

Laboratorio 12 Cursos Ciberseguridad

Sesión #12 Escaneo de vulnerabilidades

Jesús Rodrigo Toro Navarro

Universidad Popular del Cesar

Introducción

En el contexto actual de amenazas digitales cada vez más sofisticadas, es fundamental que los profesionales de TI y estudiantes de ciberseguridad comprendan a fondo cómo identificar, analizar y mitigar vulnerabilidades en sistemas informáticos. El presente laboratorio está diseñado con el propósito de ofrecer una experiencia práctica en el escaneo de vulnerabilidades utilizando herramientas accesibles y potentes en un entorno controlado. Para ello, se emplean XAMPP como plataforma de servidor local y DVWA (Damn Vulnerable Web Application) como aplicación vulnerable de prueba.


XAMPP es un paquete gratuito y de código abierto que incluye Apache, MySQL, PHP y Perl, lo que facilita la instalación y ejecución de aplicaciones web de manera local sin necesidad de configuración avanzada. Gracias a su compatibilidad con múltiples sistemas operativos y su facilidad de uso, XAMPP se convierte en una herramienta ideal para ambientes educativos y de pruebas.

Por otro lado, DVWA es una aplicación web desarrollada con el objetivo de ser deliberadamente insegura, permitiendo así que los usuarios exploren y comprendan cómo las diferentes vulnerabilidades pueden ser explotadas en la práctica. Entre las debilidades que se pueden experimentar en DVWA se incluyen inyección SQL, fallas de autenticación, ejecución remota de comandos, XSS, CSRF, entre otras. Esta variedad convierte a DVWA en un recurso valioso para simular escenarios reales de ataque y defensa en aplicaciones web.

Durante el desarrollo del laboratorio, los estudiantes configurarán su entorno de trabajo instalando XAMPP y DVWA, y luego aplicarán herramientas de escaneo como Nessus u OpenVAS para detectar vulnerabilidades presentes en la aplicación. Posteriormente, se analizarán los resultados obtenidos y se propondrán medidas de mitigación basadas en buenas prácticas de seguridad y estándares como el CVSS (Common Vulnerability Scoring System).

Descargamos XAMPP o AMPP <https://www.apachefriends.org/es/index.html> o <https://www.ampps.com/downloads/>


[Apache Friends](#) [Descargar](#) [Alojamiento](#) [Comunidad](#) [Acerca de](#) [Buscar](#) [ES](#)

 **XAMPP** Apache + MariaDB + PHP + Perl


¿Qué es XAMPP?


XAMPP es el entorno más popular de desarrollo con PHP


XAMPP es una distribución de Apache completamente gratuita y fácil de instalar que contiene MariaDB, PHP y Perl. El paquete de instalación de XAMPP ha sido diseñado para ser increíblemente fácil de instalar y usar.


XAMPP

Descargar
Pulsa aquí para otras versiones

 **XAMPP para Windows**
8.2.12 (PHP 8.2.12)

 **XAMPP para Linux**
8.2.12 (PHP 8.2.12)

 **XAMPP para OS X**
8.2.4 (PHP 8.2.4)

New XAMPP release 8.2.12, 8.1.25 and 8.0.30


Hi Apache Friends!


We just released a new version of XAMPP for Windows for PHP versions 8.2.12, 8.1.25 and 8.0.30. New versions for Linux and OS X will come soon! You can download these new installers...

[Más información »](#)

