PASSWORD CRACKING

1)Configuring of Victim's browser on proxy server:

- Open Victim's browser then goto Network Setting.
- Choose Manual Proxy and set IP address as :127.0.0.1 and Port number as:8080.

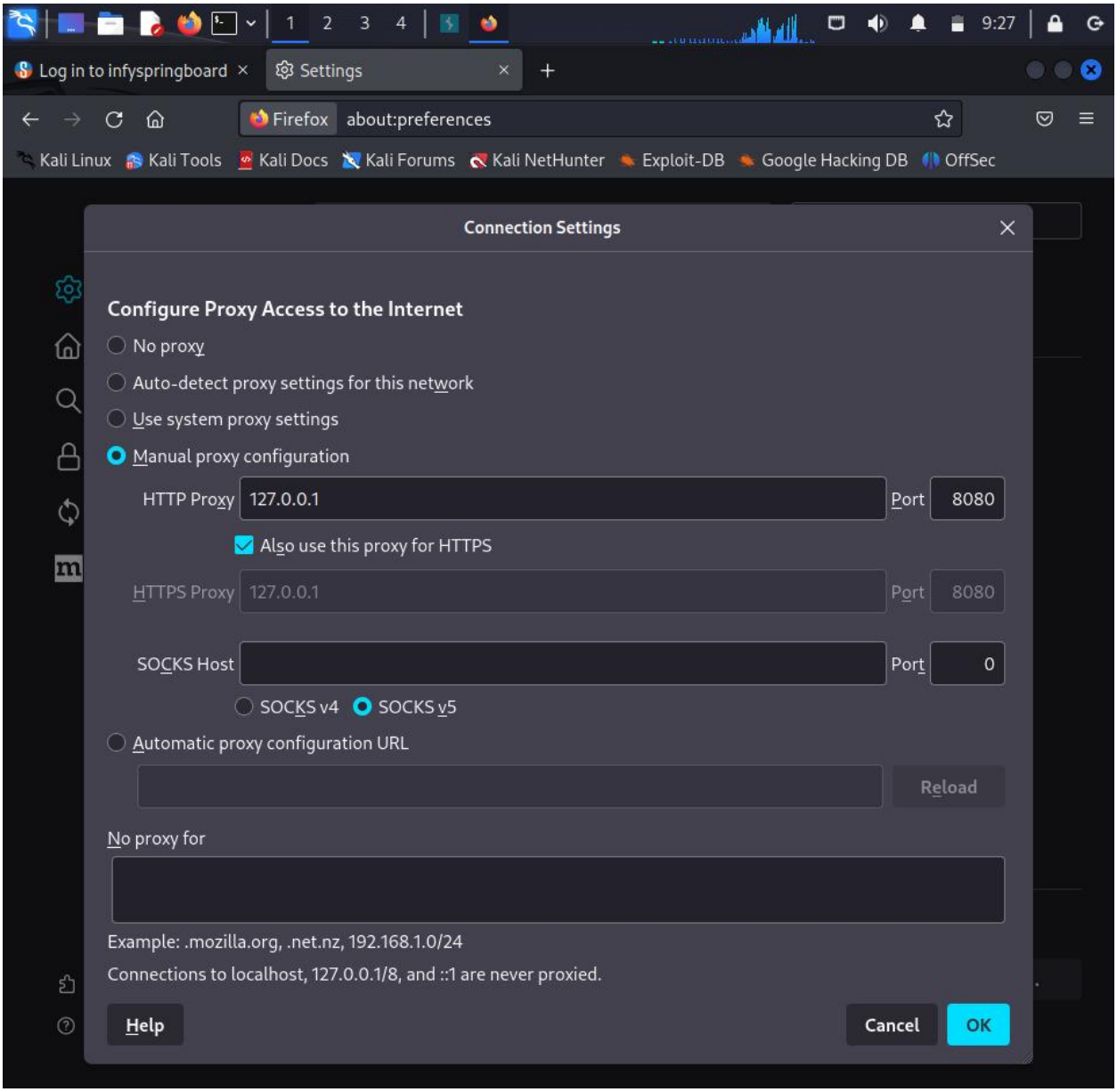

Fig. Manual Proxy Configuration in the Victim's browser

2) Capturing Victim's requested information in Burp suit:

- Turn on the Burp suit and goto Target panel.
- Find the **POST** https request and push it to **INTODUCER** panel by right clicking on mouse pad and select the **SEND TO INTRODUCER** option.

