Reto 2 - Administración sesiones y perfiles web

Thursday, June 8, 2023 2:31 PM

El departamento de tecnologías de la información tiene la sospecha de que las aplicaciones web han sido comprometidas, por lo que se debe de realizar el análisis de cada una de ellas. Para ello se deberá llevar a cabo una copia del portal web actual, realizar una inspección de vulnerabilidades de inyección, de falsificación de identidad, de explotación de solicitudes y de vulnerabilidades en los perfiles en el servidor web.

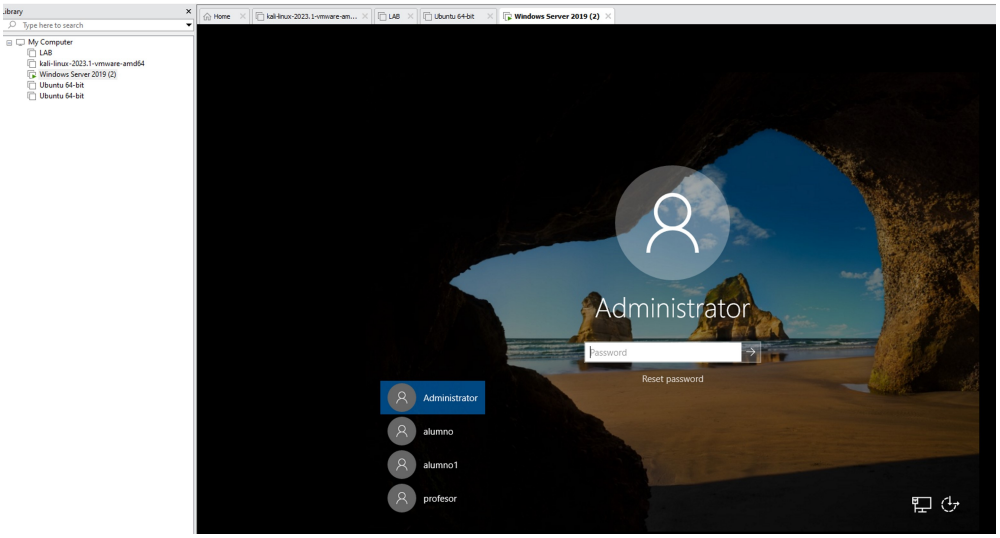
Criterios de evaluación

• Administración de sesiones y perfiles web

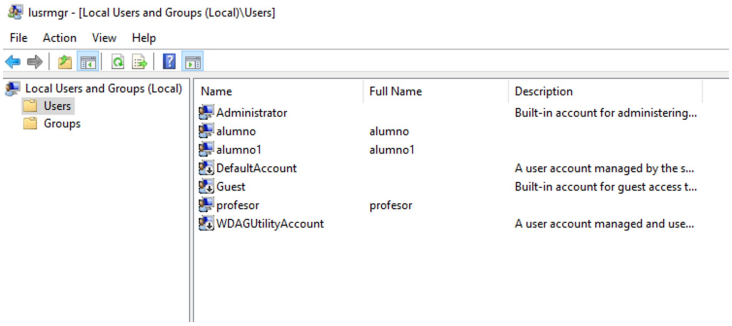
• Atacar por inyecciones y vulnerabilidades XSS

