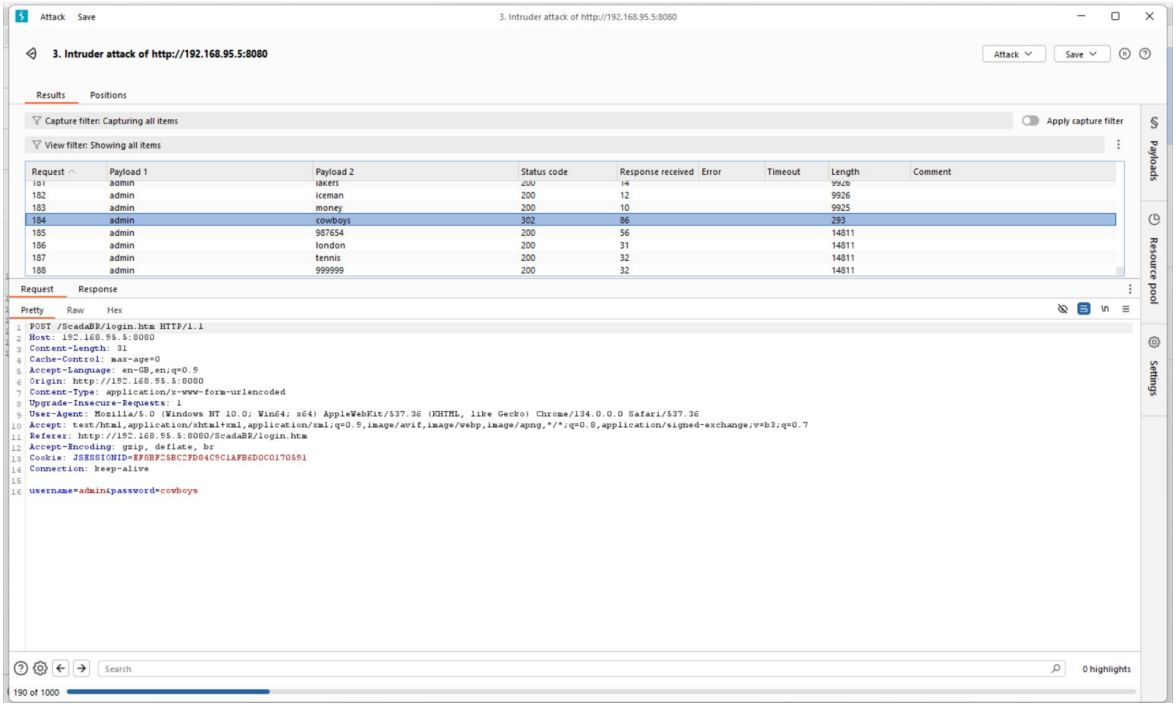
Step5: In the intruder section, I replaced the username and password with $$. I then changed the

attack to cluster bomb attack. The **Cluster Bomb** attack in Burp Suite Intruder tests multiple payloads across multiple positions using every possible combination to uncover complex input-based vulnerabilities.

Step6: I then went into the payload section and loaded a list of usernames and passwords from a file called Seclists which available on Github. Seclists contains a file named toplistusernames and passwords, I selected that. I then select the document “xato-net-10-million-passwords-#”. As you load this file in the payload configuration box, the box displays potential passwords. On starting the attack, there’s a new window which displays password attempts in real time. Payload position 1 displays username and payload position 2 displays password.



Step7: When I started the attack, I observed every attempt was giving response code as 200. After some time, one of the passwords gave a response code of 302. Here, the username: admin and password: cowboys.



Step8: Then I went back to the browser and tried these credentials AND IT WORKED!