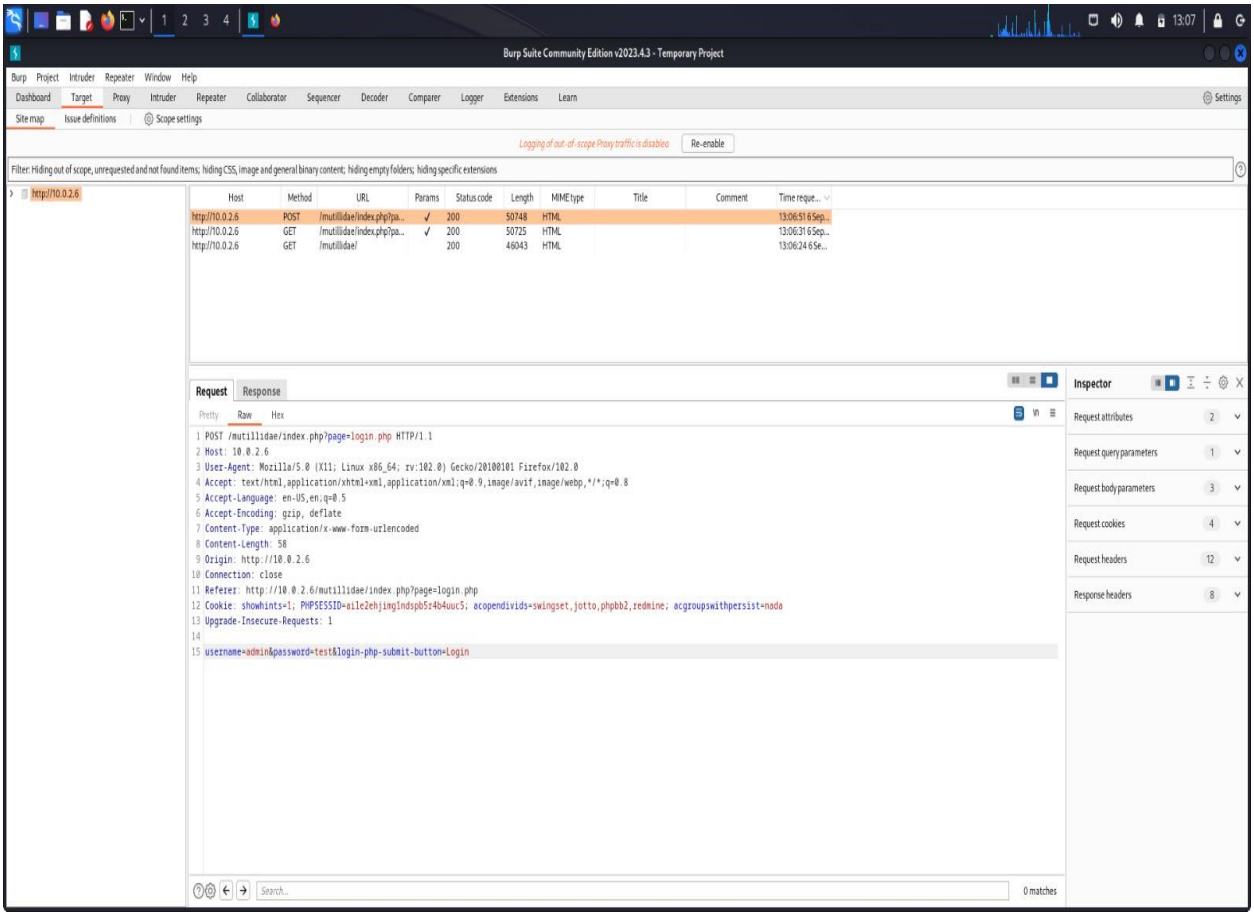

Fig. Pushing of POST request of Victim's browser to the Introducer panel

3)Configuration of OWASP tool:

- Turn on OWASP machine and search the IP address of OWASP into Kali's browser.
- Select OWASP Mutillidate II > Login/Register >login with some dummy credentials.