• Falsificar la identidad y explotar solicitudes entre sitios

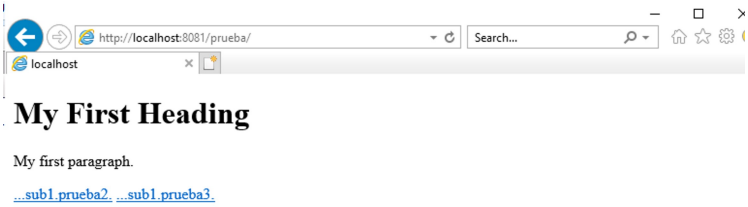
Ambiente Windows Server

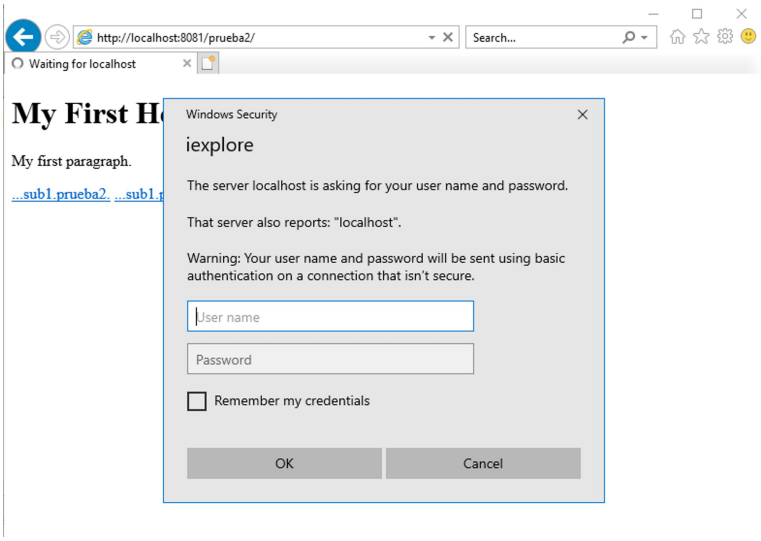


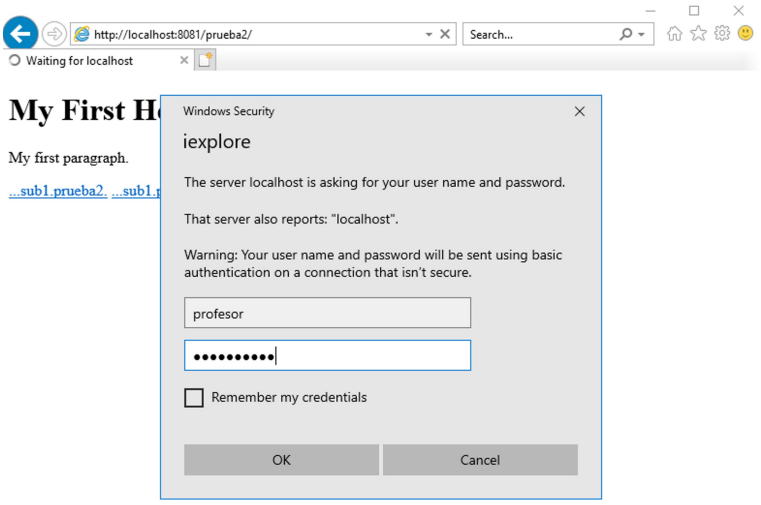
Usuarios en servidor

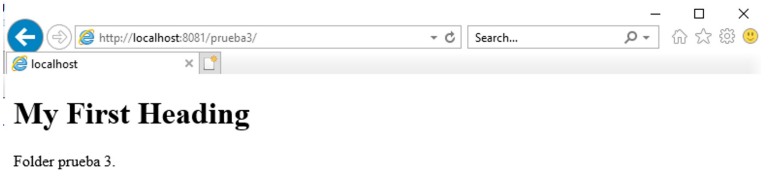


Accesos en pagina web con diferentes autorizaciones

