

Cyber security and Digital Forensics

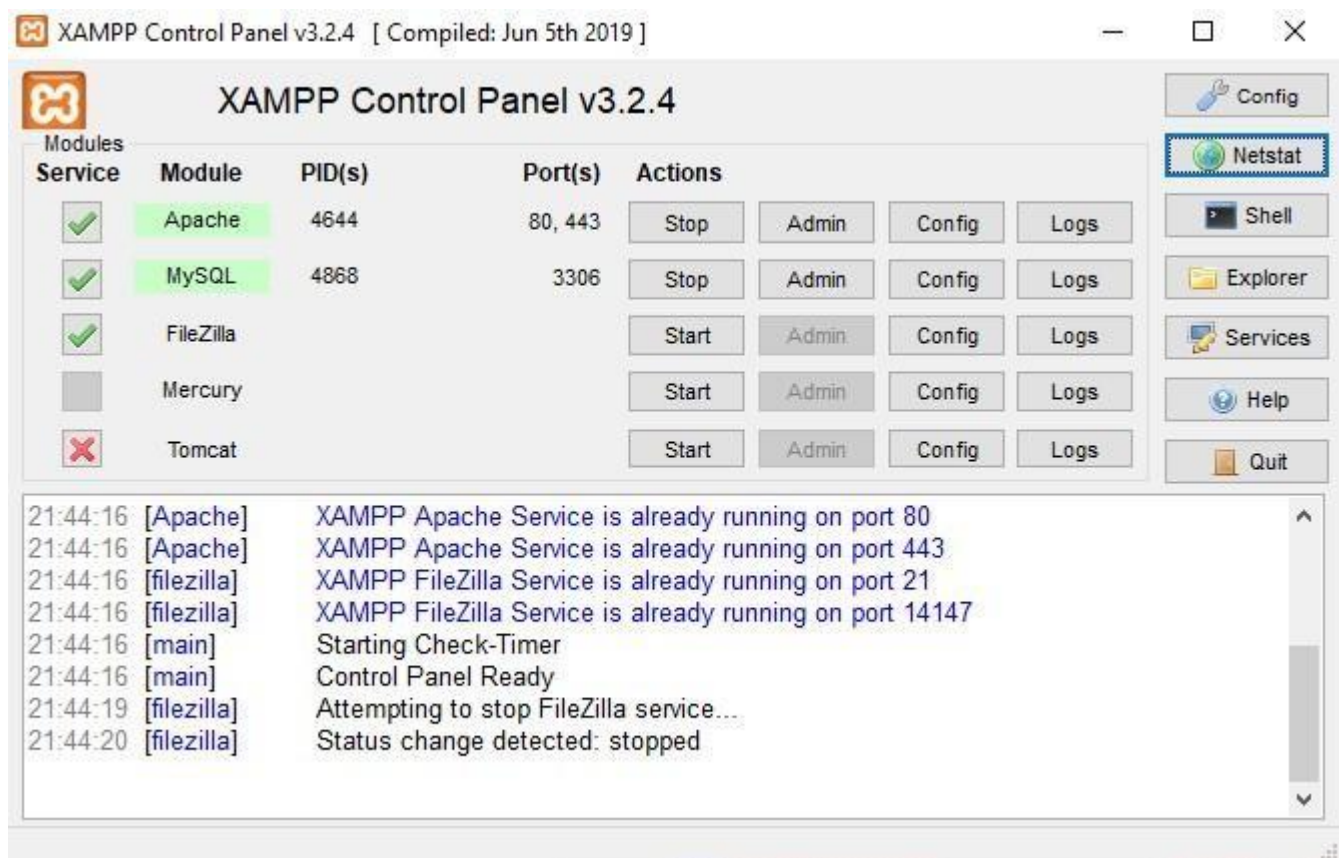
Practical 8: Security Misconfiguration

Tools required for the practical

- Mozilla Firefox Version 38.0.5.
- Burp Suite Community Suite.
- Owasp Mutillidae.

Steps :-

- Run **Xampp** ,make sure **Apache and MySQL** services are running.

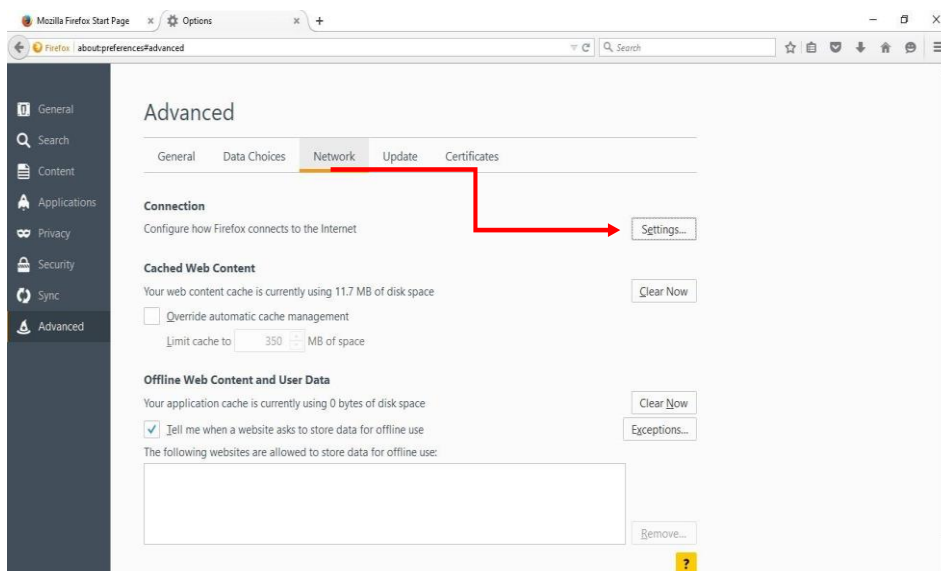


2. Configure Firefox Network setting by assigning a manual proxy ,this will help browser to connect with Burp Suite tool.