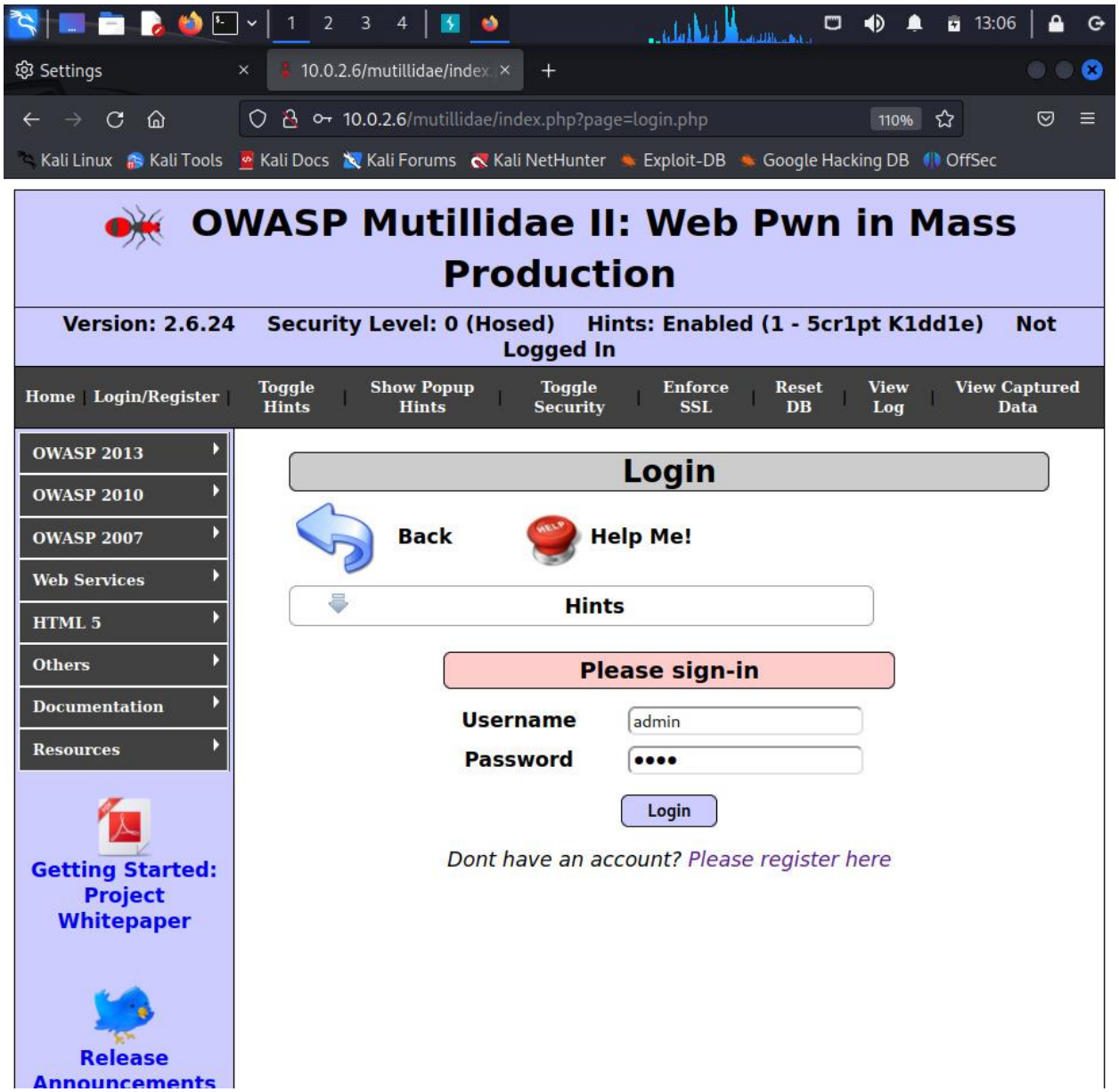

Fig. Logging in into OWASP Mutillidate II with some dummy credentials

4)Fuzzing of Password field and loading of Wordlist into the Payloads:

- The field which was unknown like, PASSWORD field was unknown in most of the cases, so select password and click on **Add $** button to select that as a Payload field.
- Type the possible number of passwords into a **Notepad** file and save it as some name <filename>.txt extension.
- Then goto **Payload** panel and click on load button and select the wordlist file and open it.
- Once Wordlist file content is loaded successfully verify every fields once again and if all fields are correct then click on **Start attack** button.
- **Note:** if only one field is unknown like, either username or password, then select attack type as **Sniper** or else select **Cluster**.

