LOCAL FILE INCLUSION

1) Configuring of Victim Browser onto Proxy server:

- Turn ON Burp Suit.
- Go to Victim browser and open Network Setting, set Manul proxy server to the IP address:127.0.0.1 and Port number:8080.
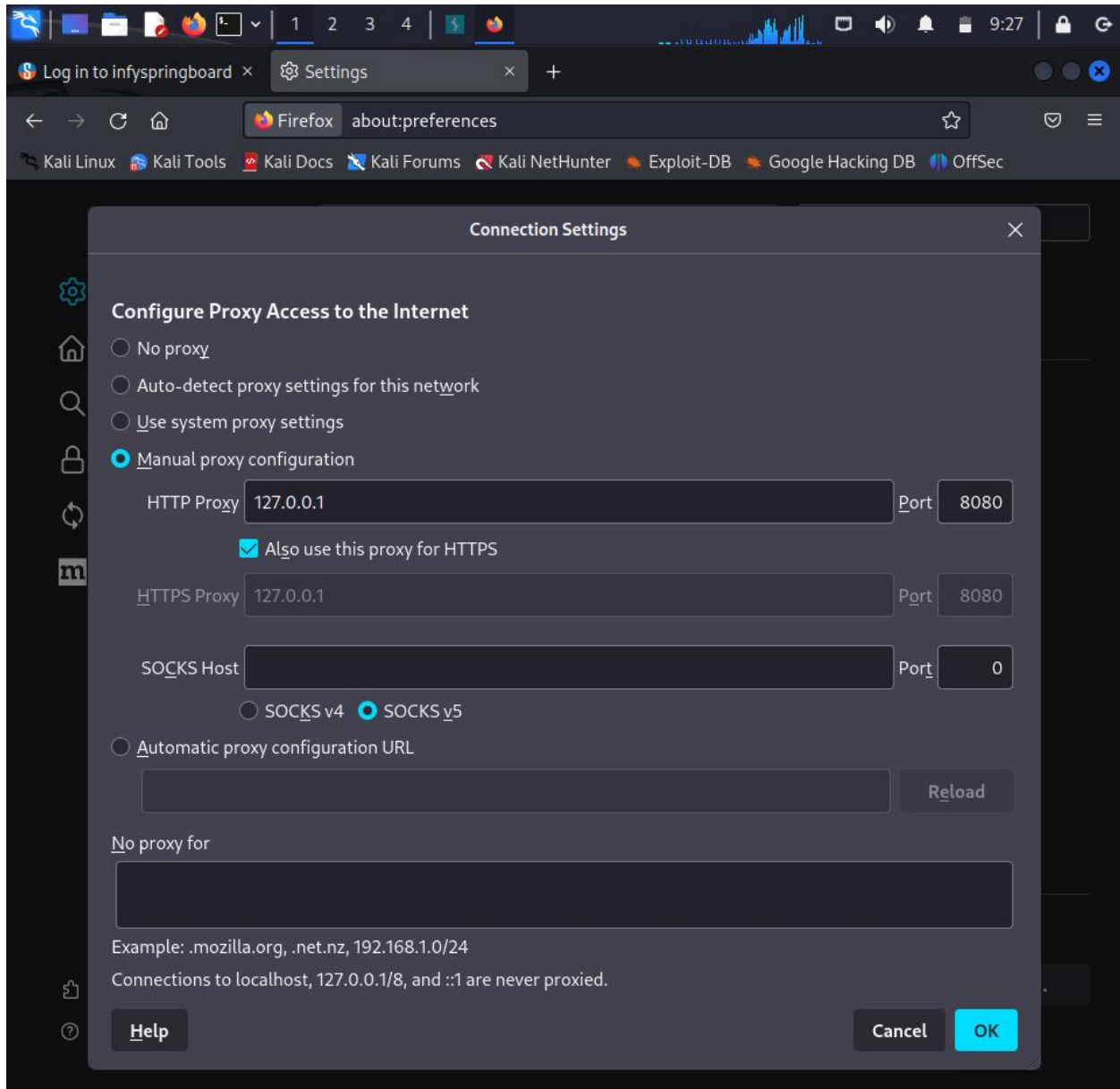

