

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:

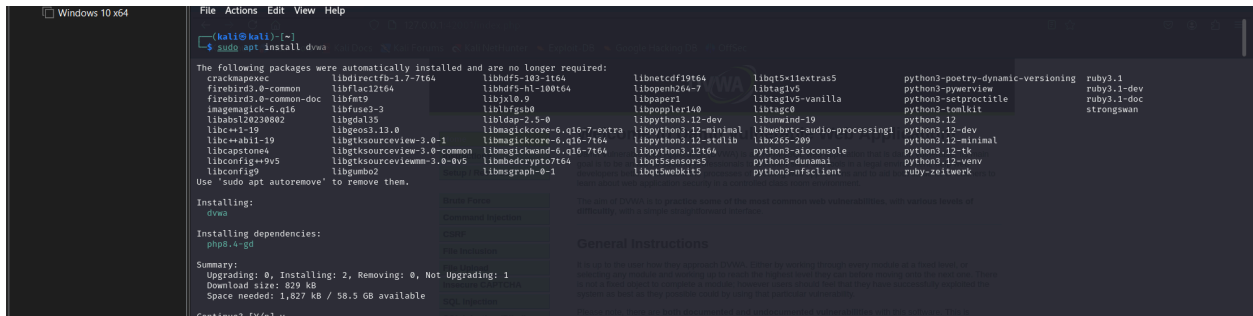
—--> **sudo apt-get update**

---> **sudo apt-get upgrade**

Step 2: Install DVWA:

After updating your system, install DVWA using:

—> **sudo apt install dvwa**



Step 3: Start DVWA

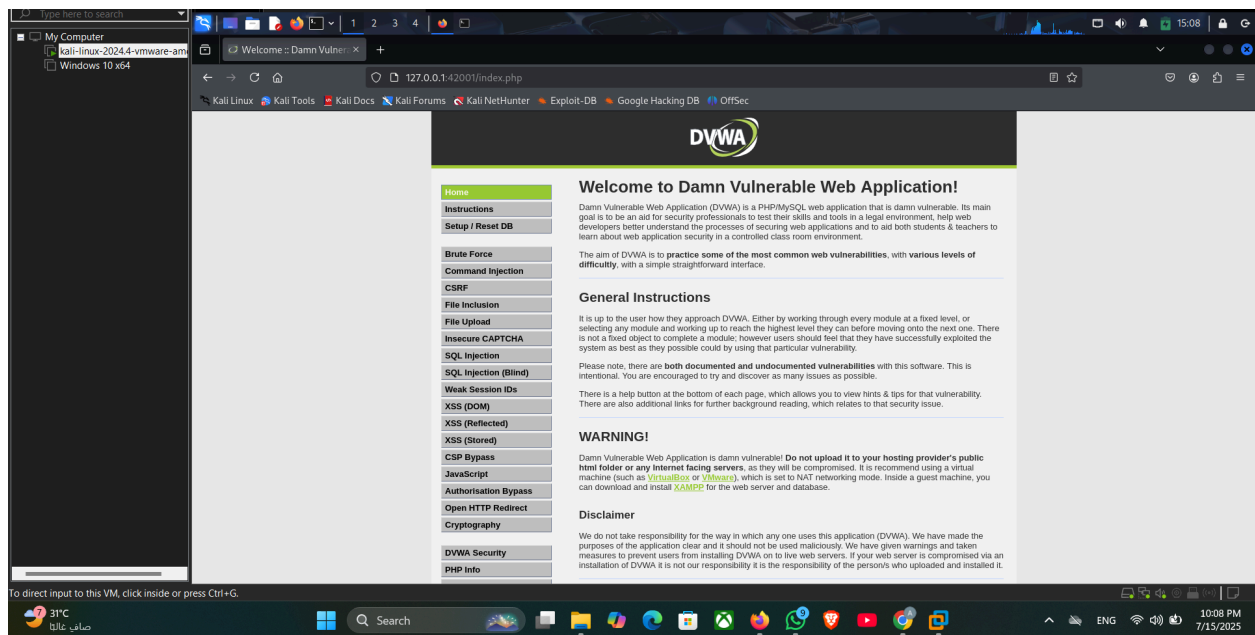
To start the DVWA web service, run the following command:

---> dvwa-start

Default Login Credentials

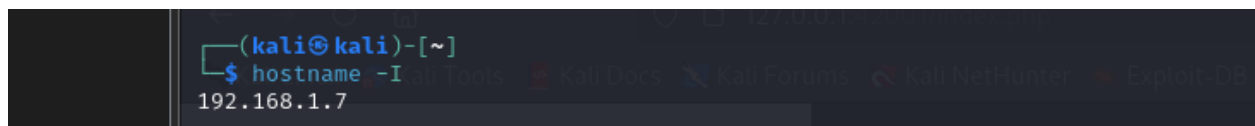
Use the default credentials to log in:

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



1. Check the IP Address (forwarder) 👍

—> **hostname -I**



```
ubuntu@ubuntu2304: ~  
ubuntu@ubuntu2304:~$ hostname -I  
192.168.1.5  
ubuntu@ubuntu2304:~$
```

2. Ping to Verify Network Connectivity

```
(kali㉿kali)-[~]  
$ ping 192.168.1.5  
PING 192.168.1.5 (192.168.1.5) 56(84) bytes of data.  
64 bytes from 192.168.1.5: icmp_seq=1 ttl=64 time=0.602 ms  
64 bytes from 192.168.1.5: icmp_seq=2 ttl=64 time=1.24 ms  
64 bytes from 192.168.1.5: icmp_seq=3 ttl=64 time=0.515 ms
```

```
ubuntu@ubuntu2304:~$ ping 192.168.1.7  
PING 192.168.1.7 (192.168.1.7) 56(84) bytes of data.  
64 bytes from 192.168.1.7: icmp_seq=1 ttl=64 time=0.503 ms  
64 bytes from 192.168.1.7: icmp_seq=2 ttl=64 time=0.489 ms  
64 bytes from 192.168.1.7: icmp_seq=3 ttl=64 time=1.11 ms
```

Add DVWA Logs to Splunk Server:

1. Navigate to the DVWA Log Directory:

—> **cd /var/log/dvwa**

```
(kali㉿kali)-[/var/log]  
$ cd dvwa  
(kali㉿kali)-[/var/log/dvwa]  
$ ls  
access.log  error.log
```

2: Add the Log File to the Splunk:

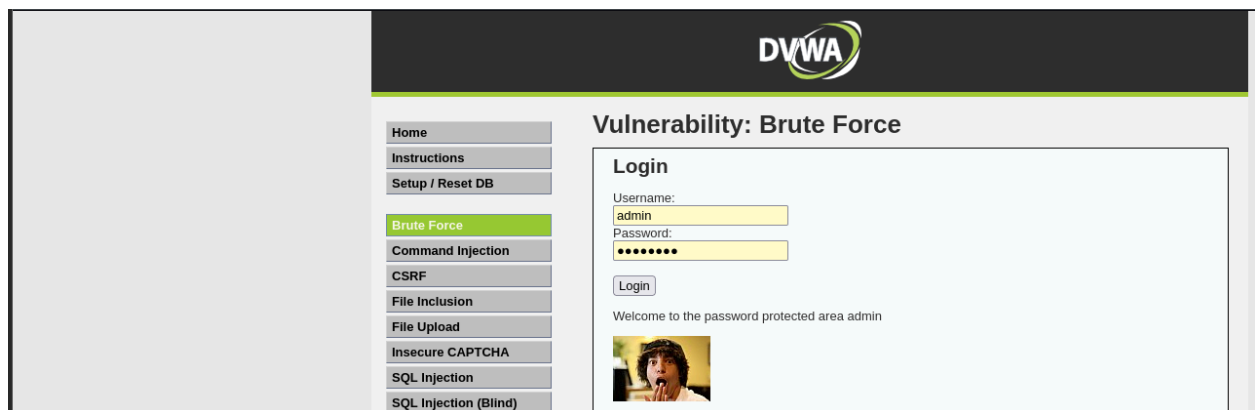
—> **sudo ./splunk add monitor /var/log/dvwa**

```
(kali@kali)-[/opt/splunkforwarder/bin]
$ sudo ./splunk add monitor /var/log/dvwa
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunk /opt/splunkforwarder"
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Added monitor of '/var/log/dvwa'.
```


<div>dvw</div>			
Source		Count	Last Update
/var/log/dvwa/access.log		53	7/15/25 4:44:11.000 PM
/var/log/dvwa/error.log		1	7/15/25 3:15:15.000 PM

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.

