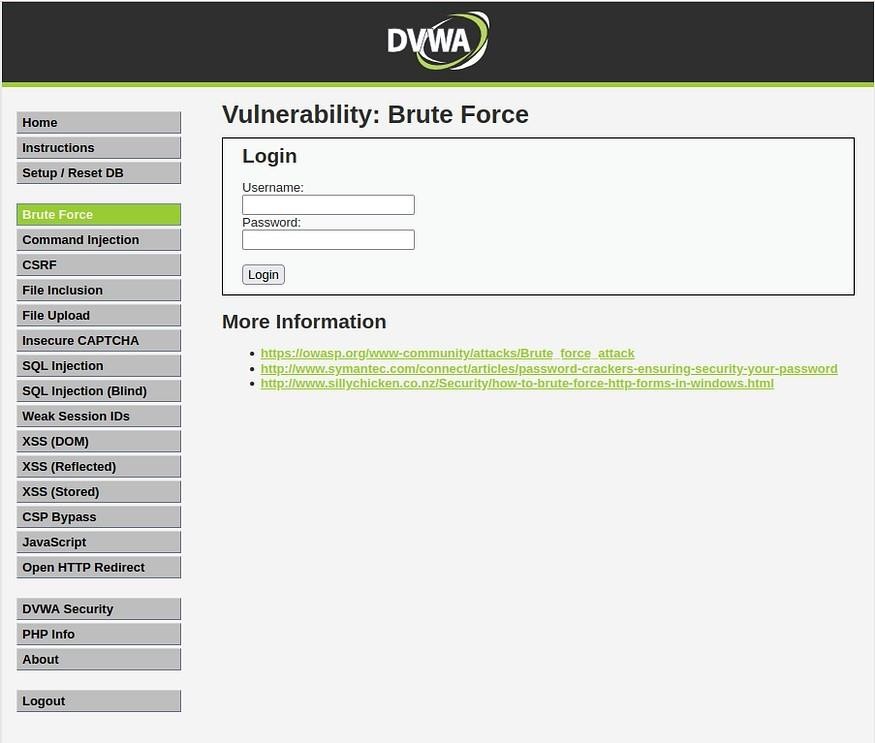
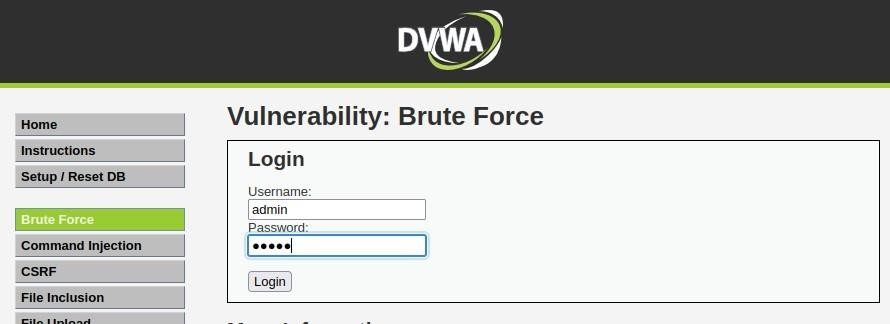
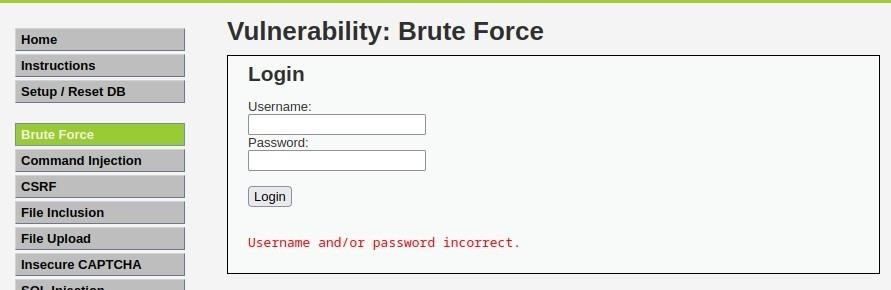
**Experiment-10(Brute Force and Dictionary Attacks-Cyber Security Workshop)**

