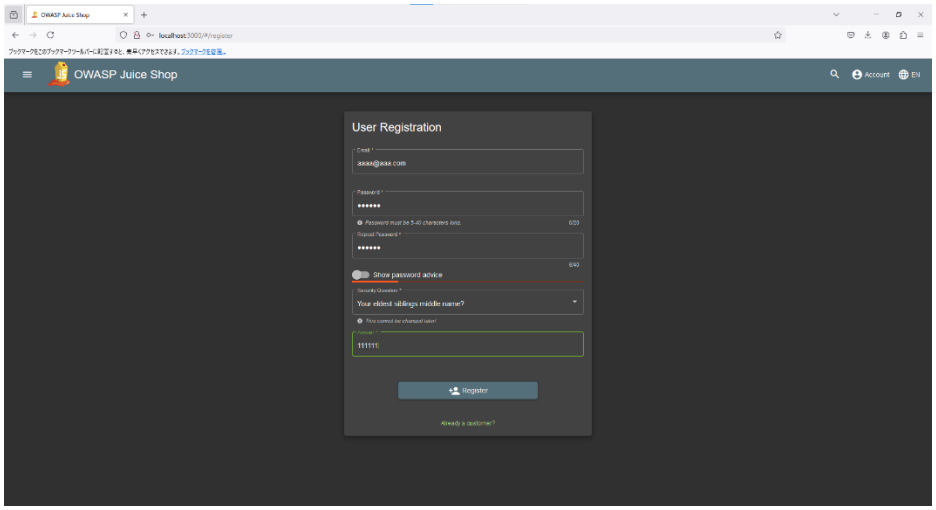
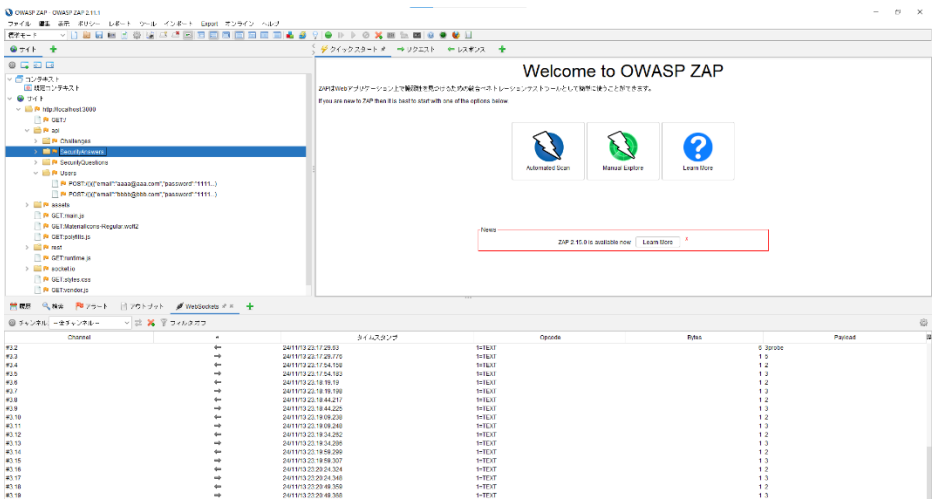
BugNet Demo