a. Open Menu

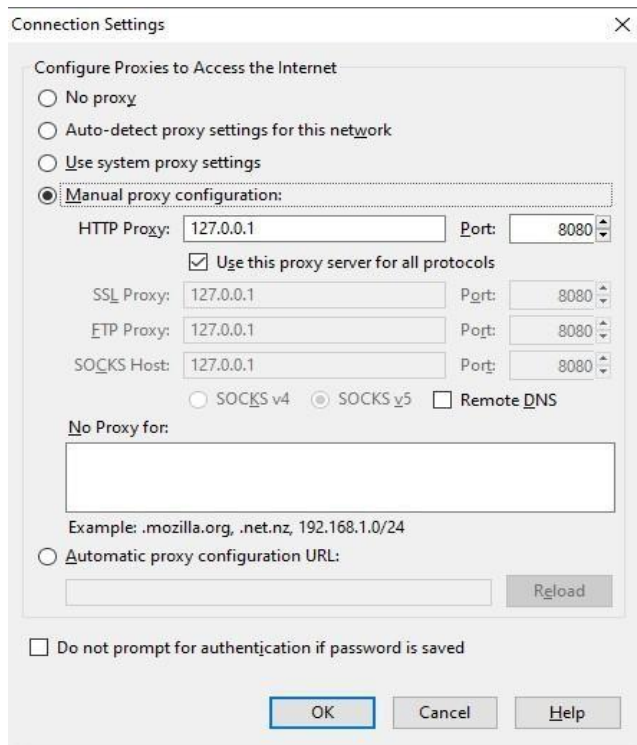


Click on **Options** Under **Advanced** Tab Select Network



C. Open **Settings** besides **Connection**. Connection Setting Dialog will open ,select manual proxy configurations and set **Http proxy as 127.0.0.1** and **Port as 8080** .Check Use this proxy for all protocols.

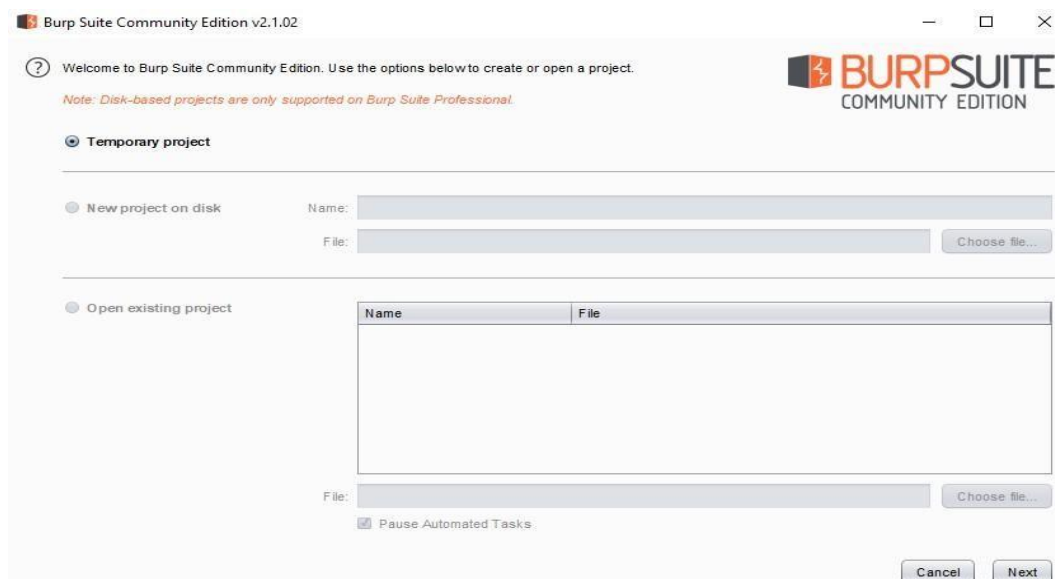
Click ok to exit.



D. The proxy settings have been configured.

3. Open **Burp Suite** tool

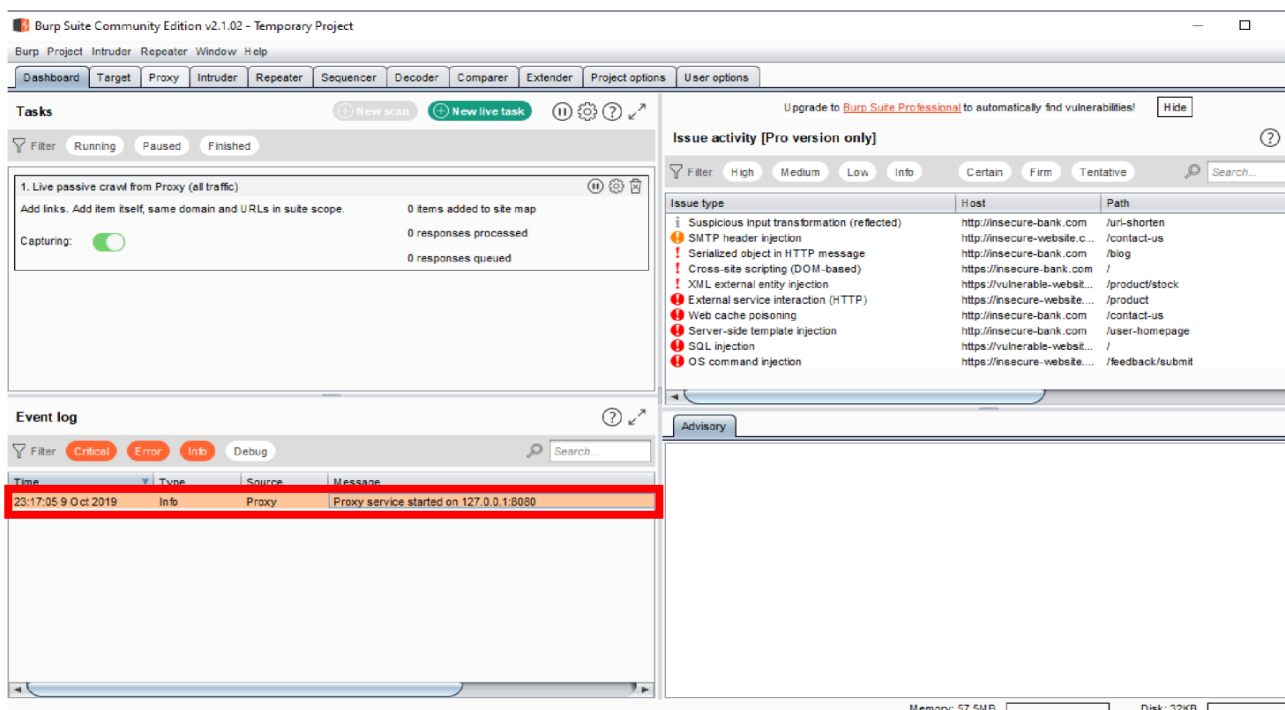
a. The temporary project will be selected by default, click Next



b. In the next Window select Use Burp Default and Start Burp

c. Burp is now running. Check if the **Proxy service** has started correctly on the configured port in under the **Event Log** Tab.