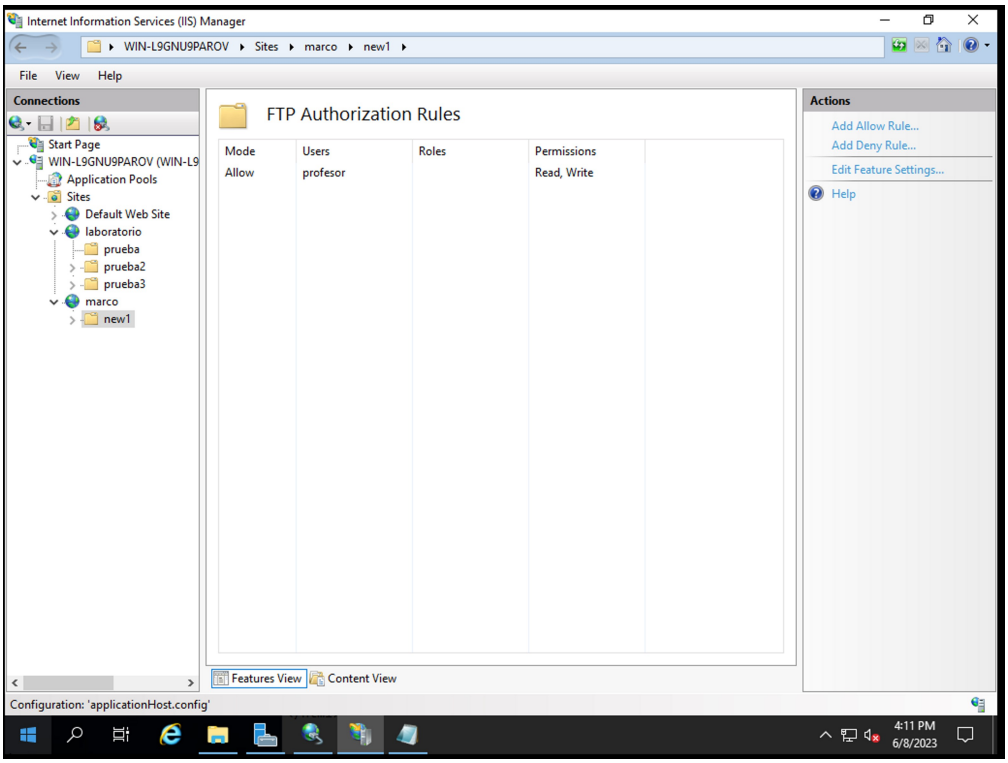




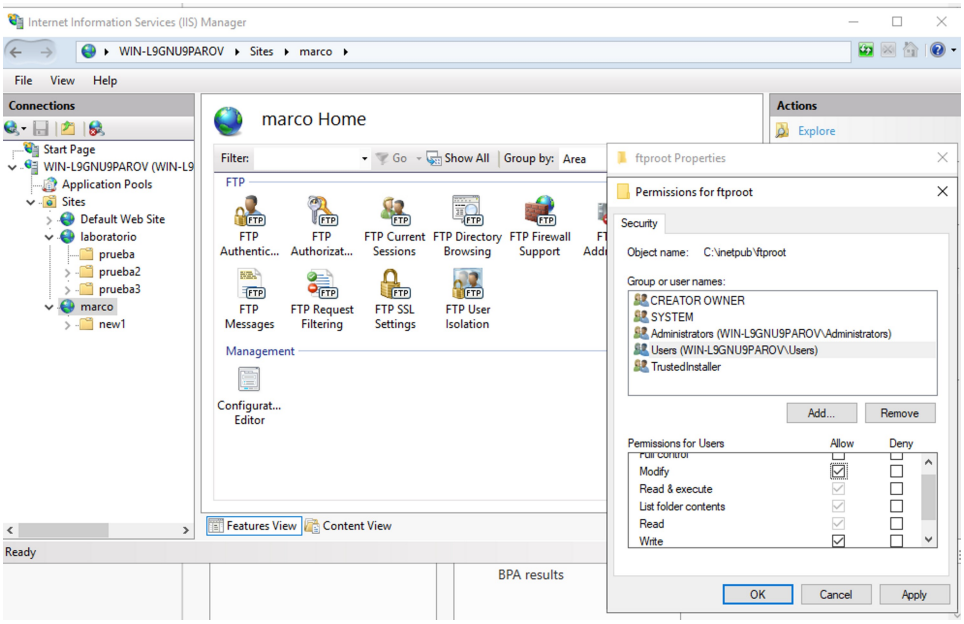




FTP - manejo autorizaciones



Agregando permisos a usuarios

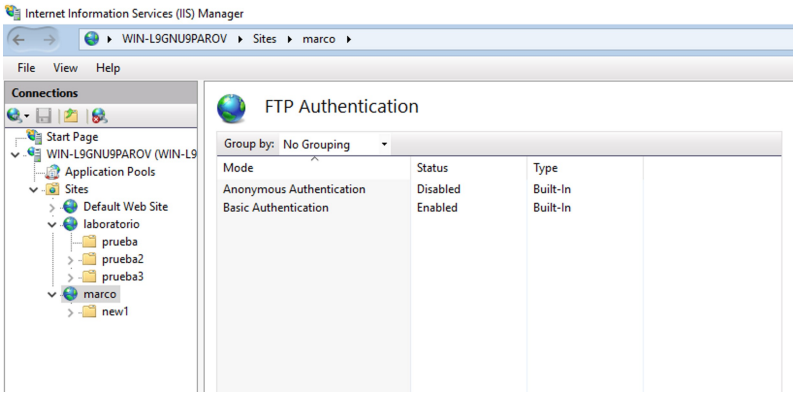


Login de usuario profesor

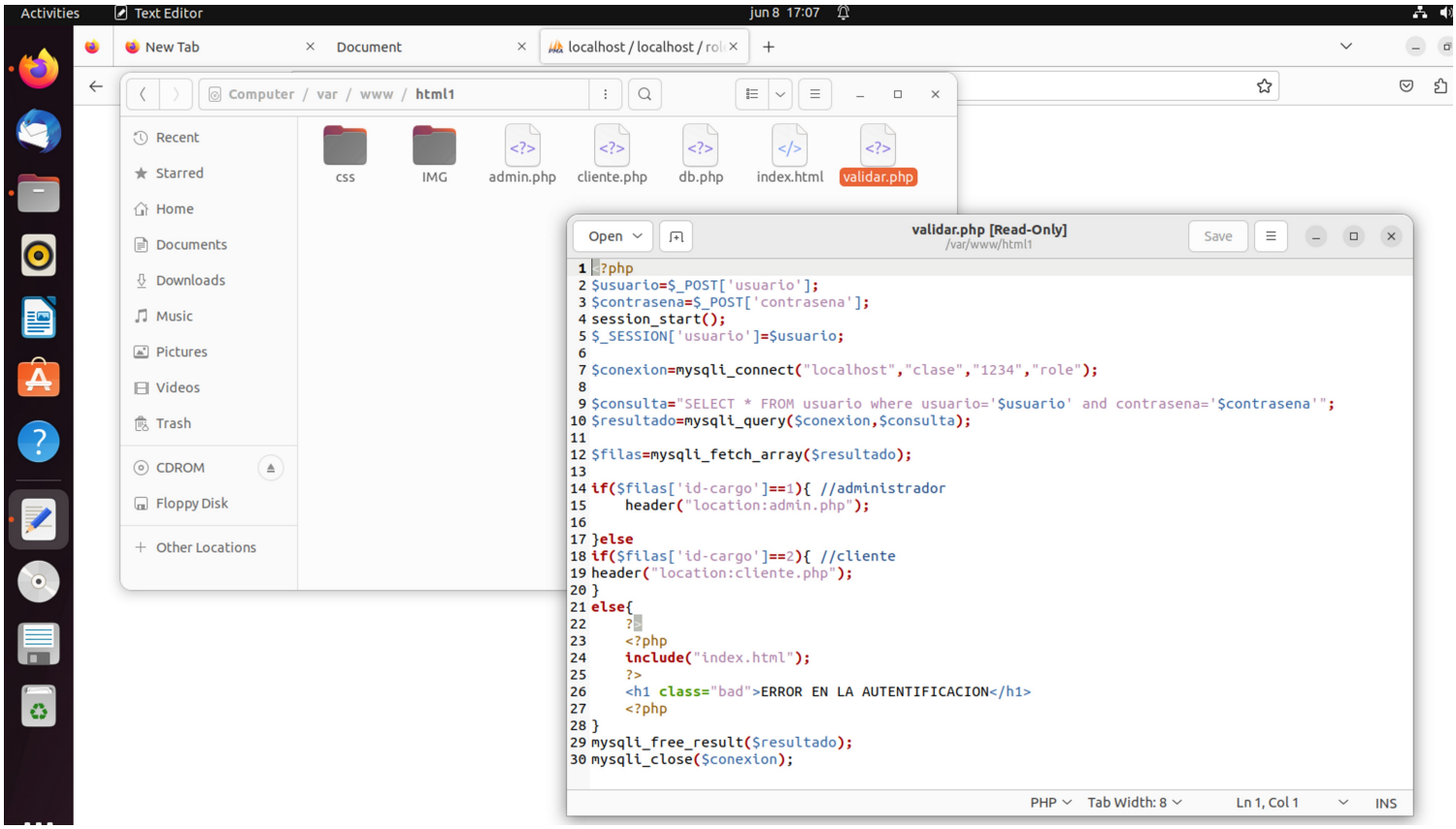
```
C:\Users\Administrator>ftp 192.168.208.132
Connected to 192.168.208.132.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.208.132:(none)): profesor
331 Password required
Password:
230 User logged in.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
05-15-23  02:23PM       <DIR>          new1
226 Transfer complete.
ftp: 48 bytes received in 0.00Seconds 48000.00Kbytes/sec.
```