Us

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

```
| table request status username password size
```

New Search

Save As ▾ Create Table View Close

```
source"/var/log/dmwa/access.log" username=""*  
| table request status username password size
```

Last 24 hours 🔍

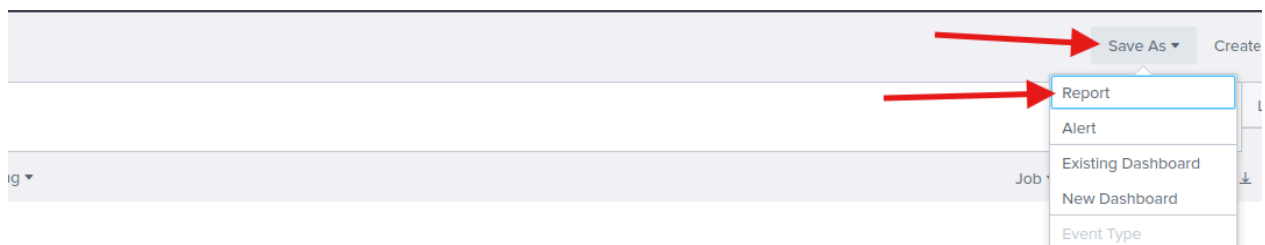
✓ 17 events (7/14/25 5:00:00.000 PM to 7/15/25 5:02:13.000 PM) No Event Sampling ▼

Job ▾ || ▮ ▯ ▸ ▹ ► Verbose Mode ▴

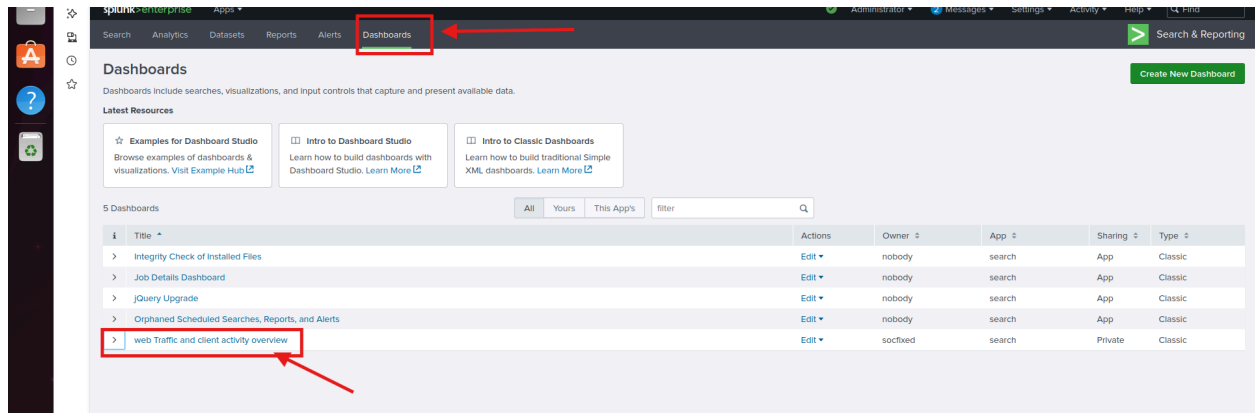
Events (17) Patterns **Statistics (17)** Visualization