**Inside DVWA, select the Brute Force option, which takes user to a Login page.**

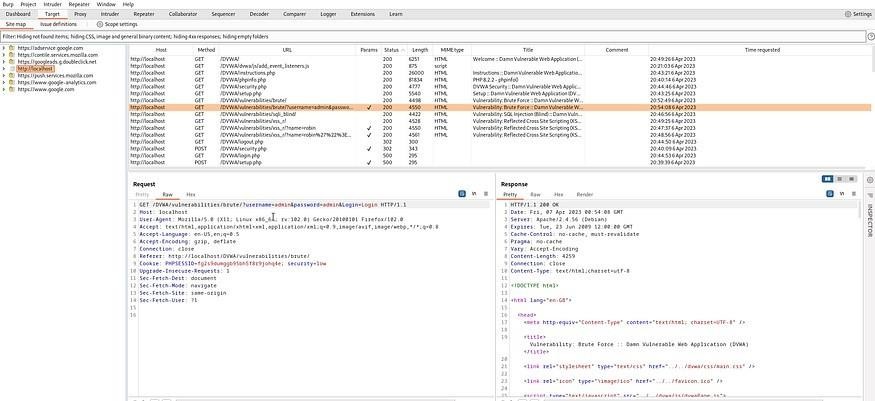
****

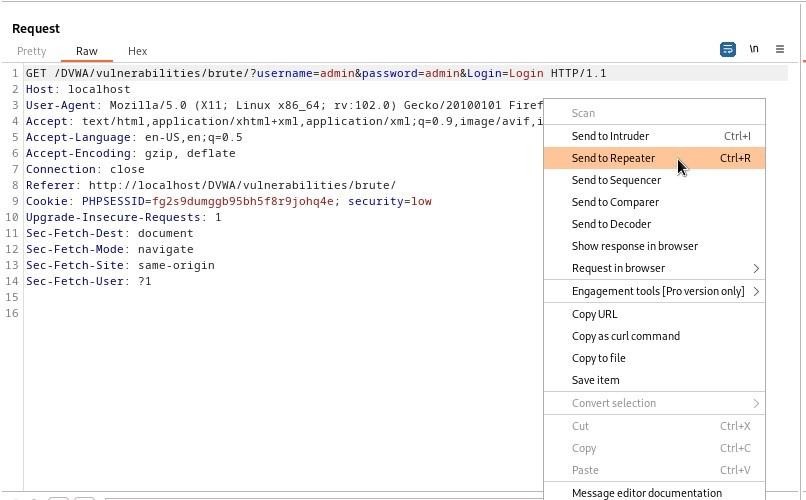
**Enter admin for the username and admin for the password, which is the wrong username and password.**