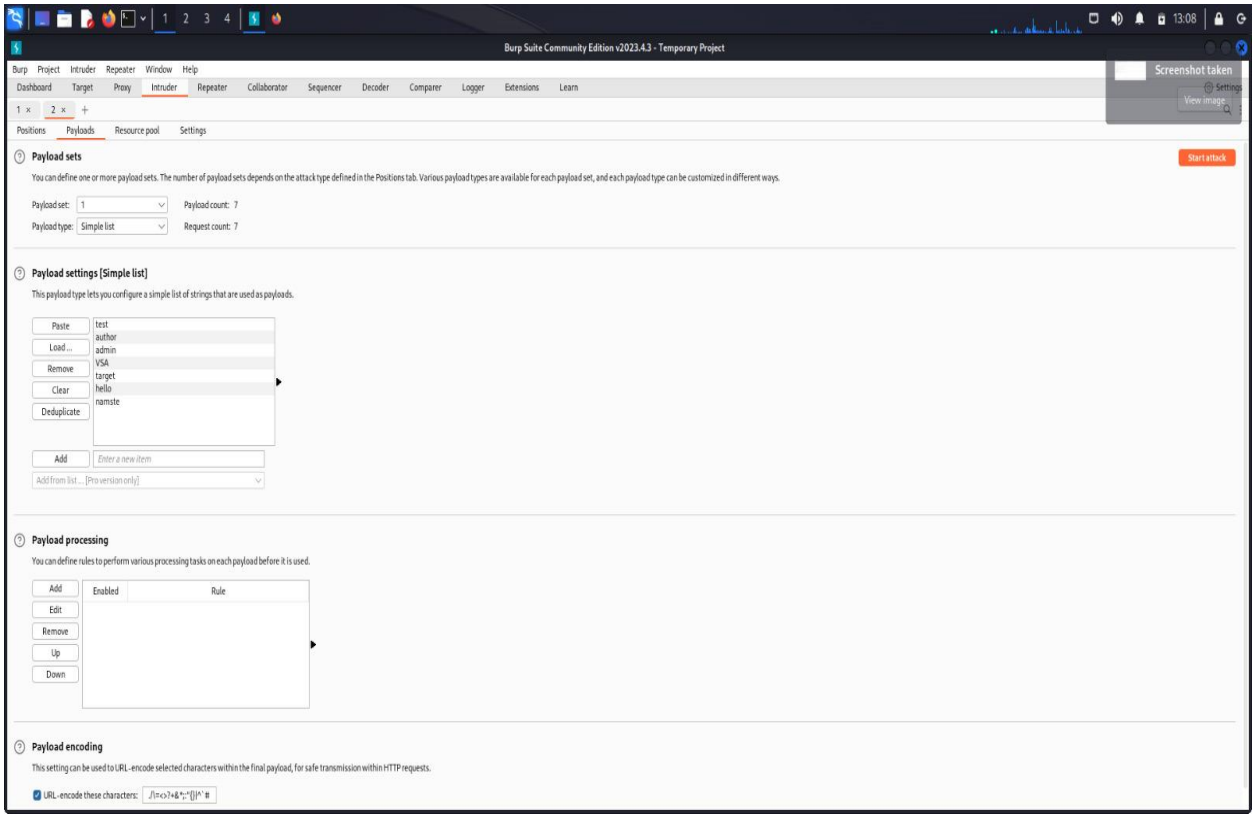

Fig. Successful loading contents from Wordlist file

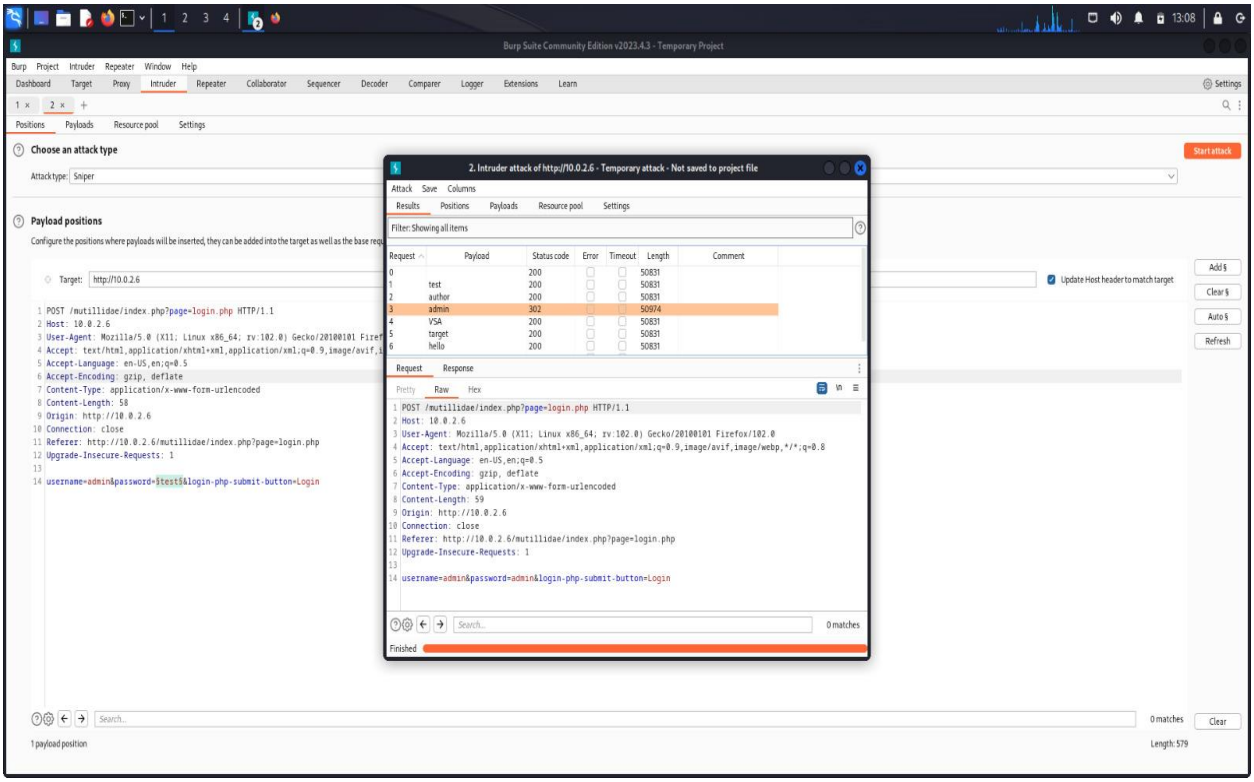

Fig. Successfully cracks the Password

