Task 4

✅ Step 1: Update and Upgrade Your Linux Machine

Before installing DVWA, always update your system to avoid broken or missing packages.
Run the following commands:

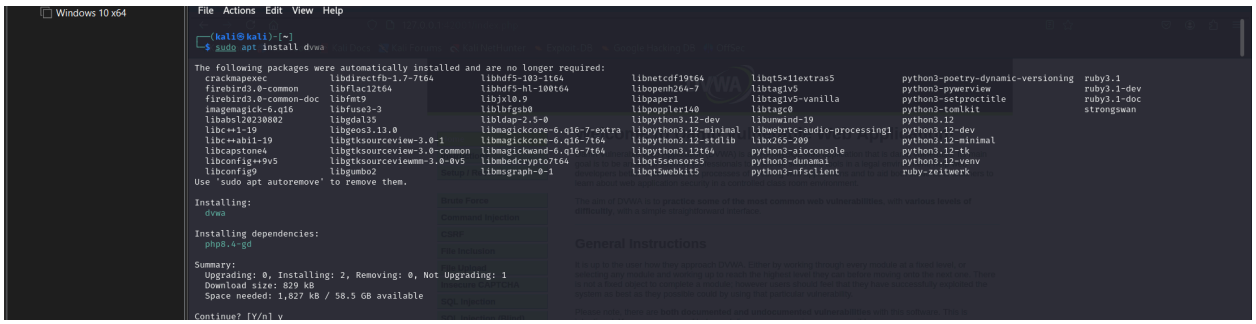
—--> sudo apt-get update

—--> sudo apt-get upgrade

🛠️ Step 2: Install DVWA:

After updating your system, install DVWA using:

—-> sudo apt install dvwa



🚀 Step 3: Start DVWA

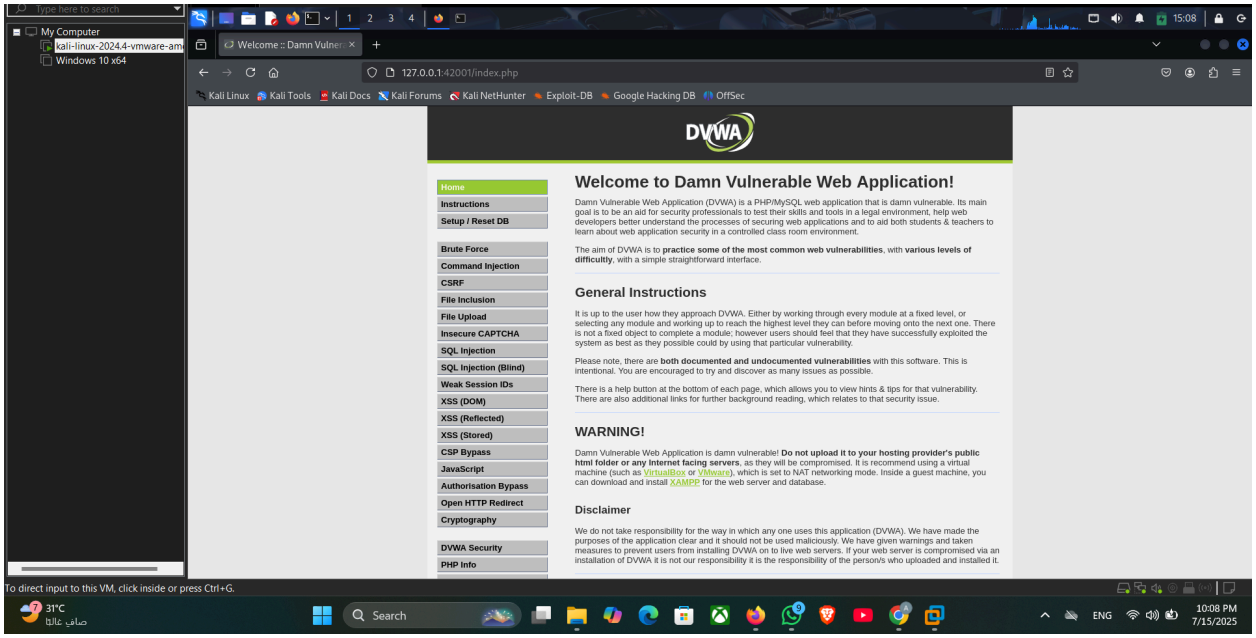
To start the DVWA web service, run the following command:

—--> dvwa-start

🔐 Default Login Credentials

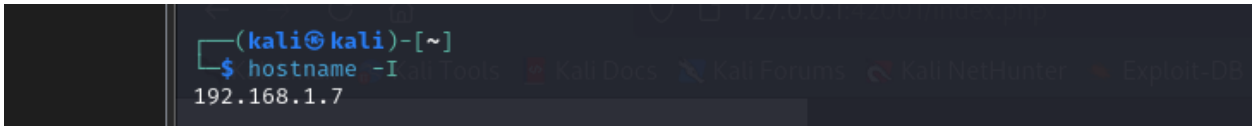
Use the default credentials to log in:

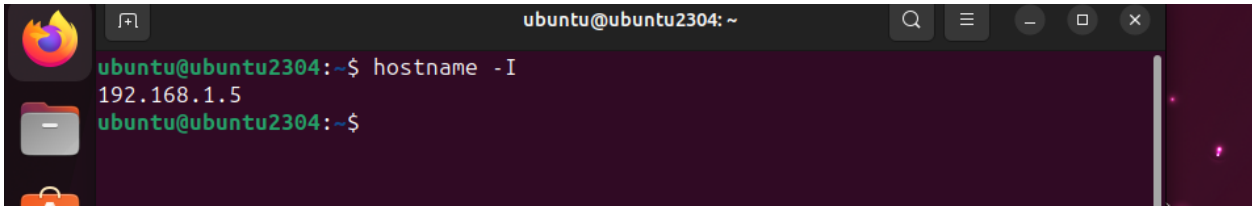
- **Username:** `admin`
- **Password:** `password`



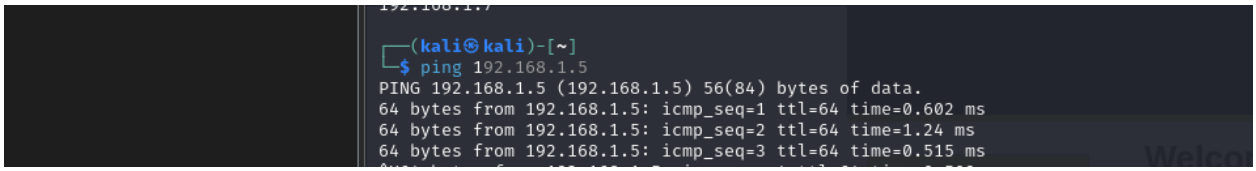
🖥️ 1. Check the IP Address (forwarder)👍

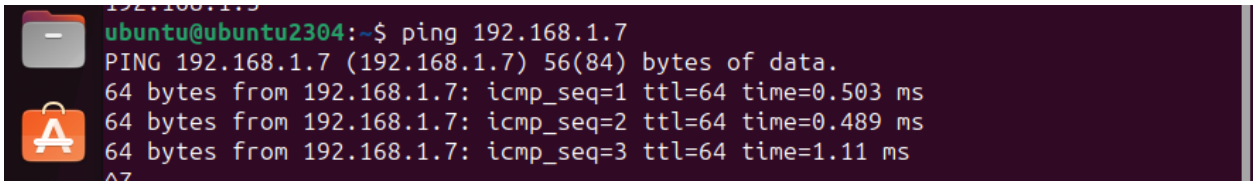
—> hostname -I





📶 **2. Ping to Verify Network Connectivity**

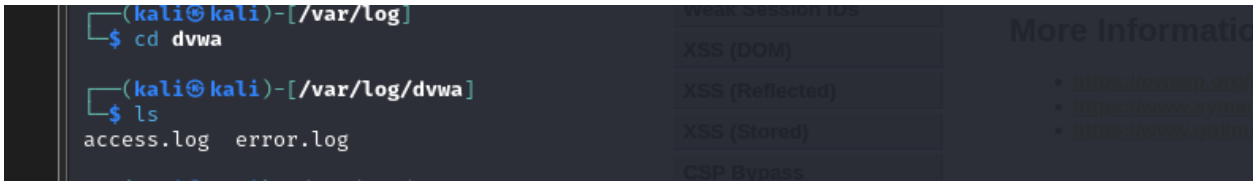




Add DVWA Logs to Splunk Server:

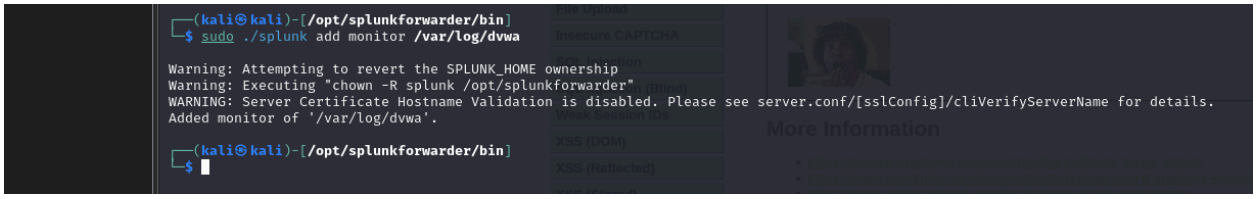
📁 **1. Navigate to the DVWA Log Directory:**

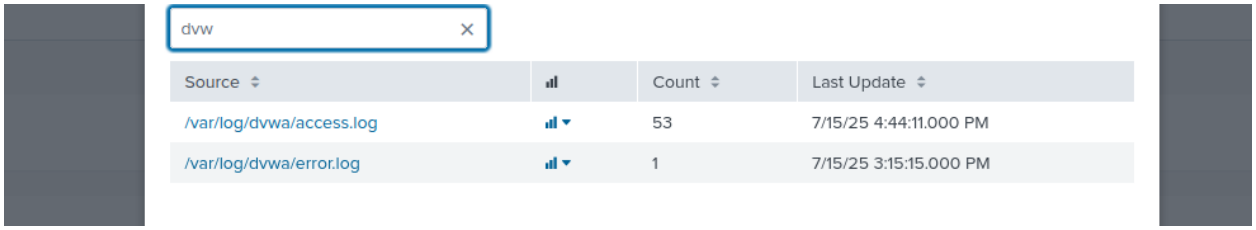
—-> cd /var/log/dvwa



2:Add the Log File to the Splunk:

—->sudo ./splunk add monitor /var/log/dvwa

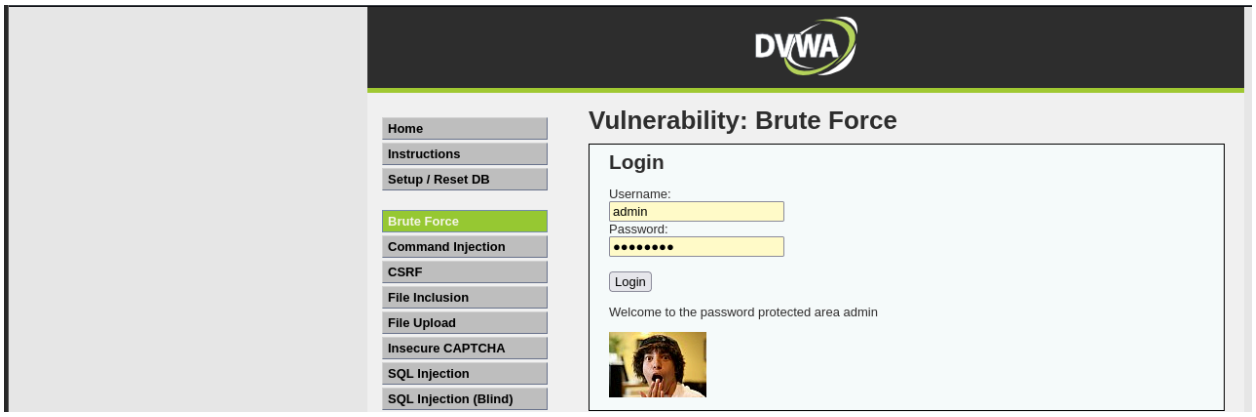




🔐 Simulate Brute-Force Attack Manually in DVWA:

🛠️ Step 1: Set DVWA Security Level to Low.

💣 Step 2: Simulate a Manual Brute Force Attack.



Click Login after each attempt to simulate a manual brute-force.