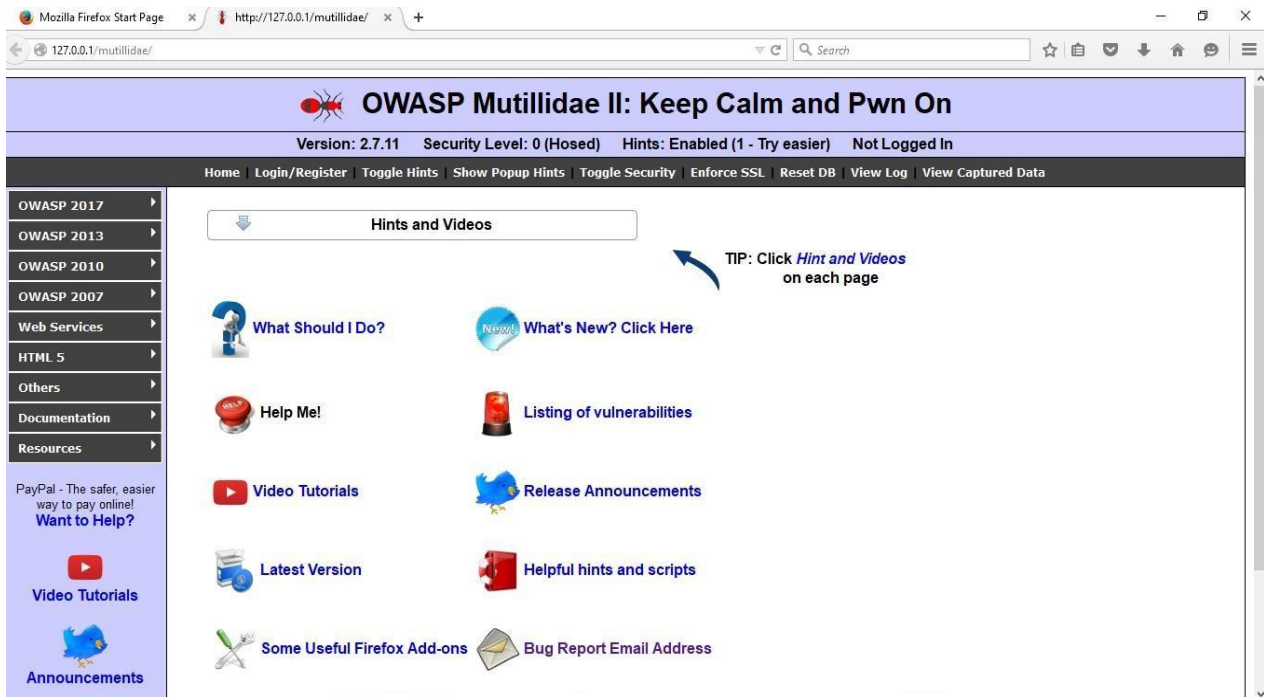
d. Minimize Burp Suite now open Firefox



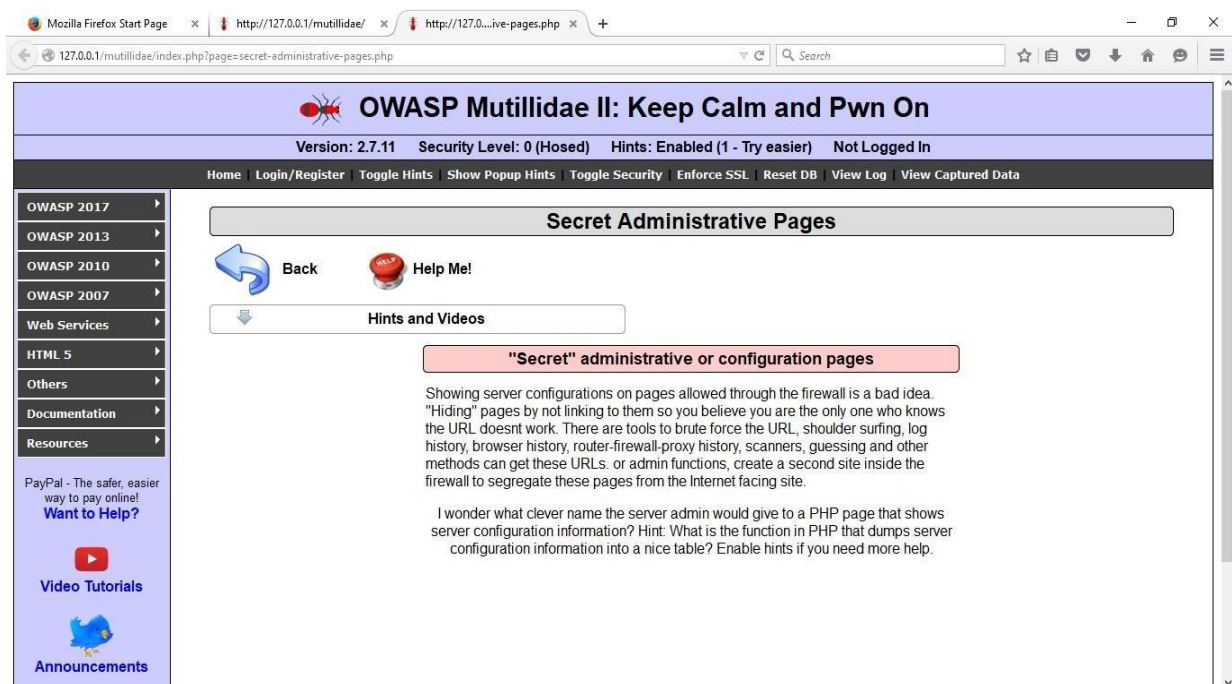
4. Run **OWASP mutillidae** using Xampp on localhost (localhost address <http://127.0.0.1/mutillidae/>).