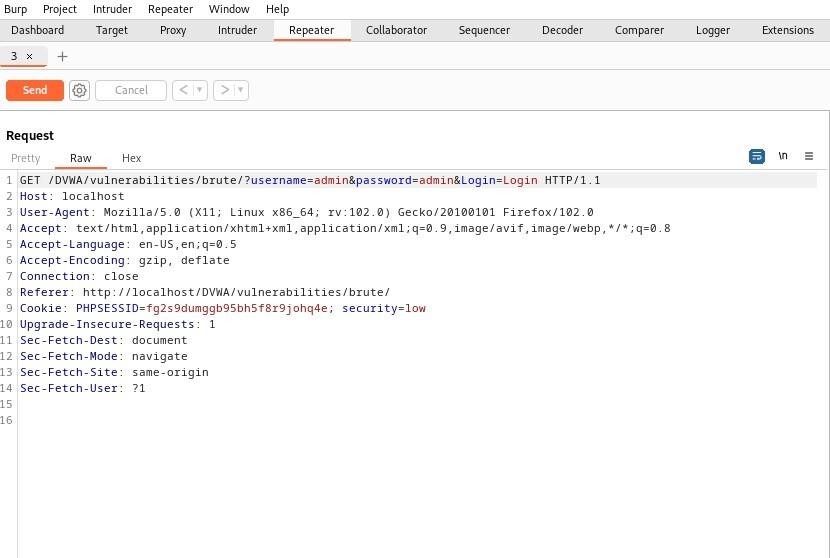
****

****

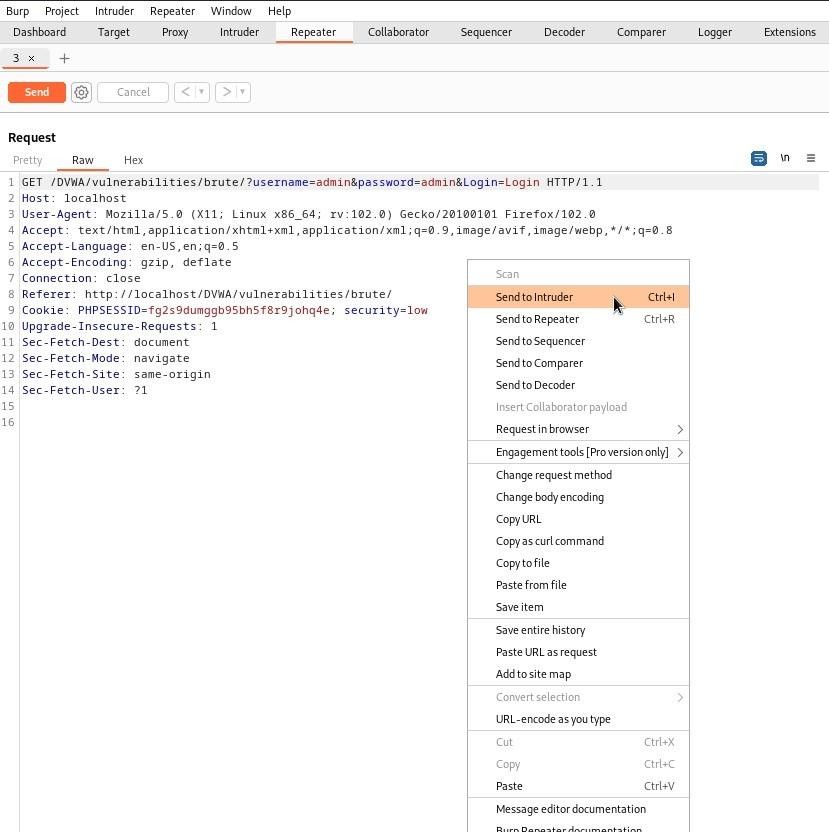
**In the Burp Suite tool, follow the path: Target → Site map →** [**http://localhost**](http://localhost/) **→ URL Containing the following:****/DVWA/vulnerabilities/brute/?username=admin&password=admin&Login=Login HTTP/1.1**

****

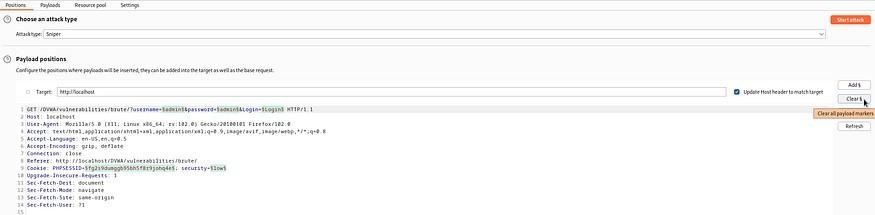
**Navigated to Request → Raw tab → Right-click inside → Send to Repeater.**

**Select the Repeater tab.**

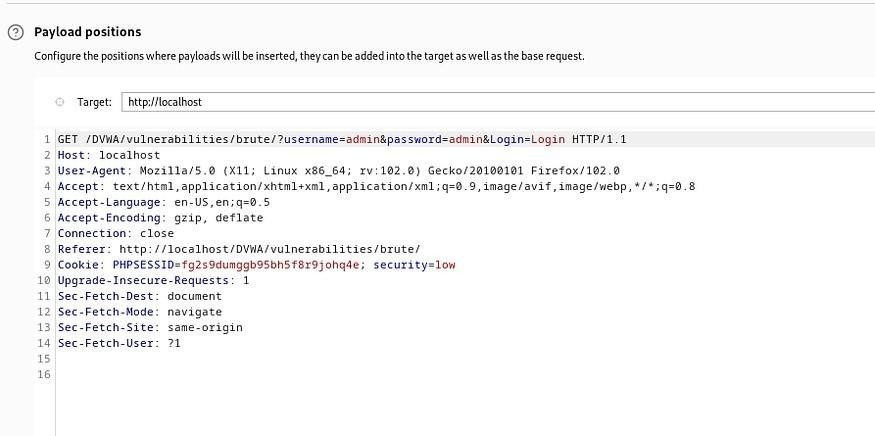
**Right-click inside the Raw data area → Send to Intruder.**