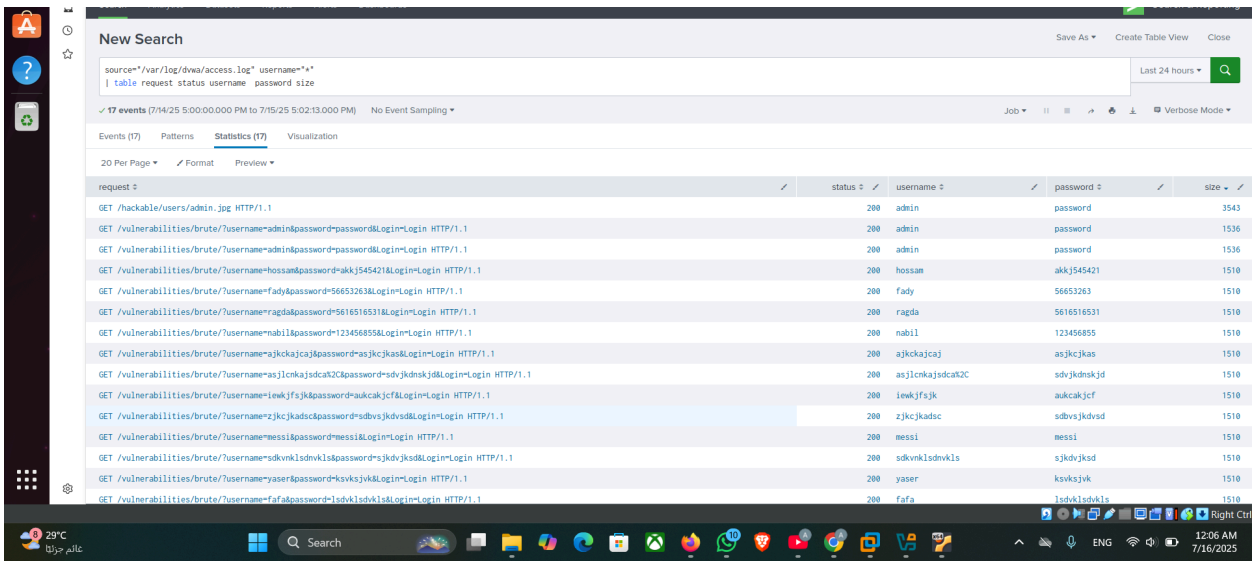
✅ Hint: You will eventually see the message:
"Welcome to the password protected area admin"
which indicates a successful login.

📊 Detect Brute-Force Attacks via Splunk Dashboard

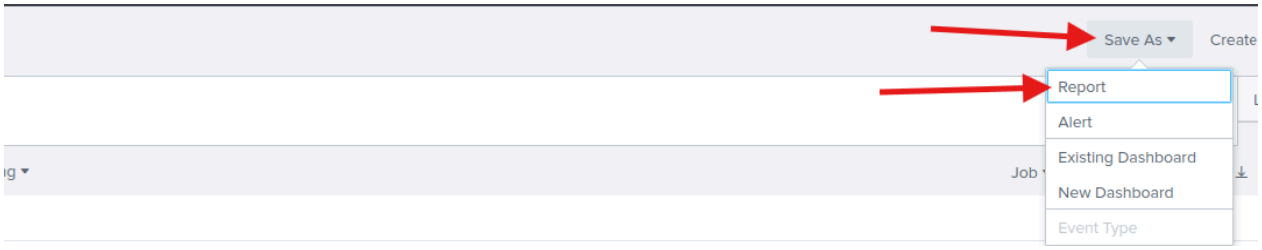
📁 Step 2: Search DVWA Access Logs:

Use the following Search Processing Language (SPL) to analyze login attempts:

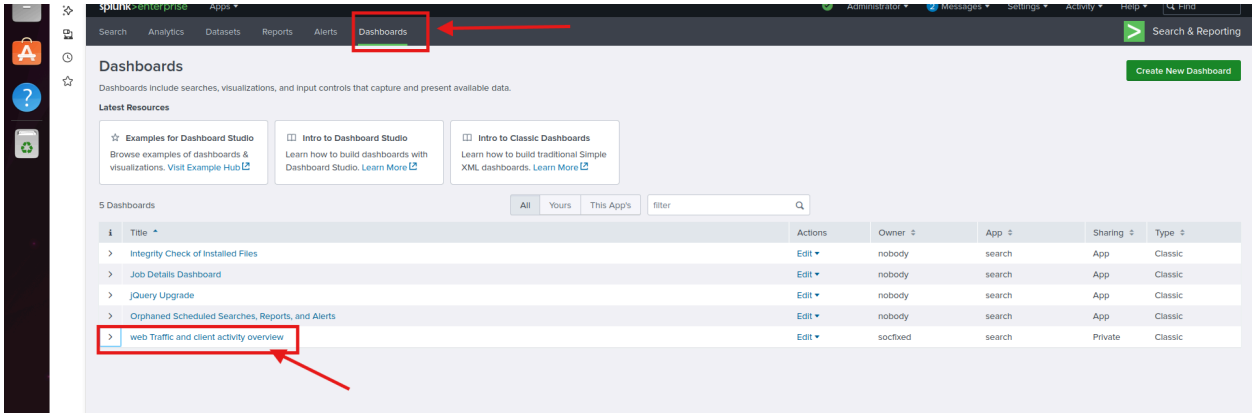
```
source="/var/log/dvwa/access.log" username="*"

| table request status username password size
```