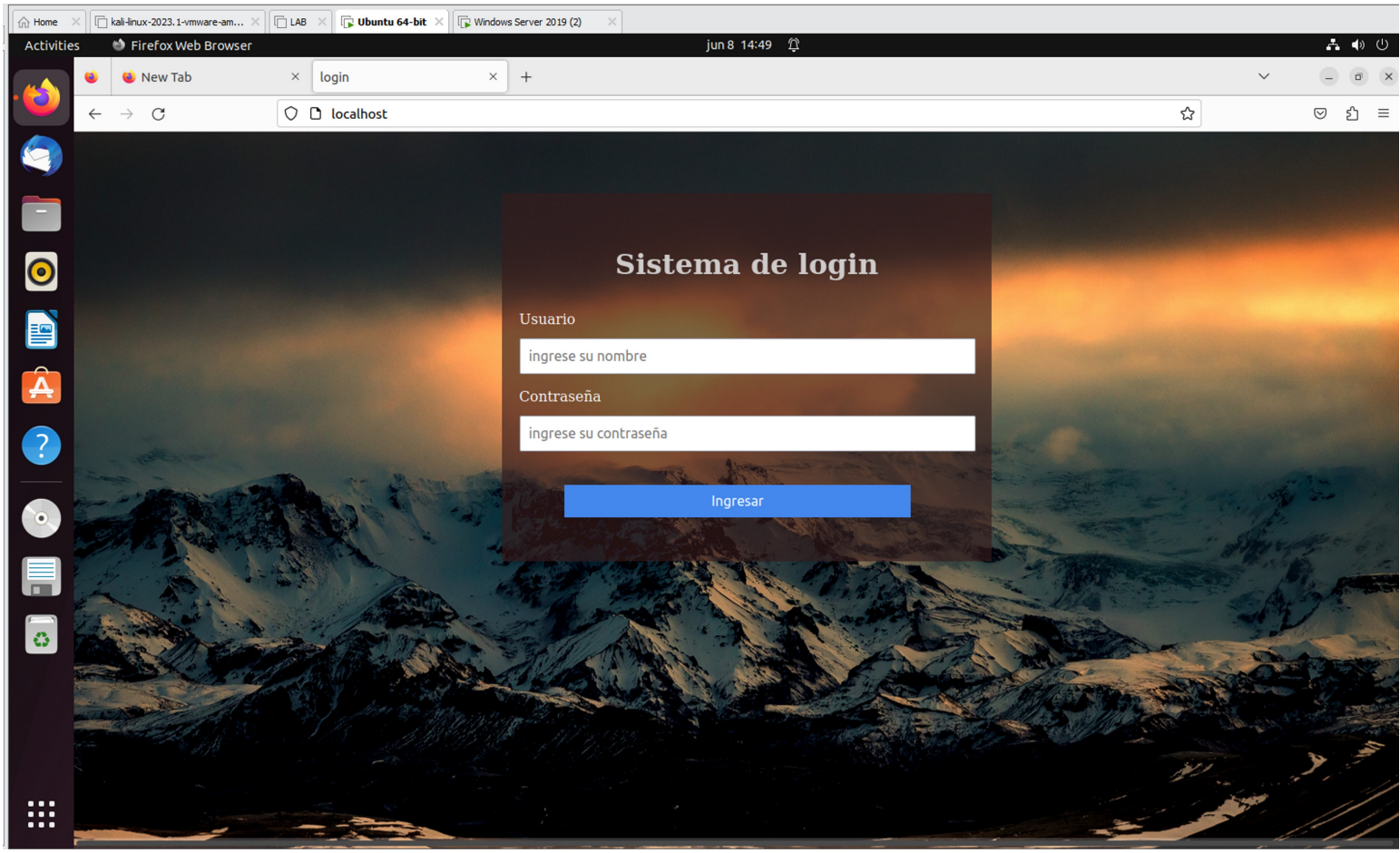
Login con user anonymous deshabilitado

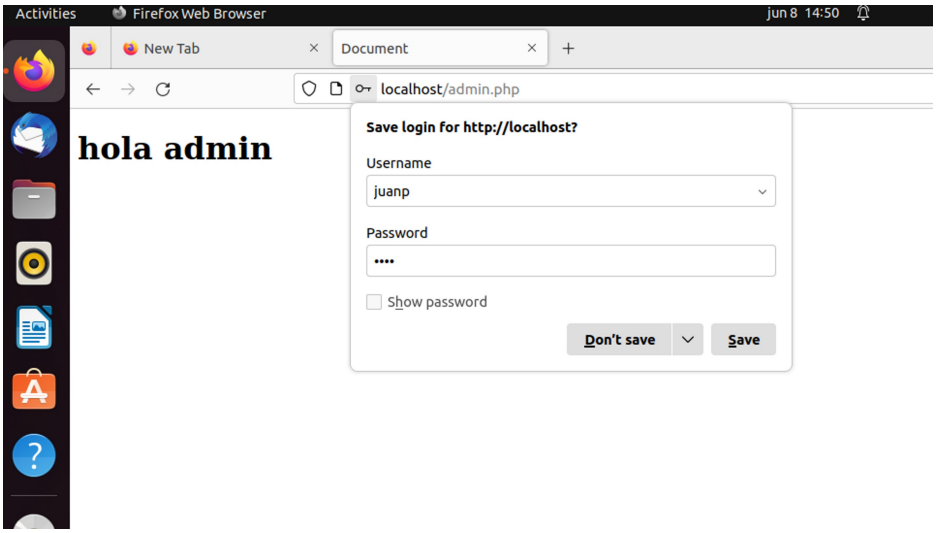
```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::f6b9:88e9:235d:5f47%5
   IPv4 Address. . . . . . . . . . . : 192.168.208.132
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.208.2

C:\Users\Administrator>ftp 192.168.208.132
Connected to 192.168.208.132.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.208.132:(none)): anonymous
331 Password required
Password:
530-User cannot log in.
 Win32 error:   The user name or password is incorrect.
 Error details: Anonymous authentication is not allowed.
530 End
Login failed.
ftp>
```