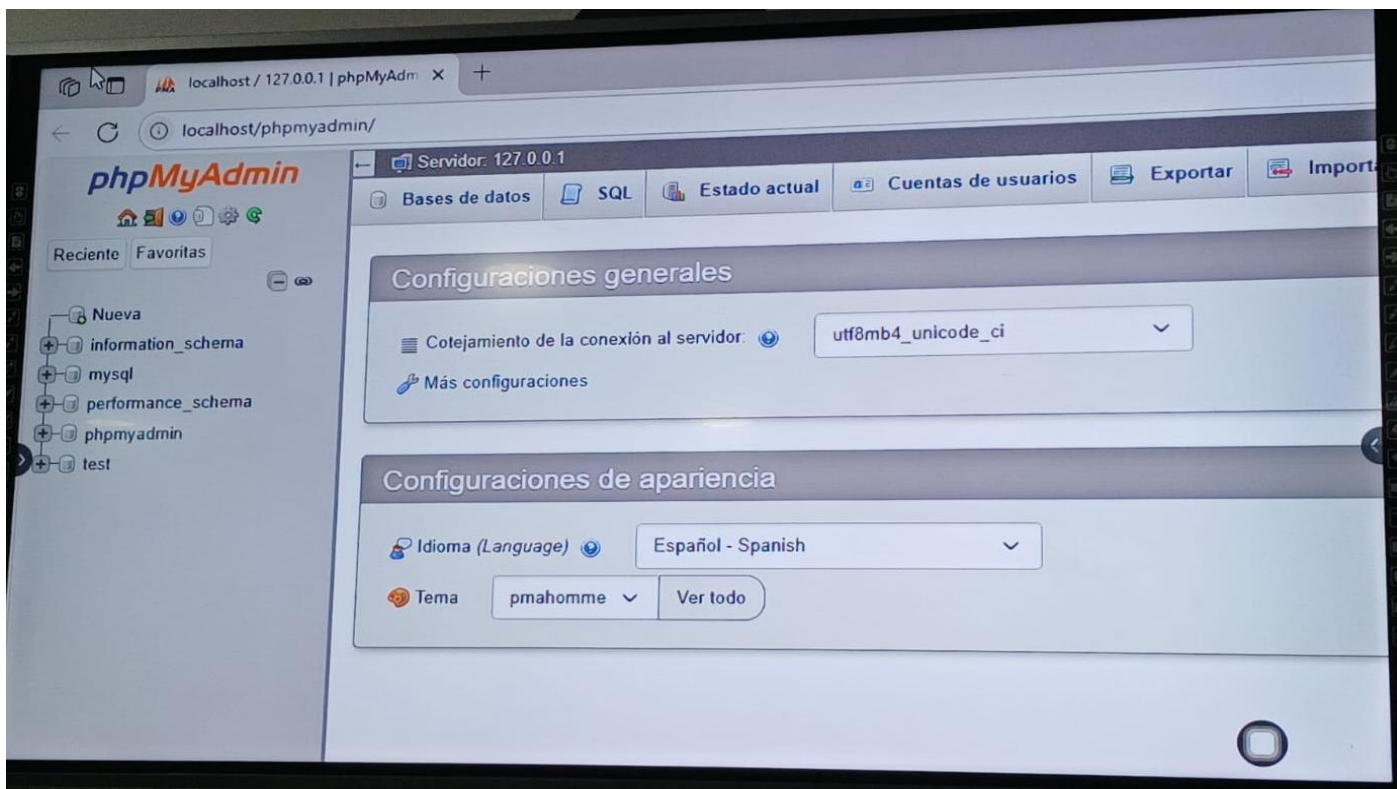
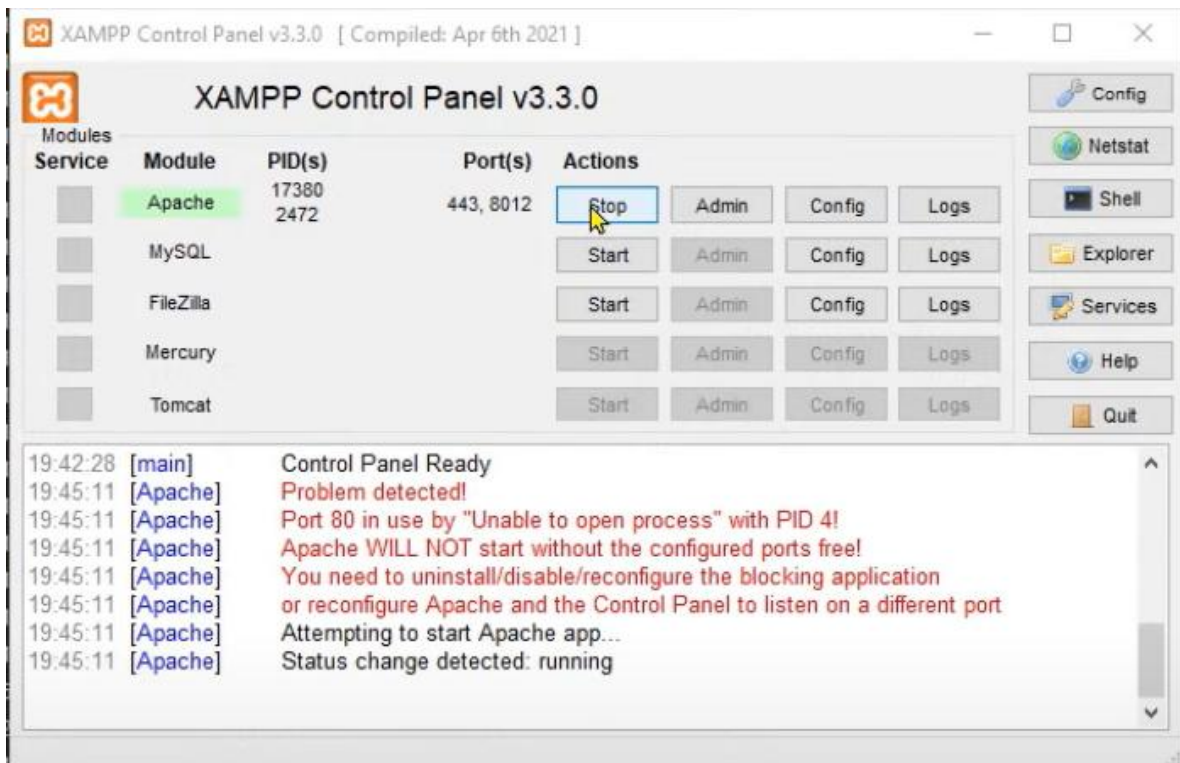
[Acerca de Apache Friends](#) [Comunidad](#) [Temas Derivados](#)