Browser version should be **Firefox 38.0.5**

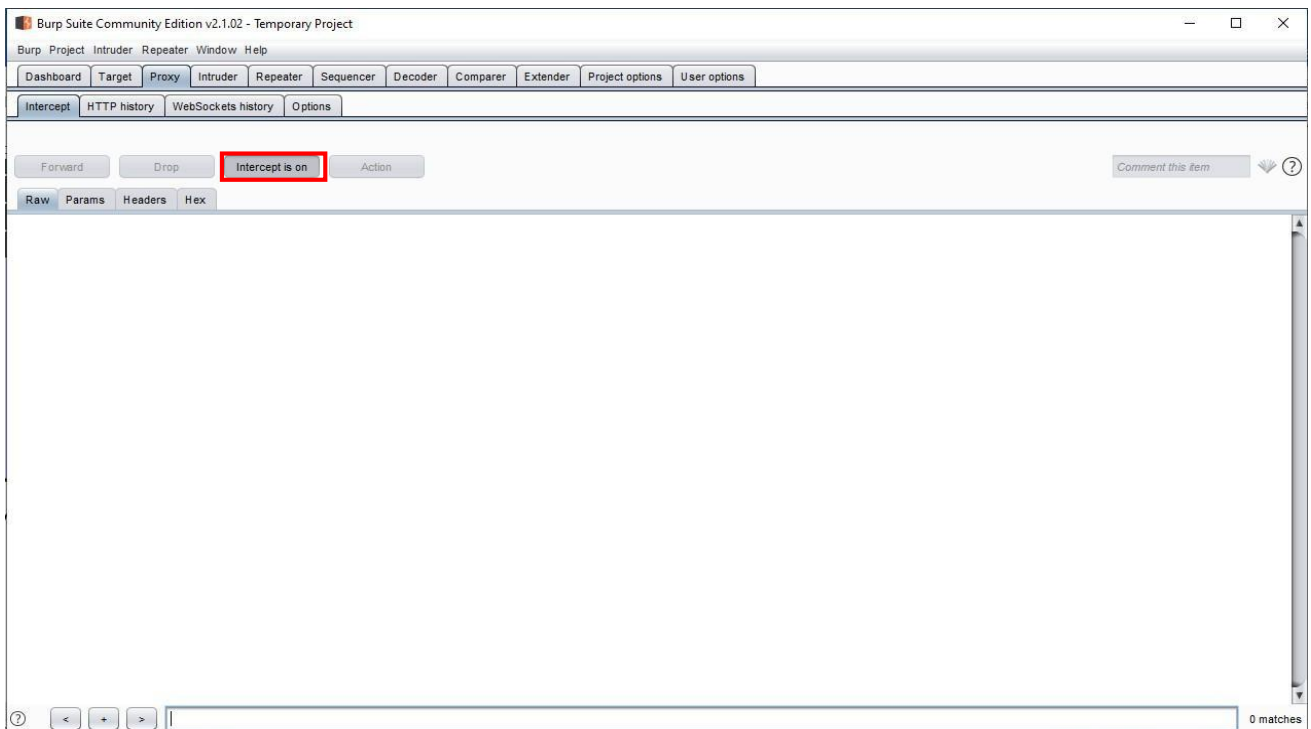
5. In a new tab , Type the following Url (<http://127.0.0.1/mutillidae/index.php?page=secret-administrative-pages.php>) in address bar



6. Minimize Firefox and Open Burp Suite again.

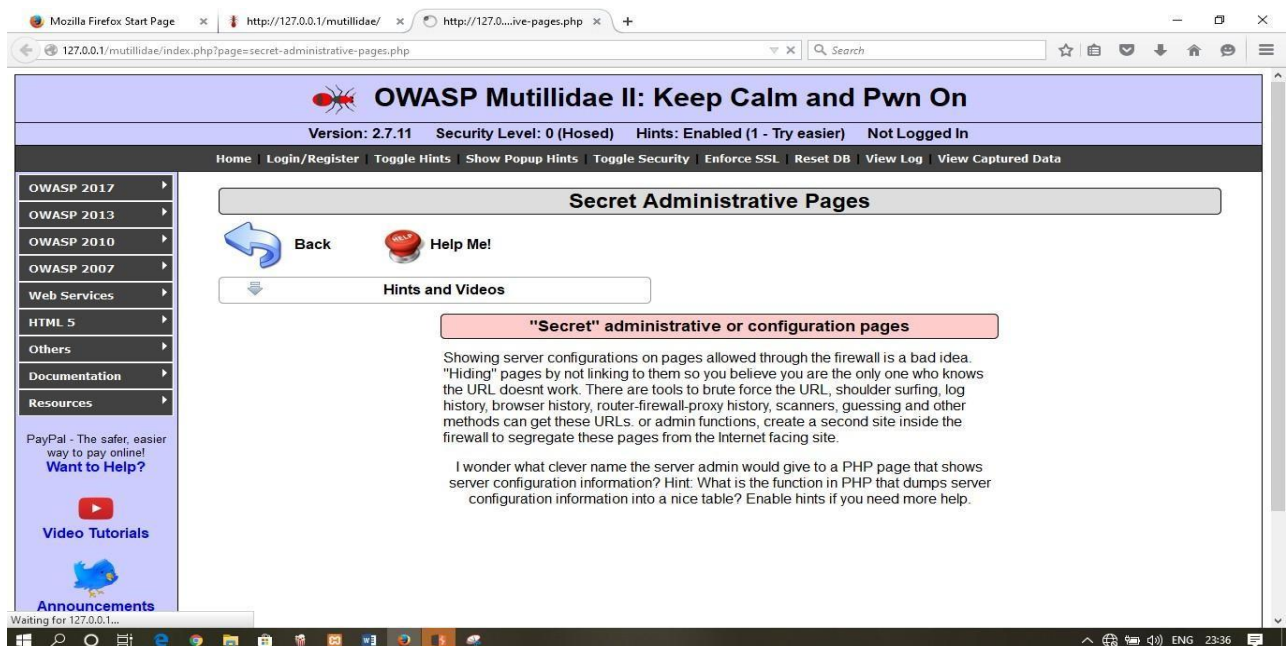


7. Under Proxy tab turn on the intercept if it is off (By turning on the interceptor burp suite will be able to intercept all the requests through the firefox browser)
8. Open Firefox **refresh** the url open in new tab, Burp suite will intercept it and will