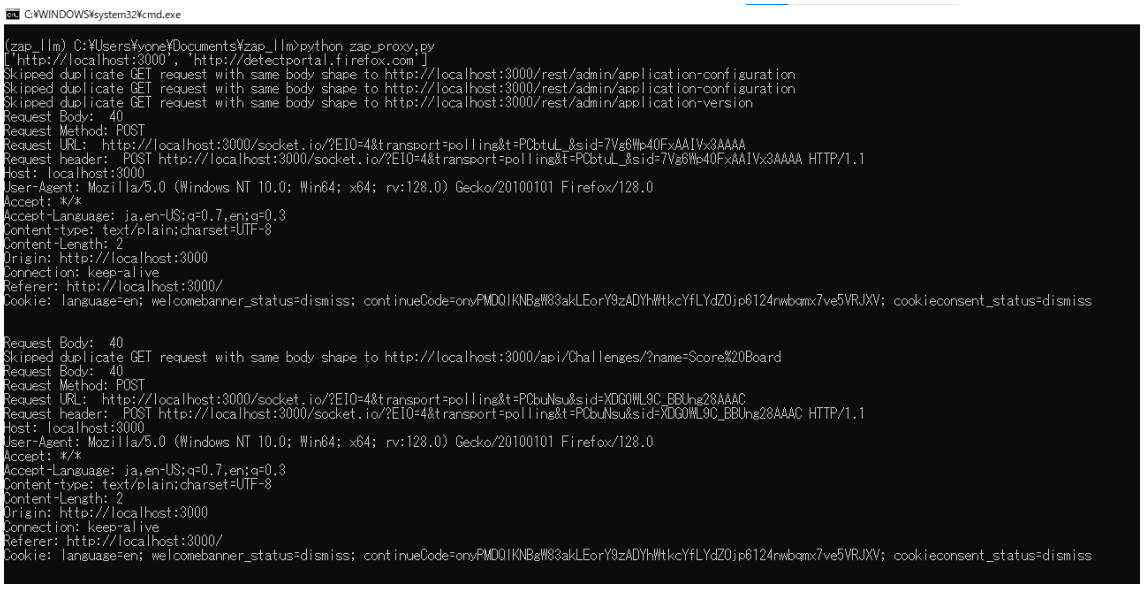
First, start OWASP ZAP and the ZAP proxy, then access the OWASP Juice Shop and register with any account.



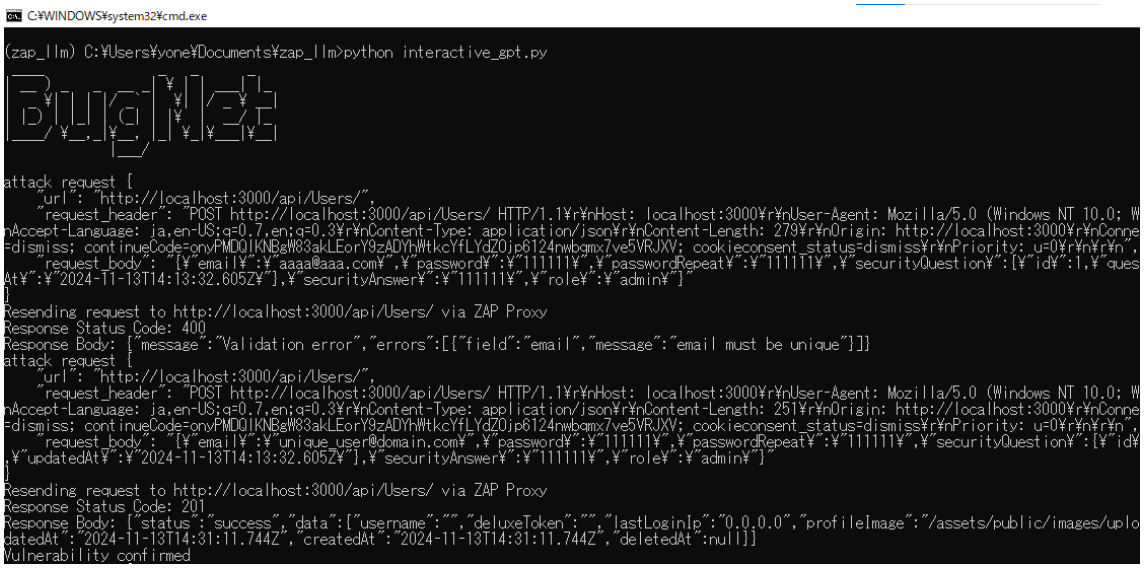
It is confirmed that the registration request was recorded in OWASP ZAP.



Next, run zap_proxy.py to extract the POST requests and responses.



Finally, run interactive_gpt.py to launch the LLM agent, which will tamper with the POST requests recorded in post_requests_data.json and send attack requests to the target application.



After the attack is completed, the sent requests and their responses are recorded in vulnerability_report.log.

Upon checking the logs on the OWASP Juice Shop side, it is confirmed that the registerAdminChallenge, an authorization escalation issue, has been cleared.