Download AMPPS

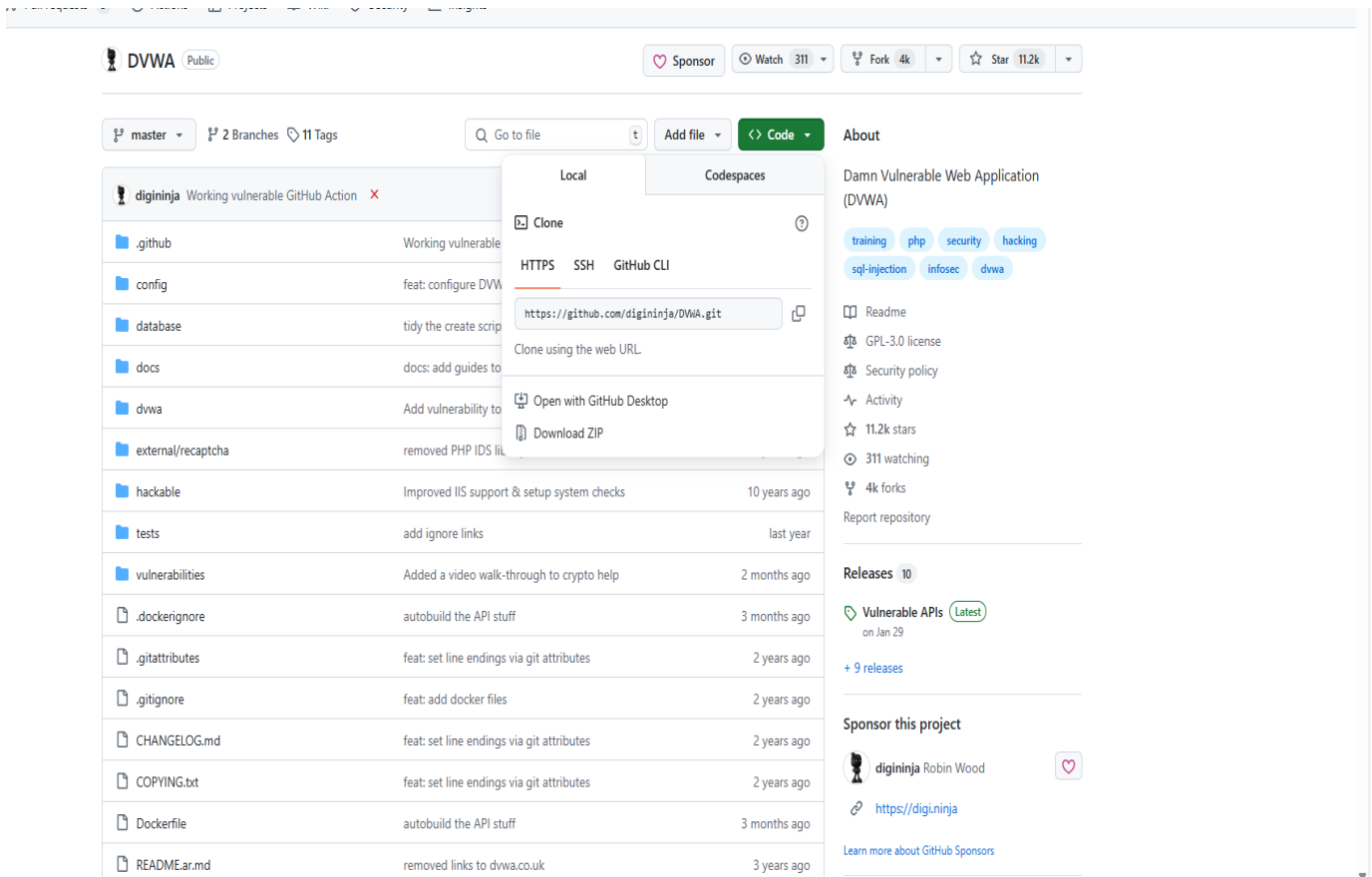

macOS
[Download](#)
Installer Package type: DMG
Supported OS
Sequoia, Sonoma, Ventura, Monterey, Big Sur & Catalina


Windows
[Download](#)
Installer Package type: EXE
Supported OS
Windows 11, 10, 7 (SP1 +), 8, Vista
Windows Server 2022, 2019, 2016, 2012
(Note: Windows XP and Windows Server 2008 or lower is not supported)

All Product Logos used are Trademarks of their Respective Companies
You must read and fully understand the License agreement before you download and use this