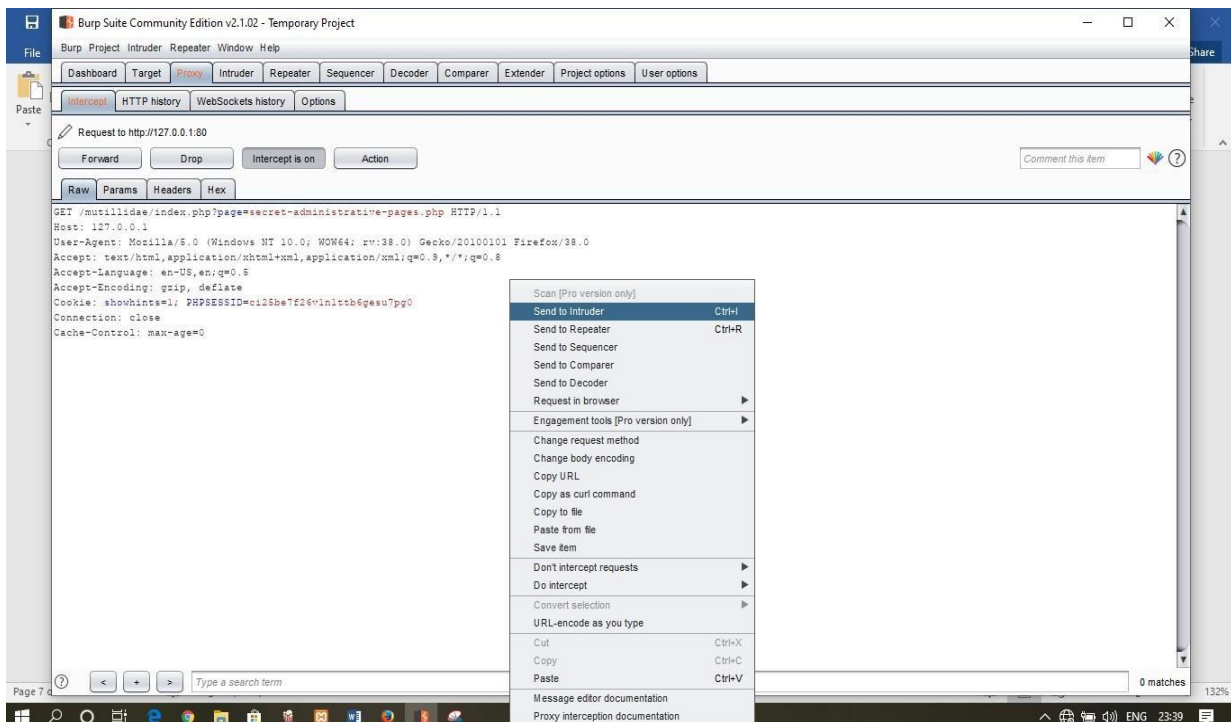
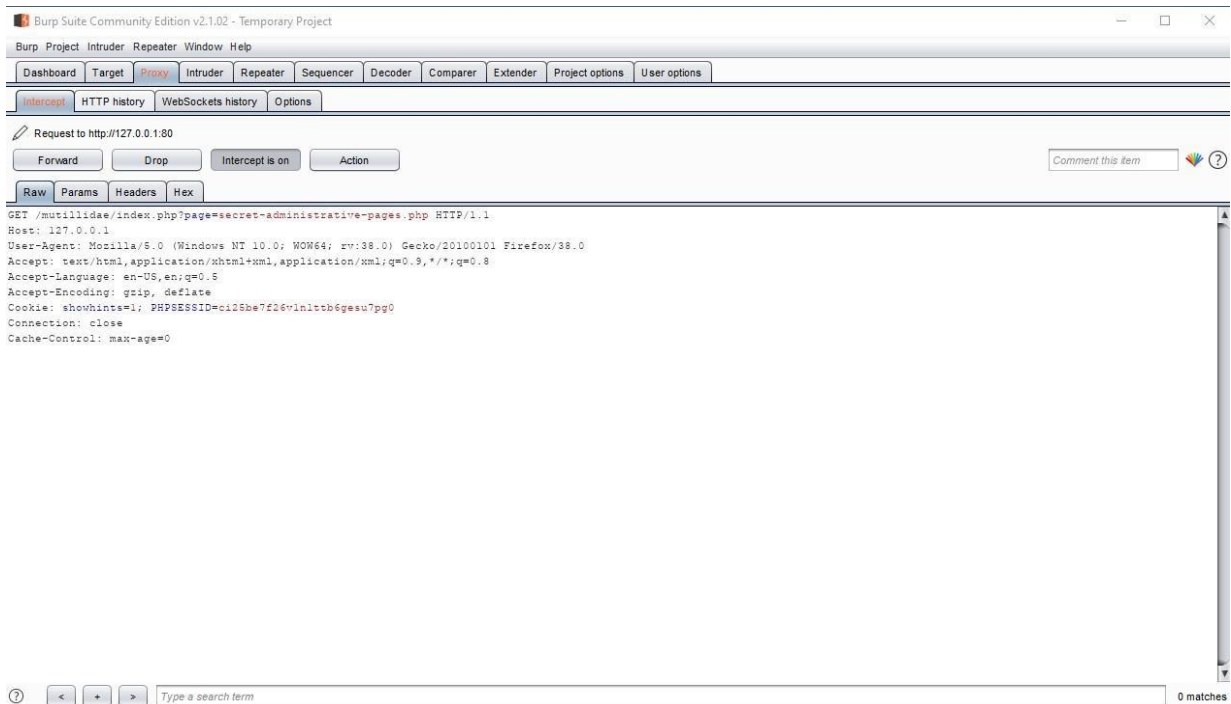