Fig. Manul Proxy Configuration in the Victim machines Browser

2)Victim requesting for the information:

- Open OWASP > OWASP webgoat > Access Control Forms > Bypass Path Based Access Control Scheme.
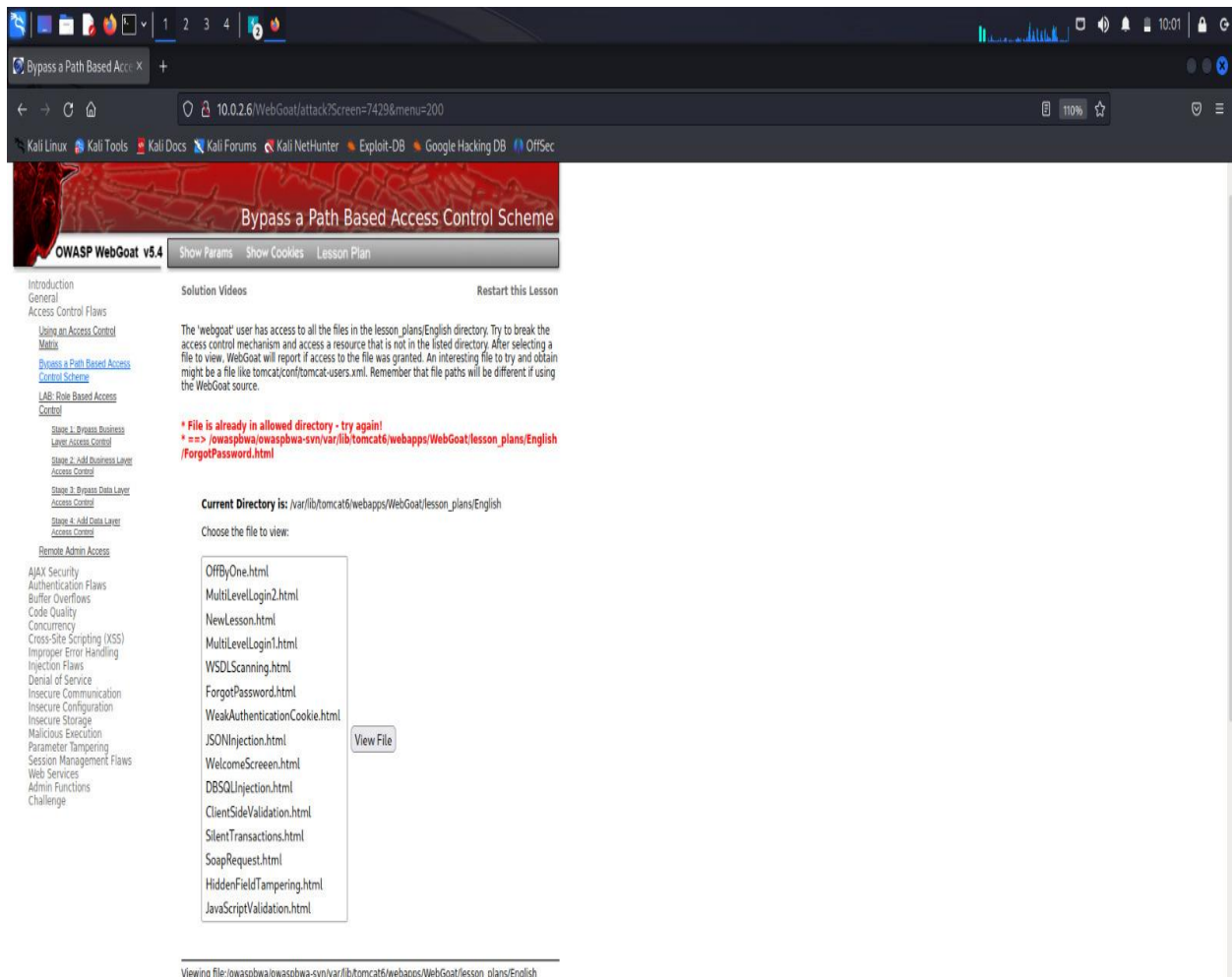- Then request for any HTML file in the list.