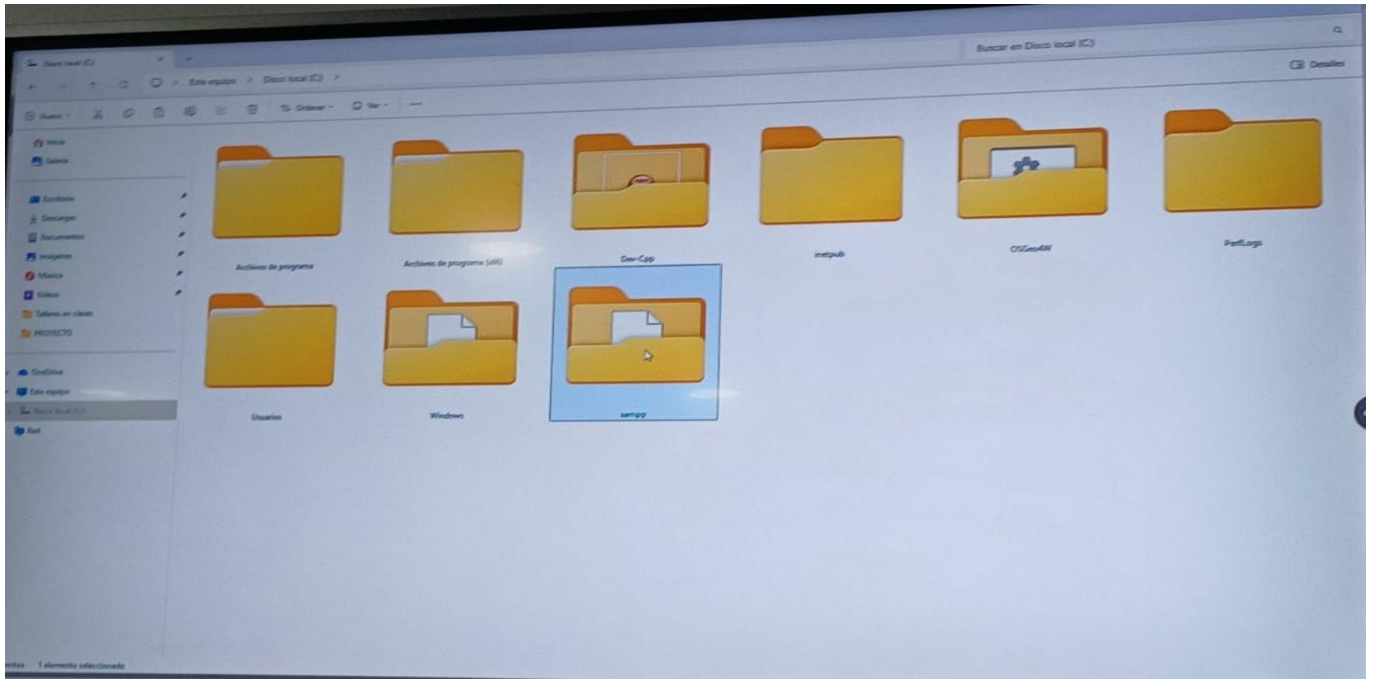


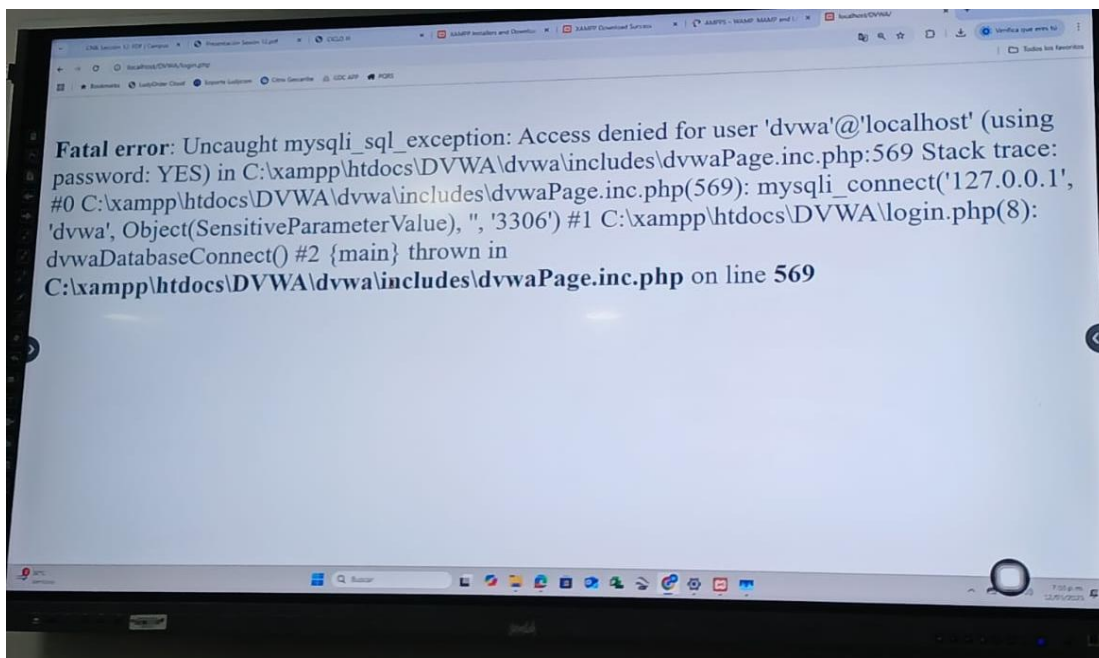