Note: The attempt which will have Unique status code indicates the correct password for login.

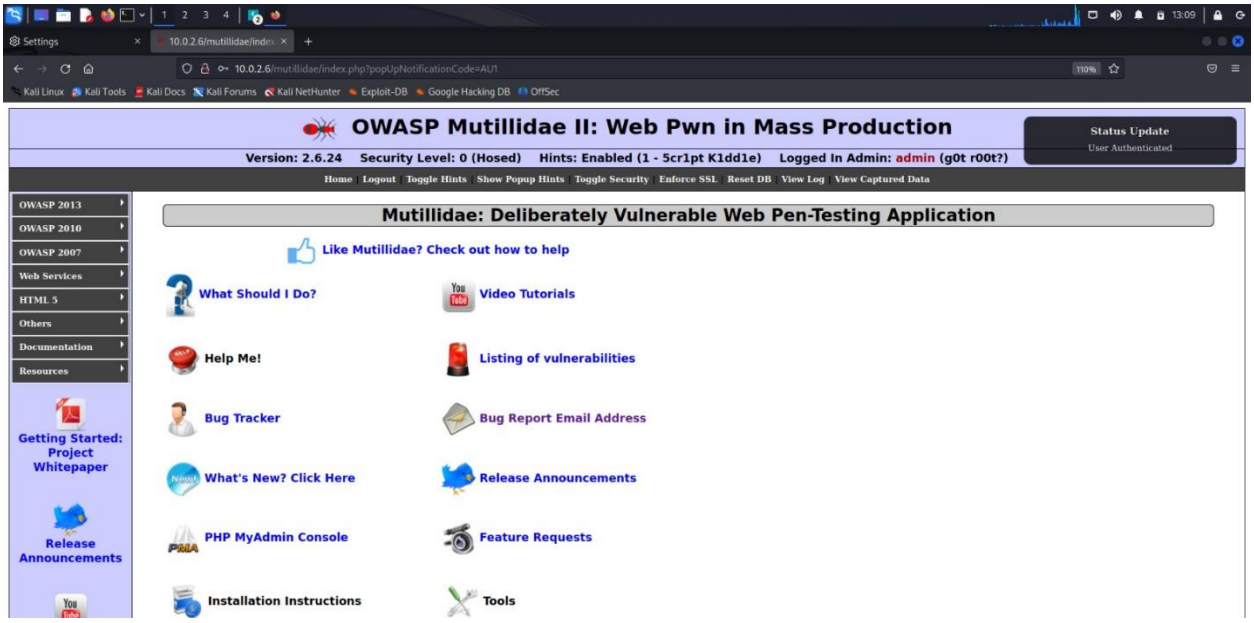

Fig. Using of cracked password and logging in