****

**Choose an attack type, Add or Clear payload markers, and Start attack.**

****

**All payload markers cleared.**

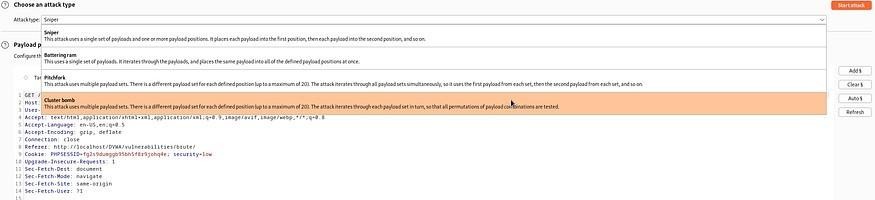
****

**Highlighted admin after username → Selected Add.**

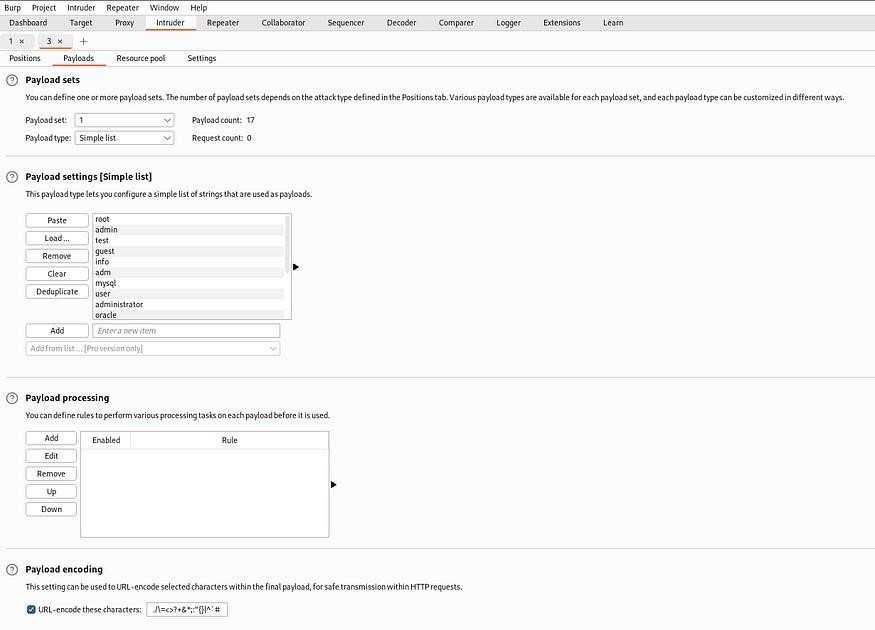
****

**Both username=admin and password=admin are marked as payloads.**

****

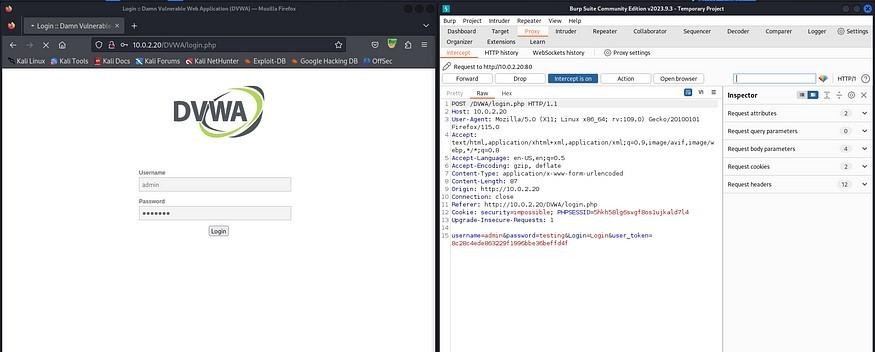
**Choose an attack type → Cluster bomb.**

**Payloads tab to configure and add a list of strings used as payloads.**

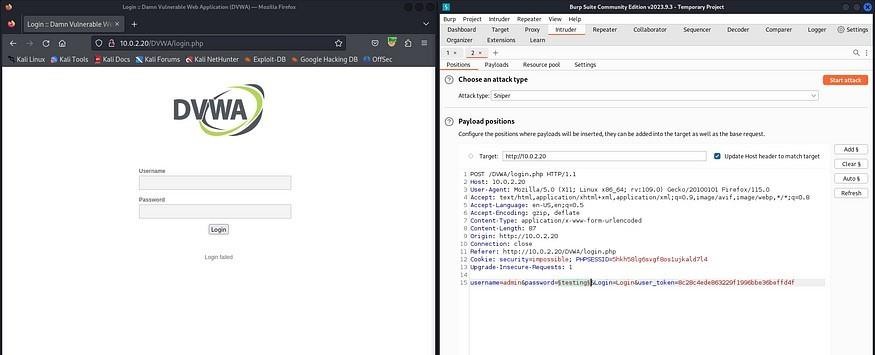
****

****

**Burp Proxy**

****

**Burp Intruder**

****