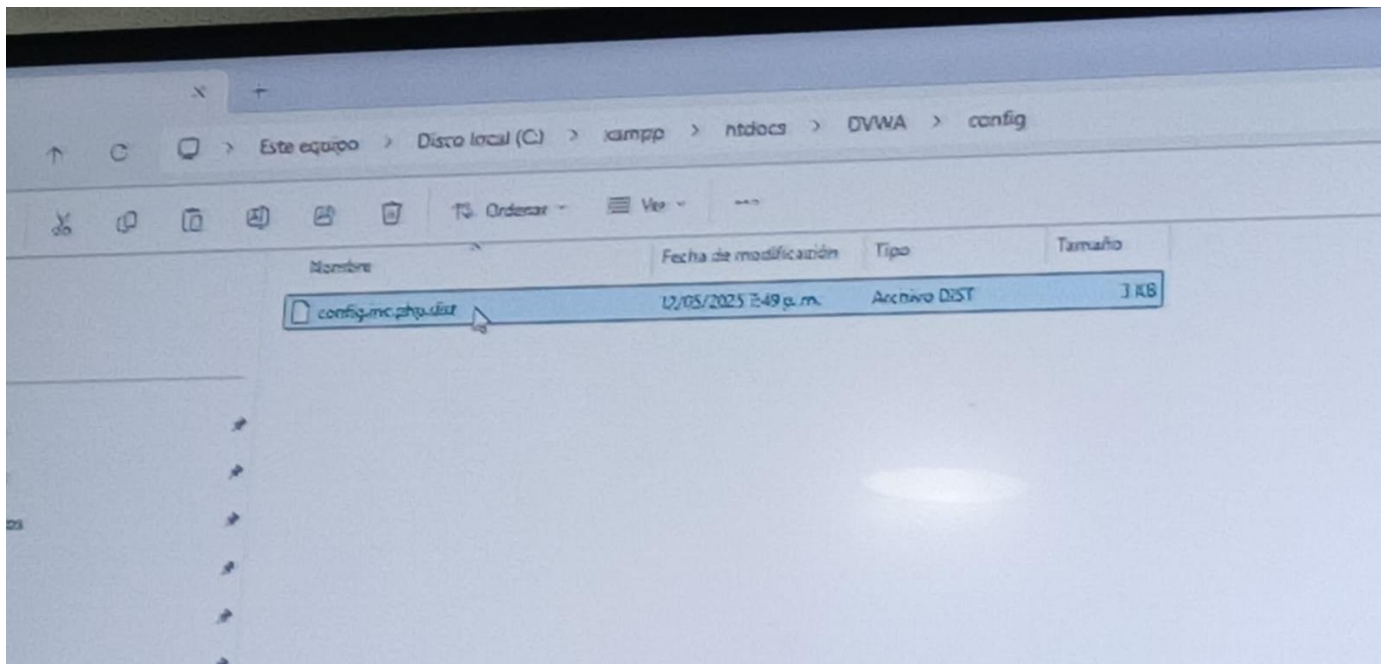
Ahora descargamos DVWA