📝 Step 3: Save the Query as a Report



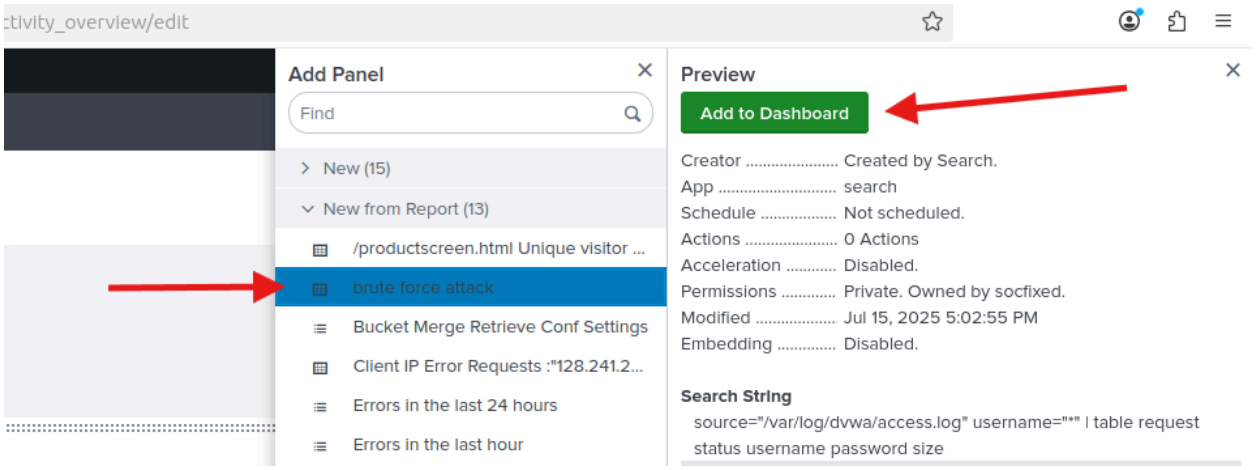
📈 Step 3: Save As Dashboard Panel

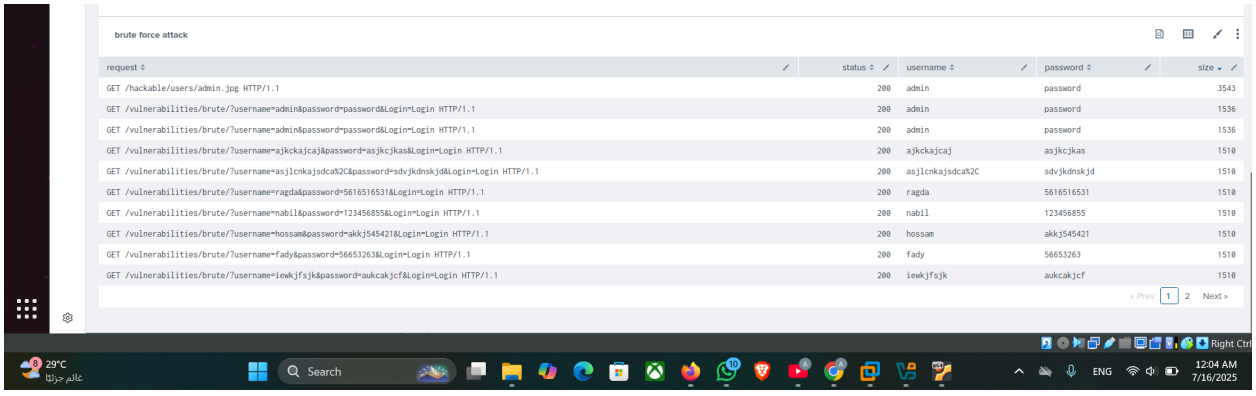


1- click edit

2-add panel

3-choose your report &click add to Dashboard

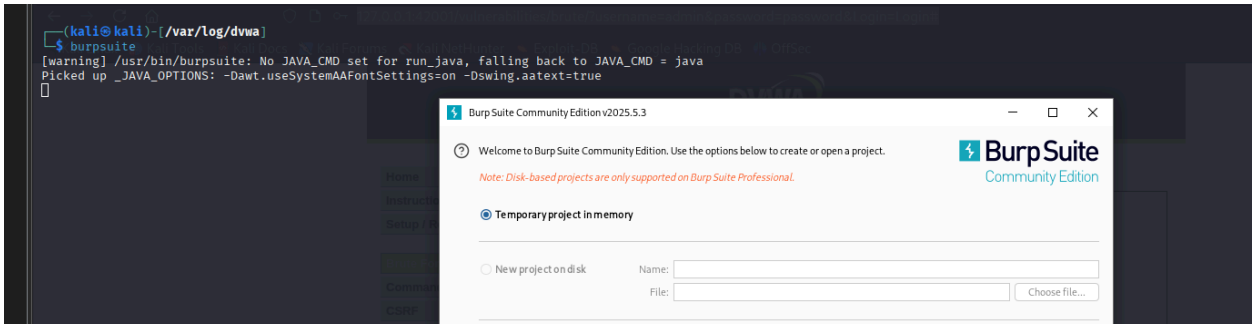




🔐 Simulate Brute Force Attack Using Burp Suite

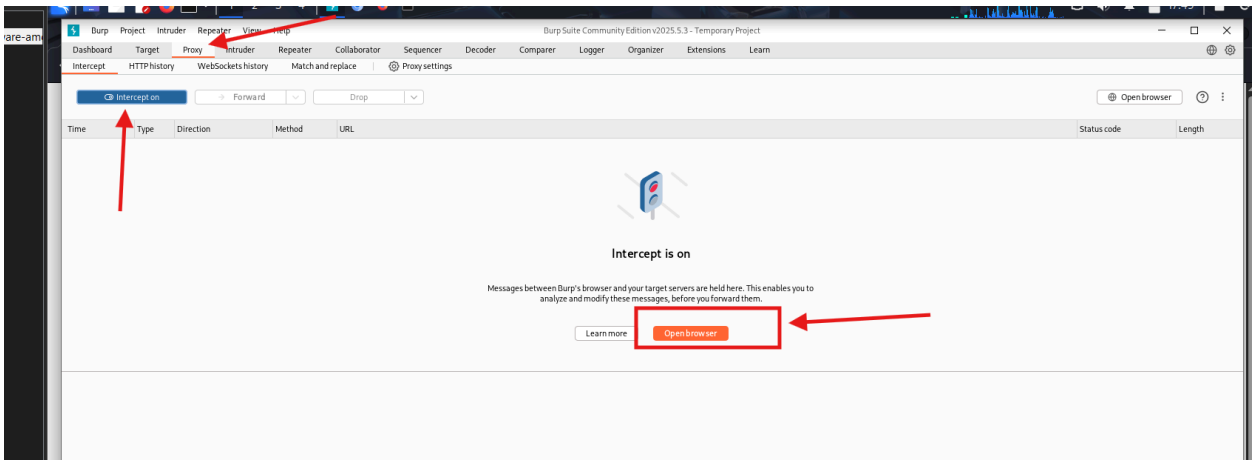
🚀 Launching Burp Suite on Linux:

—--> burpsuite



🧰 2. Open Burp Suite

- **Launch Burp Suite**
- **Go to the Proxy tab**
- **Click "Open Browser" to launch a browser controlled by Burp**



📤 4. Send to Intruder: 1- Right-click the captured request.

2-Select Send to Intruder.

3-Go to the Intruder tab.