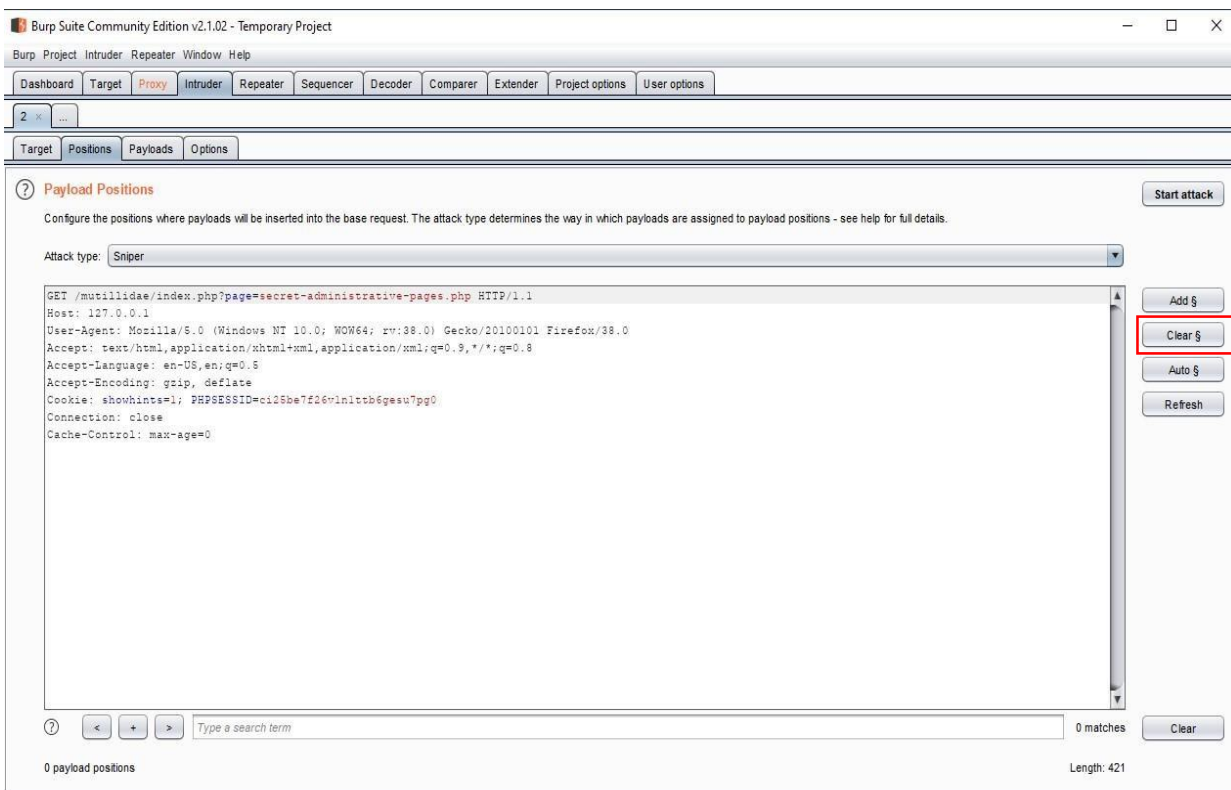
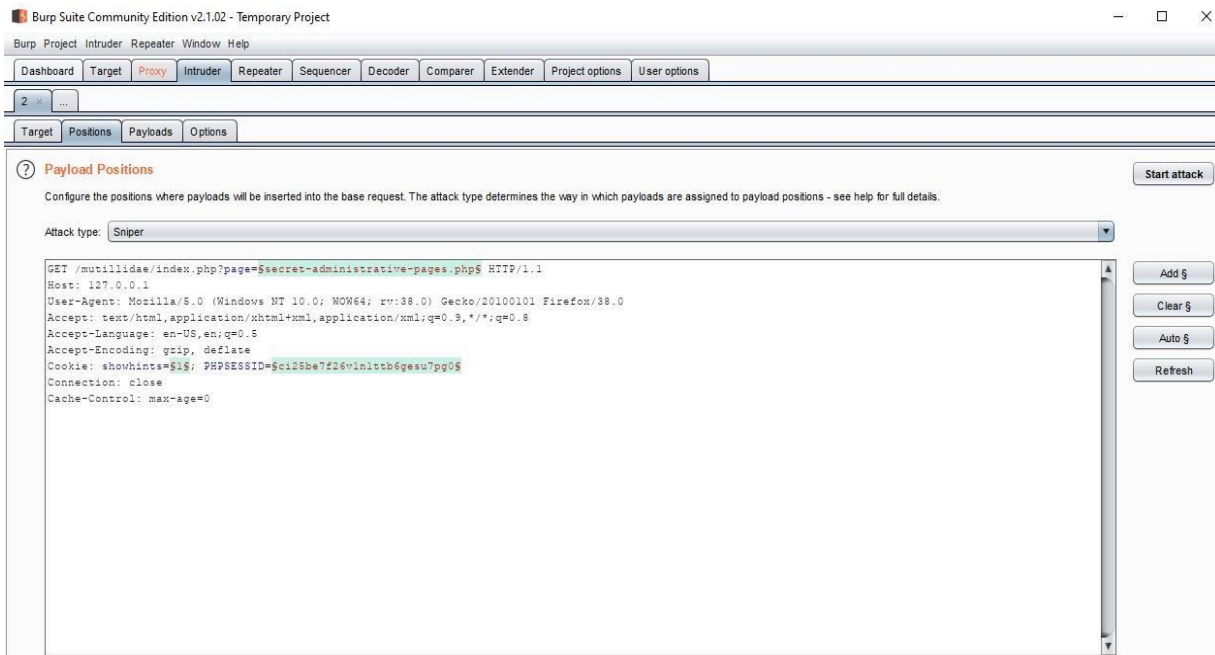
start blinking in the taskbar.

9. This will be the following output in burp Suite

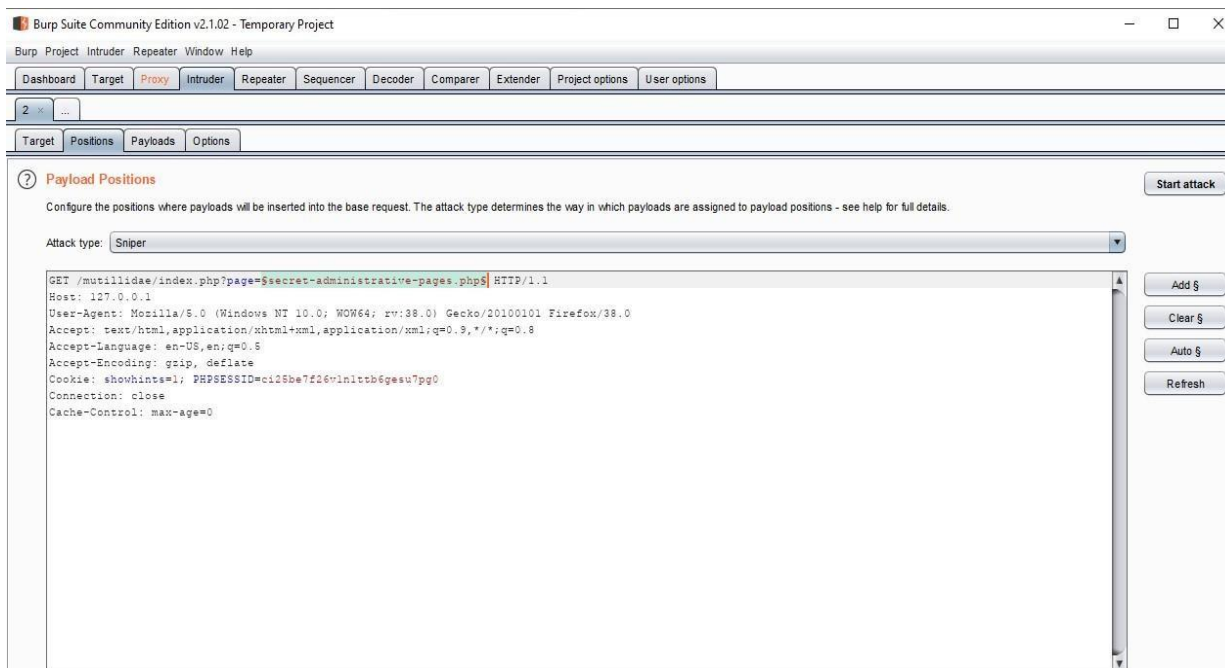
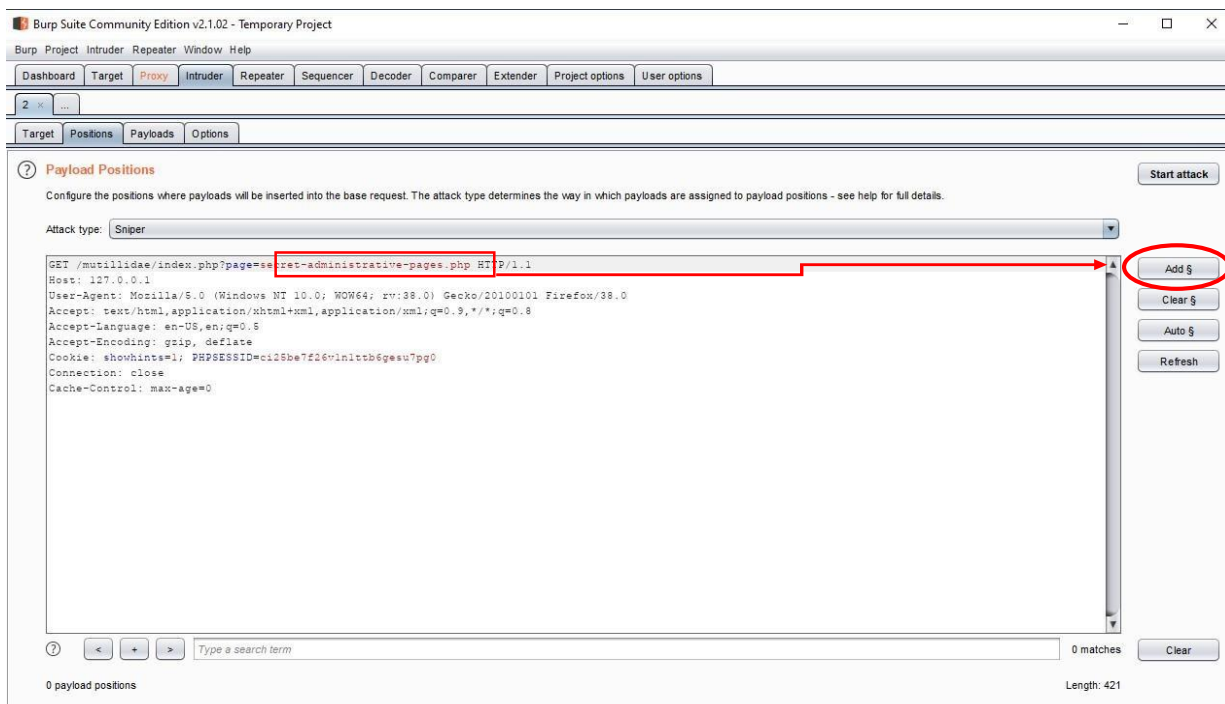