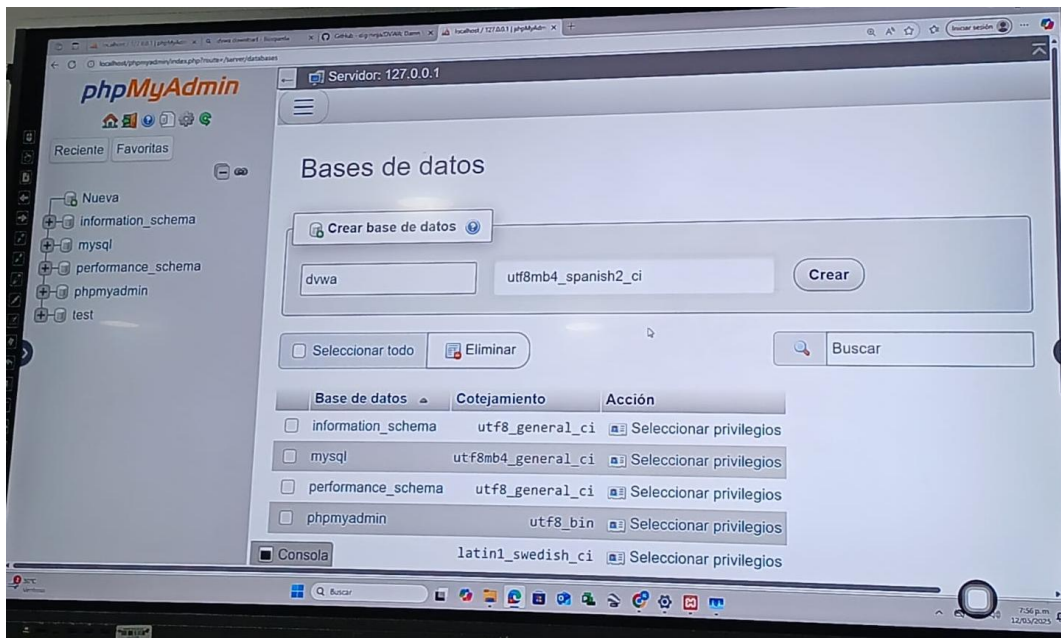
The screenshot shows the GitHub repository page for DVWA (Damn Vulnerable Web Application) by digininja. The repository is public and has 11.2k stars, 4k forks, and 311 watchers. The README describes it as a "Damn Vulnerable Web Application (DVWA)" and lists various features and tags like training, php, security, hacking, sql-injection, infosec, and dwva. A dropdown menu is open, showing options to clone the repository using HTTPS, SSH, or GitHub CLI, or to open it with GitHub Desktop or download it as a ZIP file. The repository also has a "Sponsor this project" section with a link to the sponsor page.