Fig. Victim viewing the HTML files

3) Capturing of Information in Burp Suit:

- Turn ON Burp Suit and goto Target panel, there we can find the requests of Victim's browser.
- Then push the latest file request of Victim to the Intruder panel by right clicking on mouse pad and choose **SEND TO INTRUDER** option.
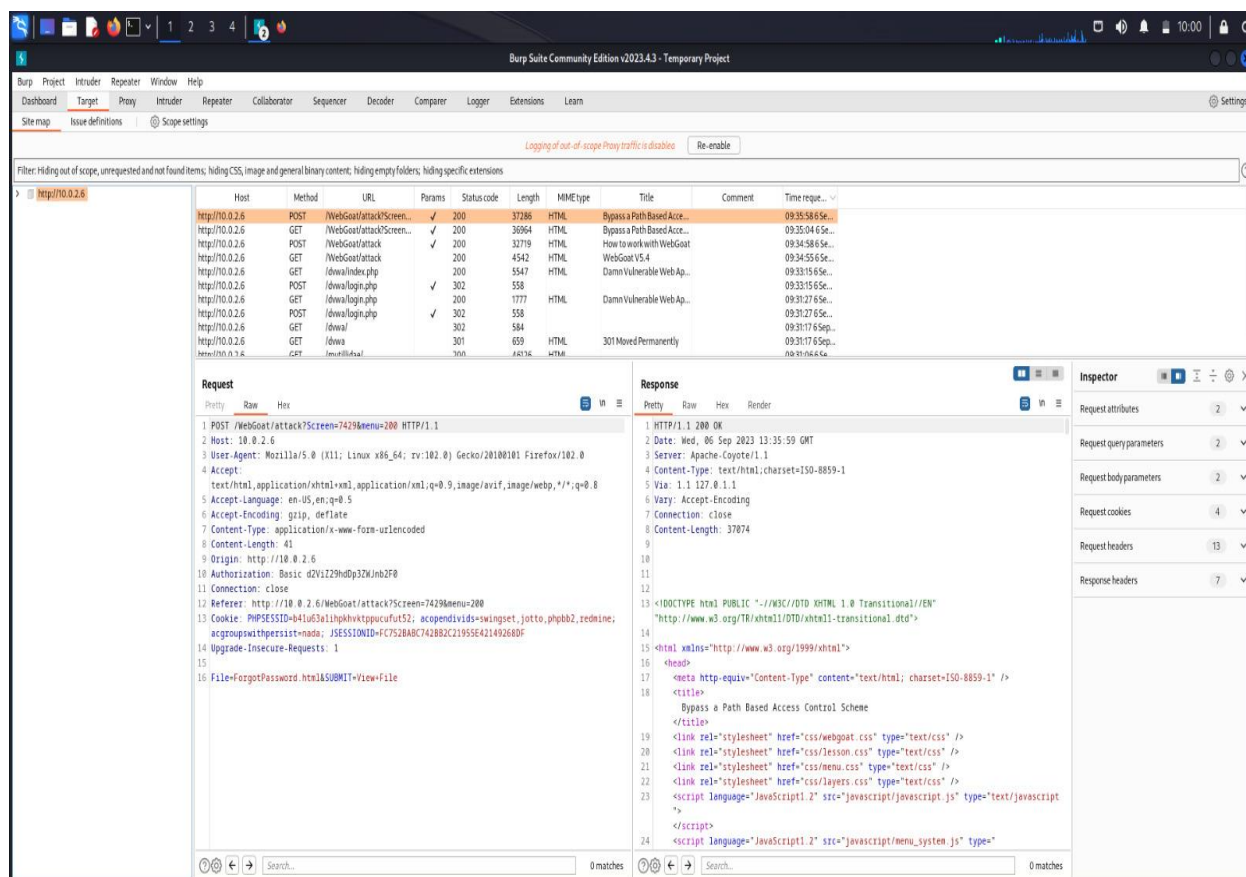