20 Per Page ▾ Format Preview ▾

request ↕	status ↕	username ↕	password ↕	size ↕
GET /hackable/users/admin.jpg HTTP/1.1	200	admin	password	3543
GET /vulnerabilities/brute/?username=admin&password=password&login= HTTP/1.1	200	admin	password	1536
GET /vulnerabilities/brute/?username=admin&password=password&login= HTTP/1.1	200	admin	password	1536
GET /vulnerabilities/brute/?username=hossam&password=akkJ54542l&login= HTTP/1.1	200	hossam	akkJ54542l	1510
GET /vulnerabilities/brute/?username=fady&password=56653263&l&login= HTTP/1.1	200	fady	56653263	1510
GET /vulnerabilities/brute/?username=ragda&password=561651653l&login= HTTP/1.1	200	ragda	561651653l	1510
GET /vulnerabilities/brute/?username=nabil&password=123456855&l&login= HTTP/1.1	200	nabil	123456855	1510
GET /vulnerabilities/brute/?username=ajkcakajcaj&password=asjkckas&l&login= HTTP/1.1	200	ajkcakajcaj	asjkckas	1510
GET /vulnerabilities/brute/?username=asjlcnkajsdca2c&password=sdvkjksd&l&login= HTTP/1.1	200	asjlcnkajsdca2c	sdvjksd	1510
GET /vulnerabilities/brute/?username=lewkjfjsjk&password=aucakcjcf&l&login= HTTP/1.1	200	lewkjfjsjk	aucakcjcf	1510
GET /vulnerabilities/brute/?username=zjkjdsc&password=sdbvsjkdv&l&login= HTTP/1.1	200	zjkjdsc	sdbvsjkdv	1510
GET /vulnerabilities/brute/?username=messi&password=messil&login= HTTP/1.1	200	messi	messi	1510
GET /vulnerabilities/brute/?username=sdvknlsdv&l&password=sdkvdksd&l&login= HTTP/1.1	200	sdvknlsdv	sdkvdksd	1510
GET /vulnerabilities/brute/?username=yaser&password=kvsksj&l&login= HTTP/1.1	200	yaser	kvsksj	1510
GET /vulnerabilities/brute/?username=fafad&password=sdvklsdk&l&login= HTTP/1.1	200	fafa	sdvklsdk	1510



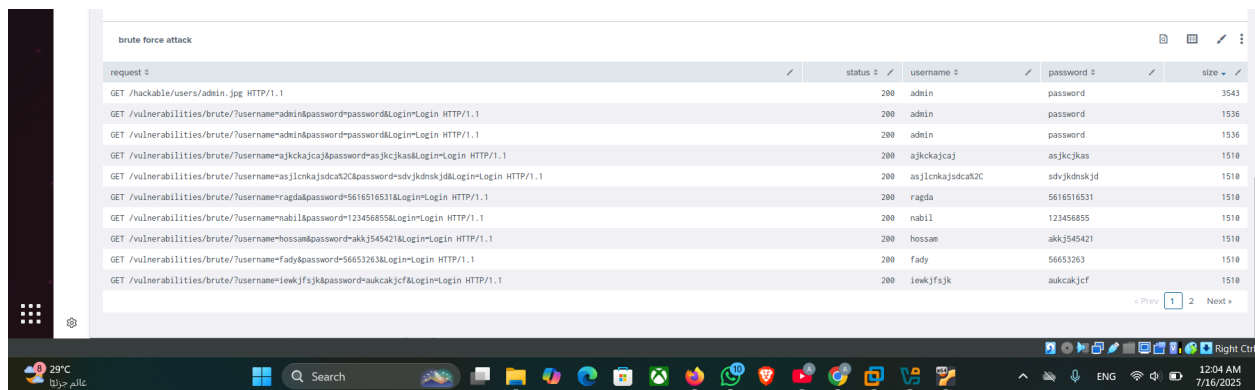
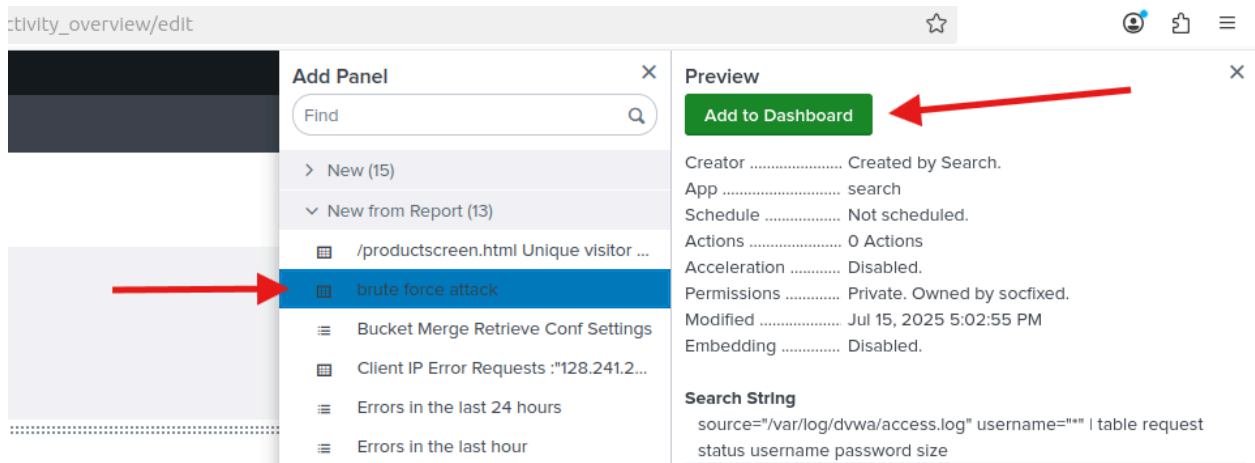
Step 3: Save As Dashboard Panel