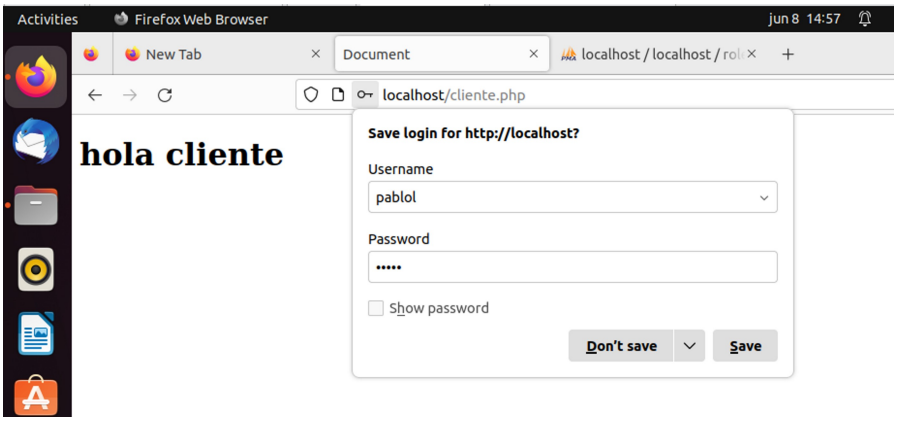


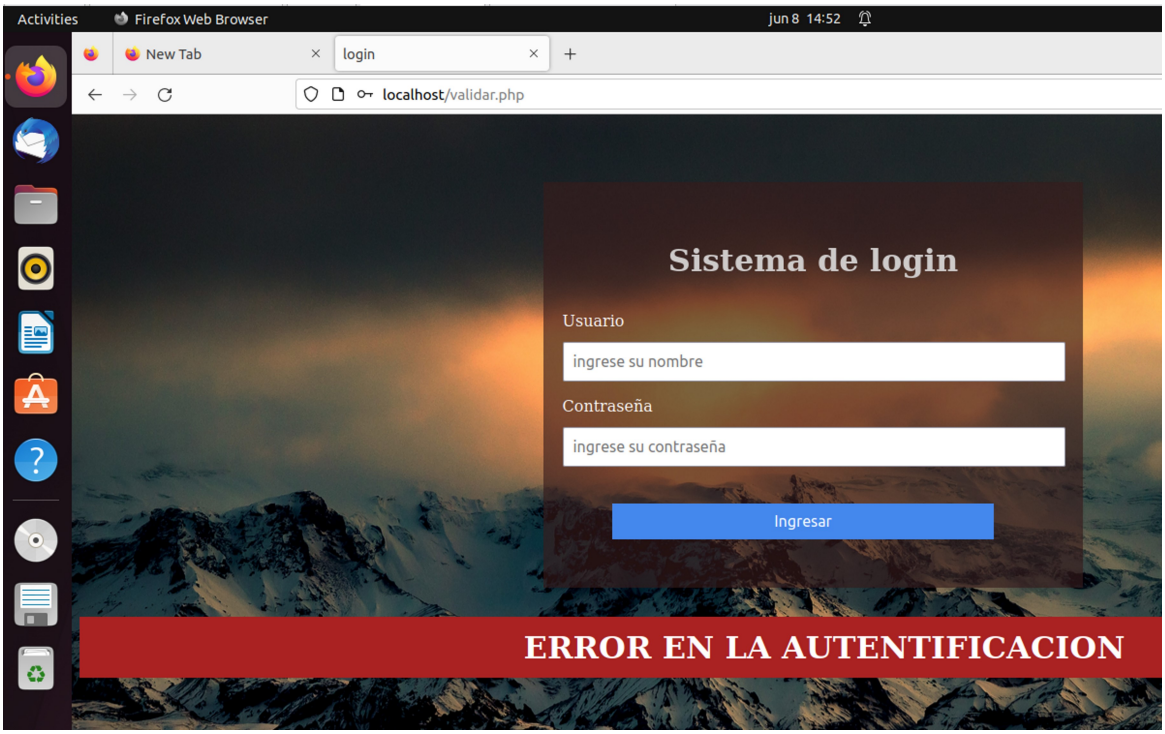
Manejo de usuarios y accesos en ambiente Linux