Fig. Victim's requested Information captured into Burp suit

4)Fuzzing by adding Local File name path from Wordlist:

- Type the different-different file names into a Notepad file.
- Save it by giving some name <filename>.txt extension.
- Then goto Intruder panel > Payloads, their load the content of the wordlist.
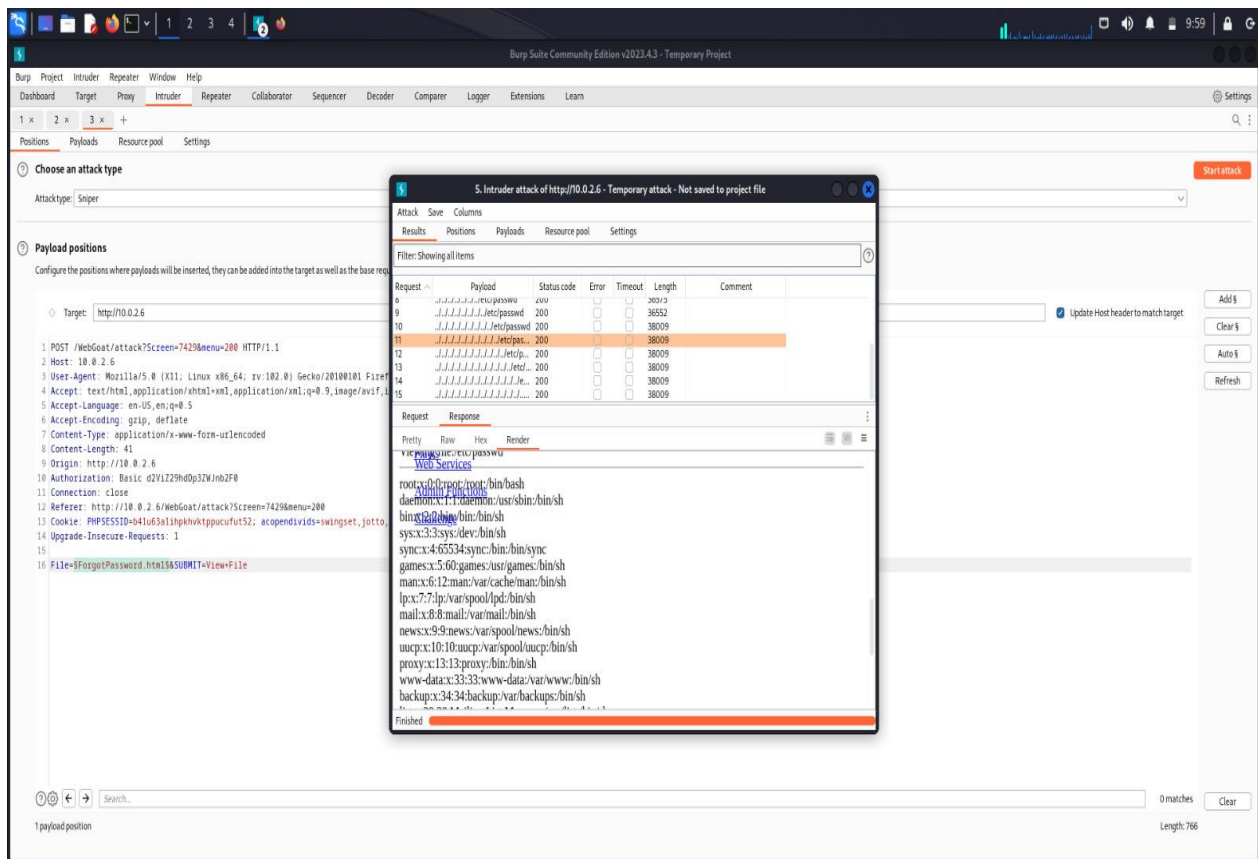- Verify the details once and click on **Start attack.**

Fig. Final result after the successful attack