1- click edit

2-add panel

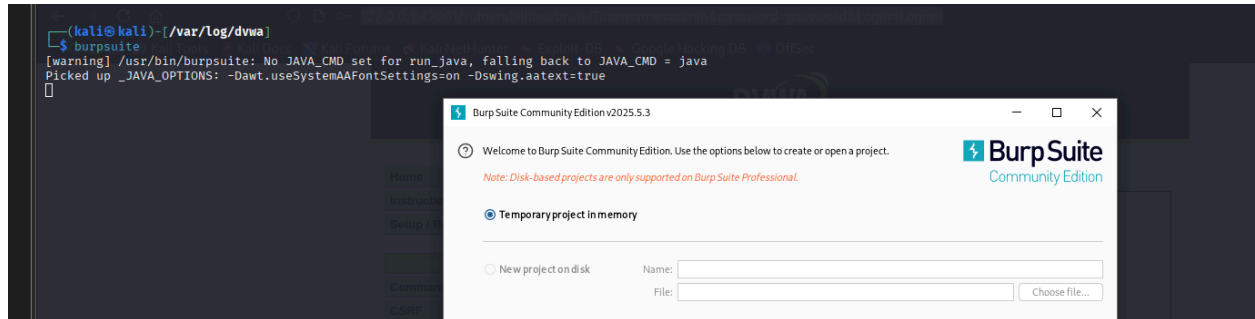
3-choose your report & click add to Dashboard



🔒 Simulate Brute Force Attack Using Burp Suite

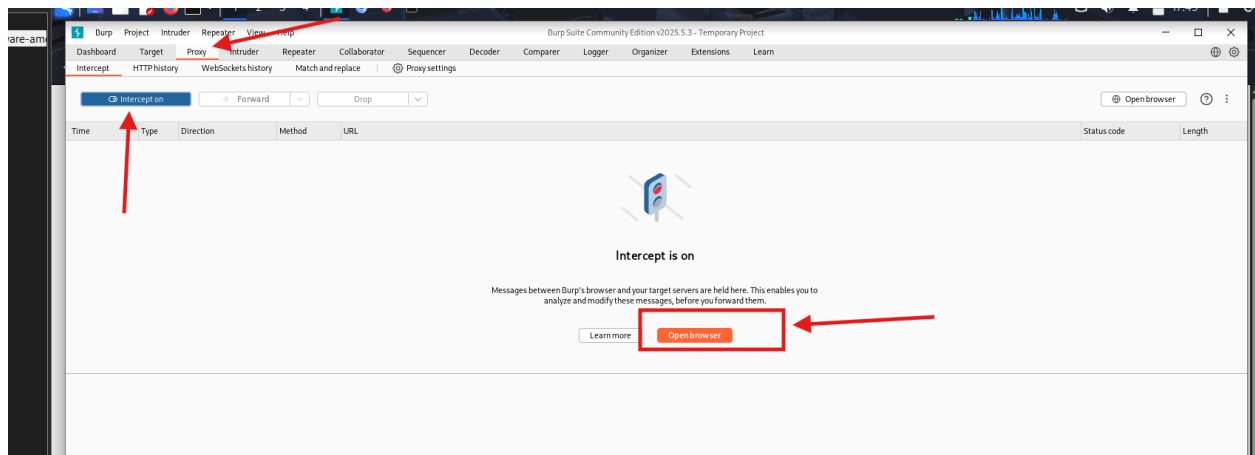
🚀 Launching Burp Suite on Linux:

----> 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.