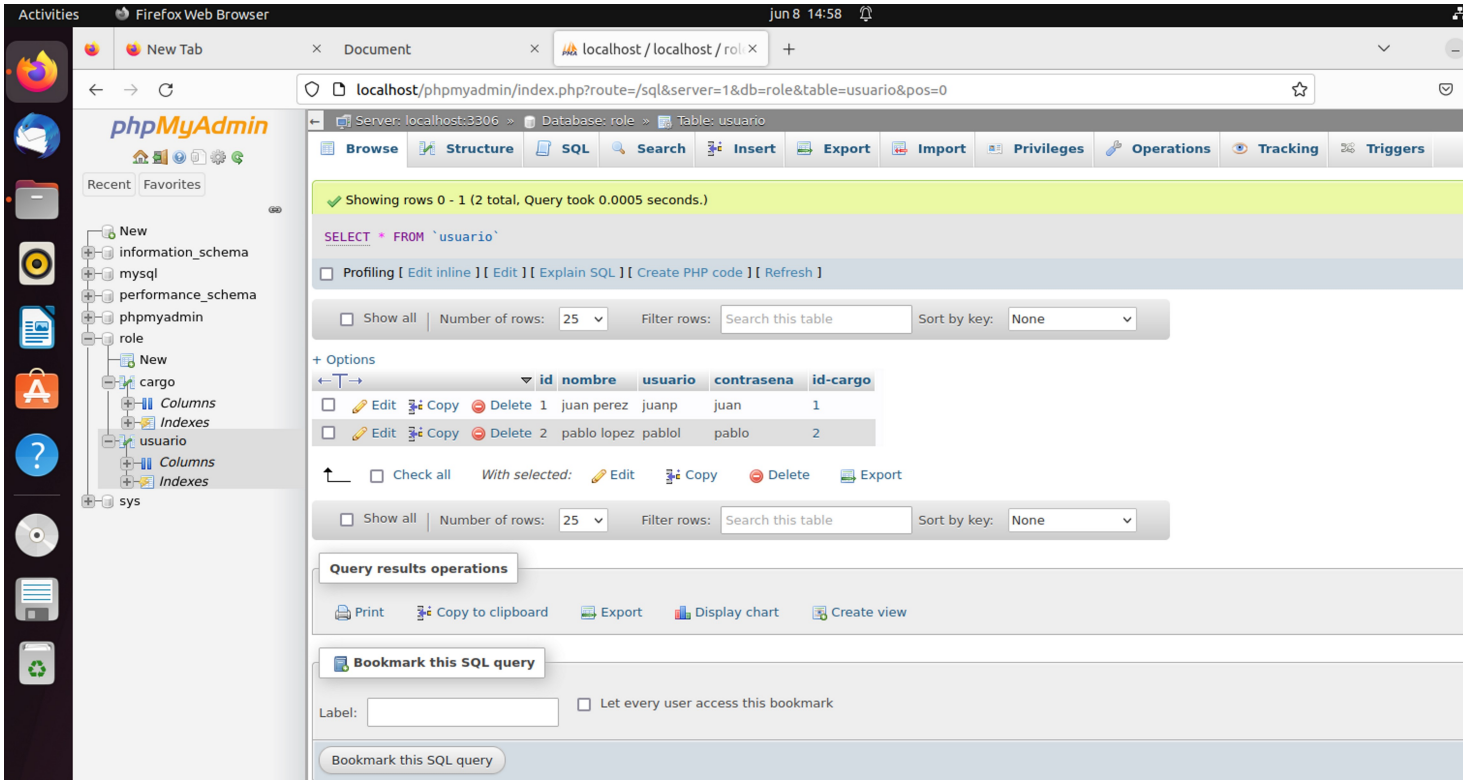


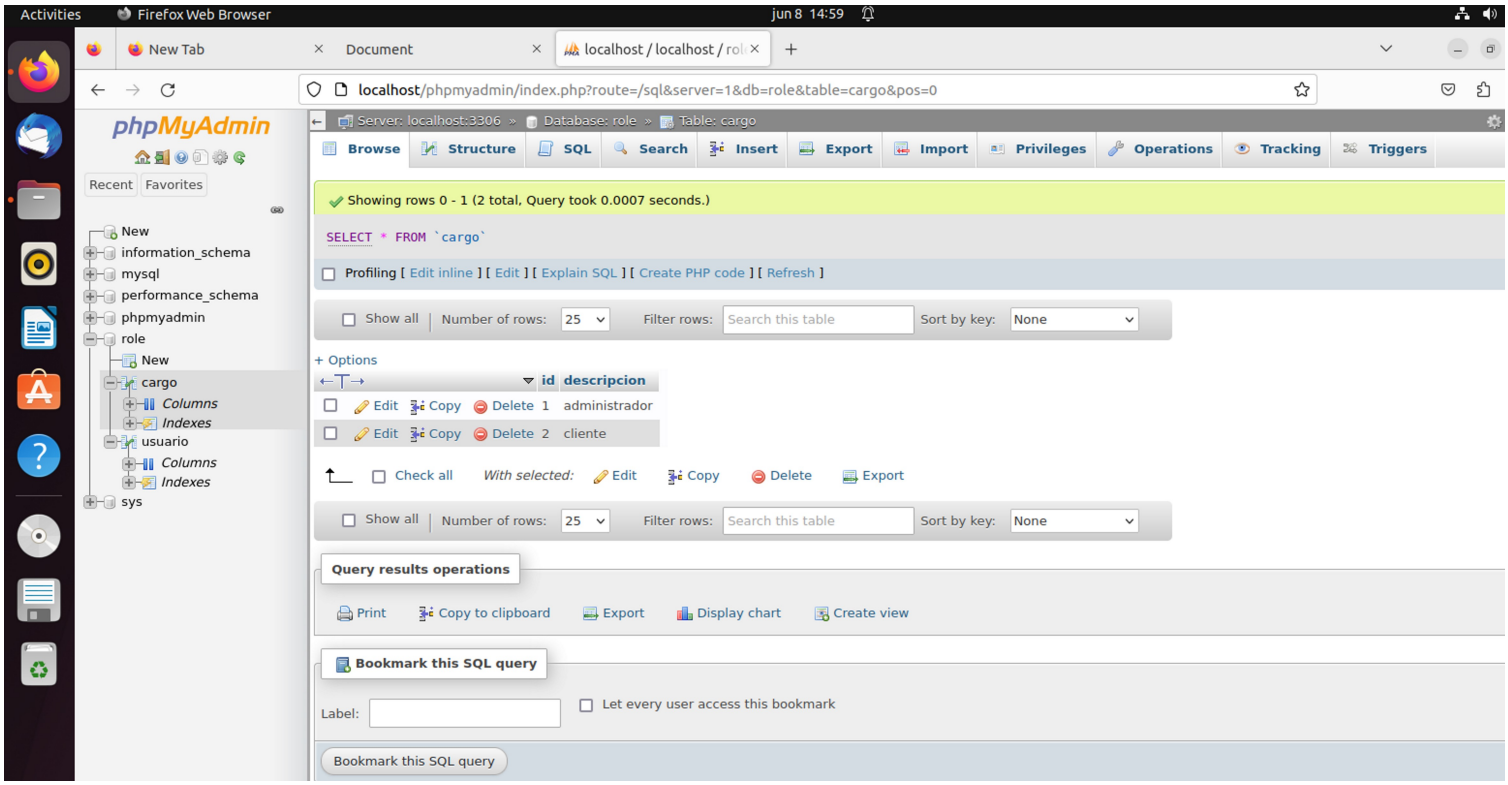

Home
kali-linux-2023.1-vmware-am...
LAB
Ubuntu 64-bit
Windows Server 2019 (2)
Activities
Firefox Web Browser
jun 8 14:49
New Tab
login
localhost
Sistema de login
Usuario
ingrese su nombre
Contraseña
ingrese su contraseña
Ingresar


Activities
Firefox Web Browser
jun 8 14:50
New Tab
Document
localhost/admin.php
hola admin
Save login for http://localhost?
Username
juanp
Password
Show password
Don't save
Save


Activities
Firefox Web Browser
jun 8 14:57
New Tab
Document
localhost / localhost / rol
localhost/cliente.php
hola cliente
Save login for http://localhost?
Username
pablol
Password
Show password
Don't save
Save


Activities
Firefox Web Browser
jun 8 14:52
New Tab
login
localhost/validar.php
Sistema de login
Usuario
ingrese su nombre
Contraseña
ingrese su contraseña
Ingresar
ERROR EN LA AUTENTIFICACION


Activities
Firefox Web Browser
jun 8 14:58
New Tab
Document
localhost / localhost / rol
localhost/phpmyadmin/index.php?route=/sql&server=1&db=role&table=usuario&pos=0
phpMyAdmin
Recent
Favorites
New
information_schema
mysql
performance_schema
phpmyadmin
role
New
cargo
Columns
Indexes
usuario
Columns
Indexes
sys
Server: localhost:3306 » Database: role » Table: usuario
Browse
Structure
SQL
Search
Insert
Export
Import
Privileges
Operations
Tracking
Triggers
Showing rows 0 - 1 (2 total, Query took 0.0005 seconds.)
SELECT * FROM `usuario`
Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
Show all
Number of rows: 25
Filter rows: Search this table
Sort by key: None
+ Options
id nombre usuario contrasena id-cargo
Edit Copy Delete 1 juan perez juanp juan 1
Edit Copy Delete 2 pablo lopez pablol pablo 2
Check all
With selected:
Edit
Copy
Delete
Export
Query results operations
Print
Copy to clipboard
Export
Display chart
Create view
Bookmark this SQL query
Label:
Let every user access this bookmark
Bookmark this SQL query


Activities
Firefox Web Browser
jun 8 14:59
New Tab
Document
localhost / localhost / rol
localhost/phpmyadmin/index.php?route=/sql&server=1&db=role&table=cargo&pos=0
phpMyAdmin
Recent
Favorites
New
information_schema
mysql
performance_schema
phpmyadmin
role
New
cargo
Columns
Indexes
usuario
Columns
Indexes
sys
Server: localhost:3306 » Database: role » Table: cargo
Browse
Structure
SQL
Search
Insert
Export
Import
Privileges
Operations
Tracking
Triggers
Showing rows 0 - 1 (2 total, Query took 0.0007 seconds.)
SELECT * FROM `cargo`
Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
Show all
Number of rows: 25
Filter rows: Search this table
Sort by key: None
+ Options
id descripcion
Edit Copy Delete 1 administrador
Edit Copy Delete 2 cliente
Check all
With selected:
Edit
Copy
Delete
Export
Query results operations
Print
Copy to clipboard
Export
Display chart
Create view
Bookmark this SQL query
Label:
Let every user access this bookmark
Bookmark this SQL query