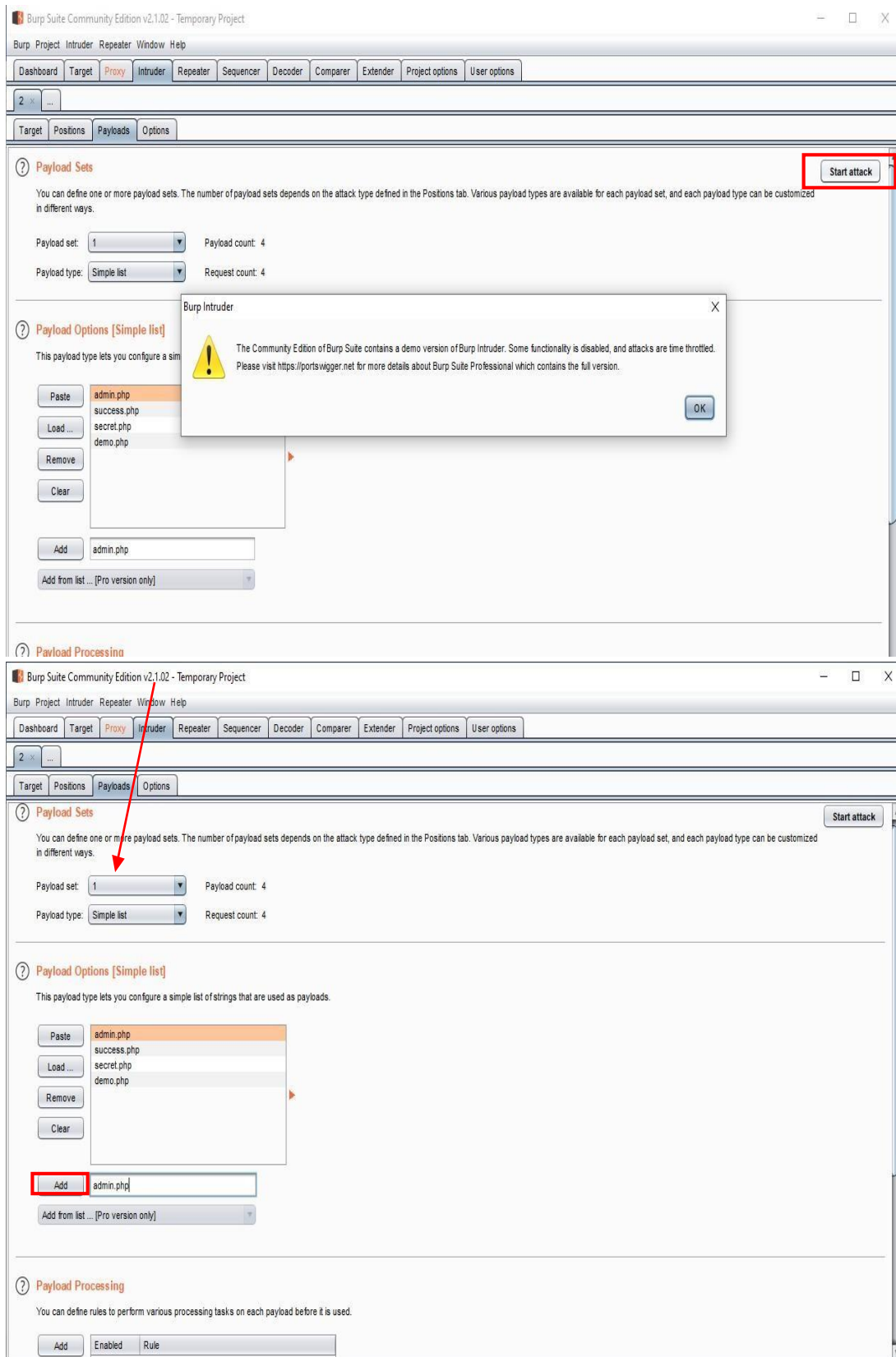
10. Right Click in the window and select Send to intruder.



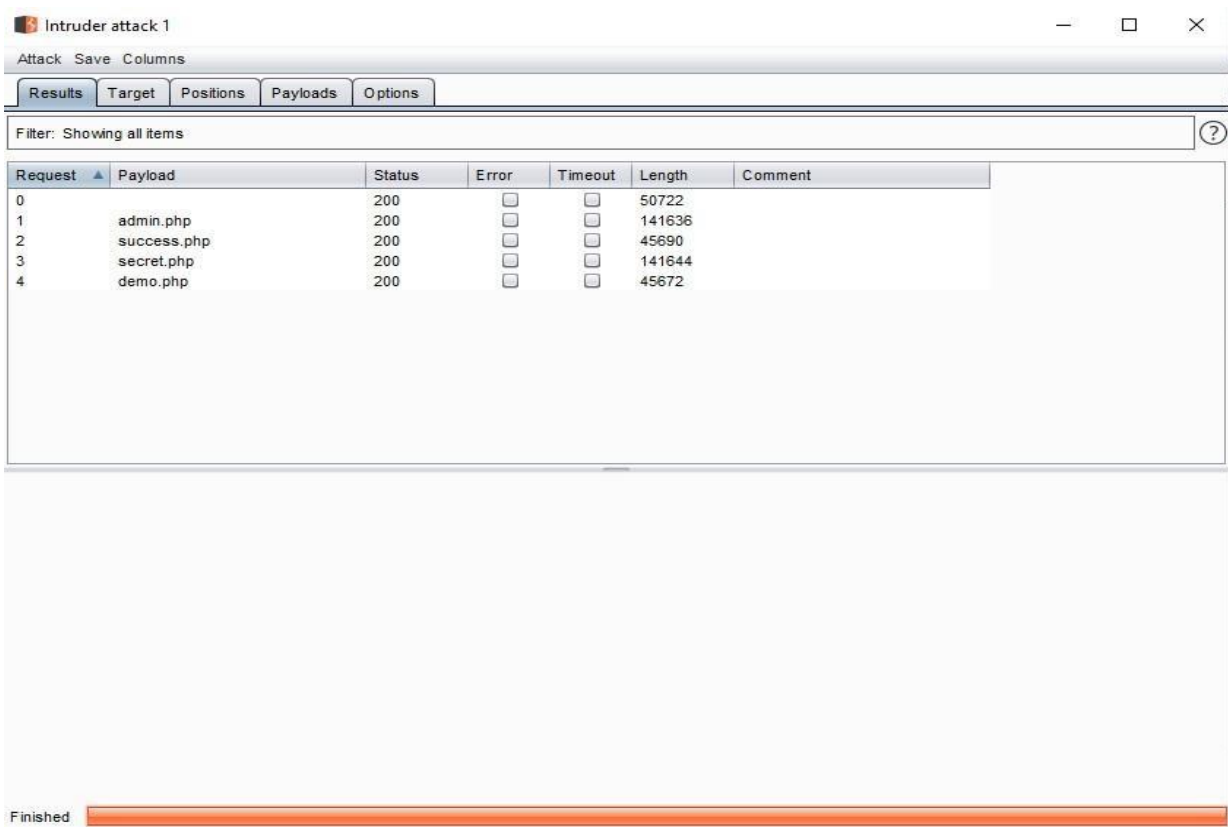
11. Under **Intruder** tab Select **Positions** Click on **Clear** .

12. Select the highlighted path then click Add.

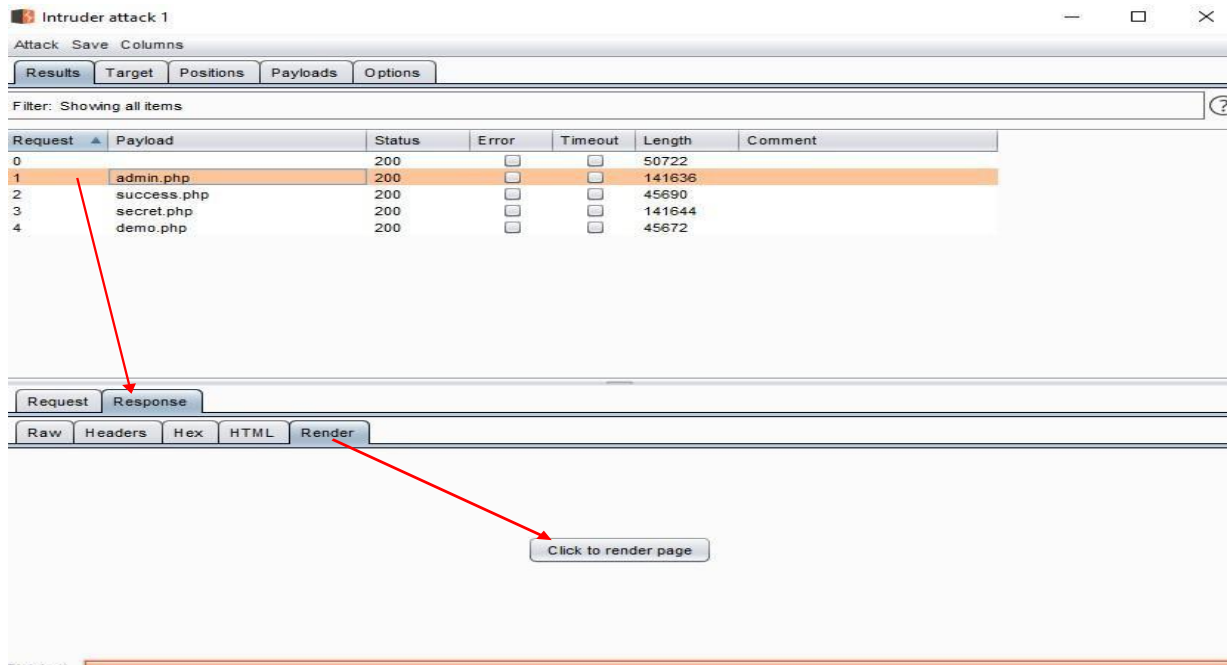




13. Under Payloads ☐ Payload options add 4 Php files(admin.php,success.php,secret.php,demo.php) not necessarily inserted in the same order.
14. Now click on start attack .Warning occurs everytime we carry attack Click OK to continue.
15. After the attack has Finished **Intruder attack** windows will open



16. Render the php to get secret info from the webpage. Select any one of the php files to render.
Under response tab select Render and then click on render.



17. A new window will open displaying the hidden info only known to privileged users on the webpage.