File	Description	Updated
.github	Working vulnerable	
config	feat: configure DVWA	
database	tidy the create scrip	
docs	docs: add guides to	
dwva	Add vulnerability to	
external/recaptcha	removed PHP IDS li	
hackable	Improved IIS support & setup system checks	10 years ago
tests	add ignore links	last year
vulnerabilities	Added a video walk-through to crypto help	2 months ago
.dockerignore	autobuild the API stuff	3 months ago
.gitattributes	feat: set line endings via git attributes	2 years ago
.gitignore	feat: add docker files	2 years ago
CHANGELOG.md	feat: set line endings via git attributes	2 years ago
COPYING.txt	feat: set line endings via git attributes	2 years ago
Dockerfile	autobuild the API stuff	3 months ago
README.ar.md	removed links to dwva.co.uk	3 years ago

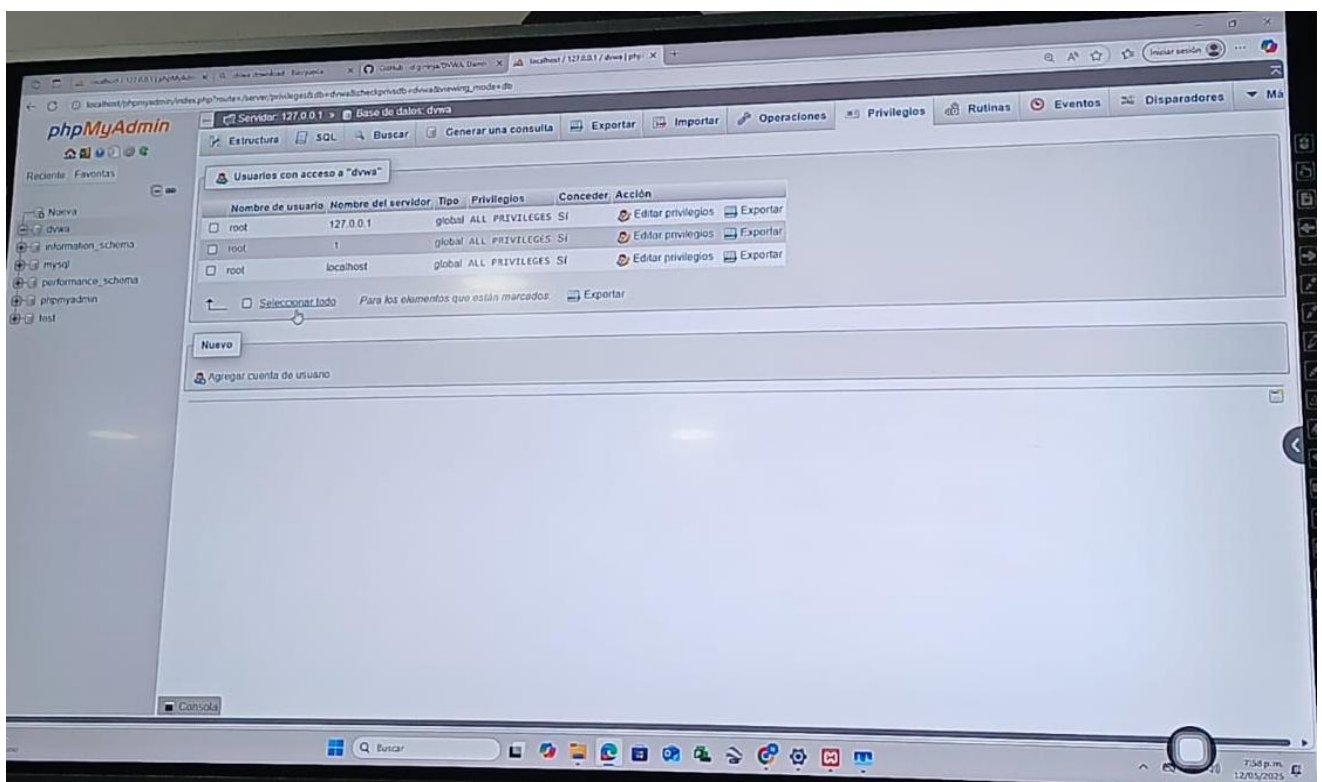


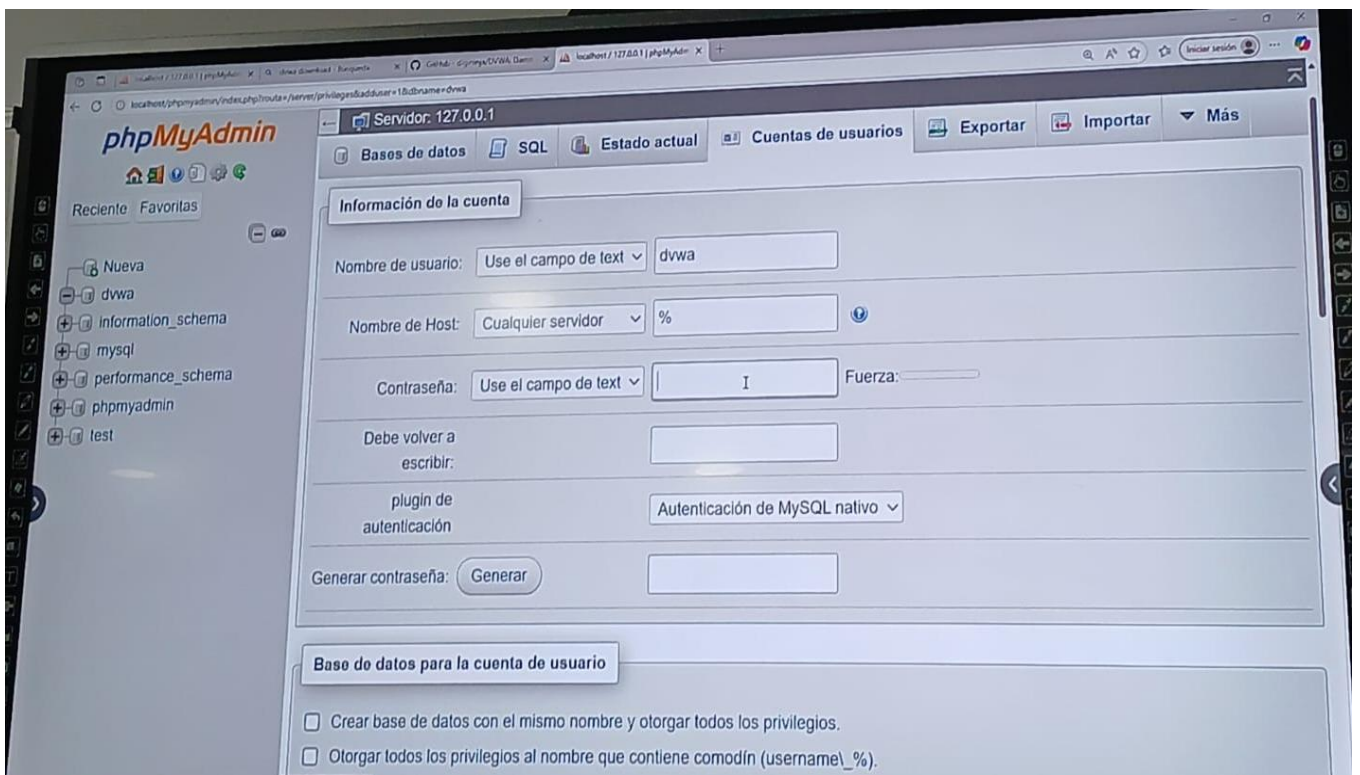
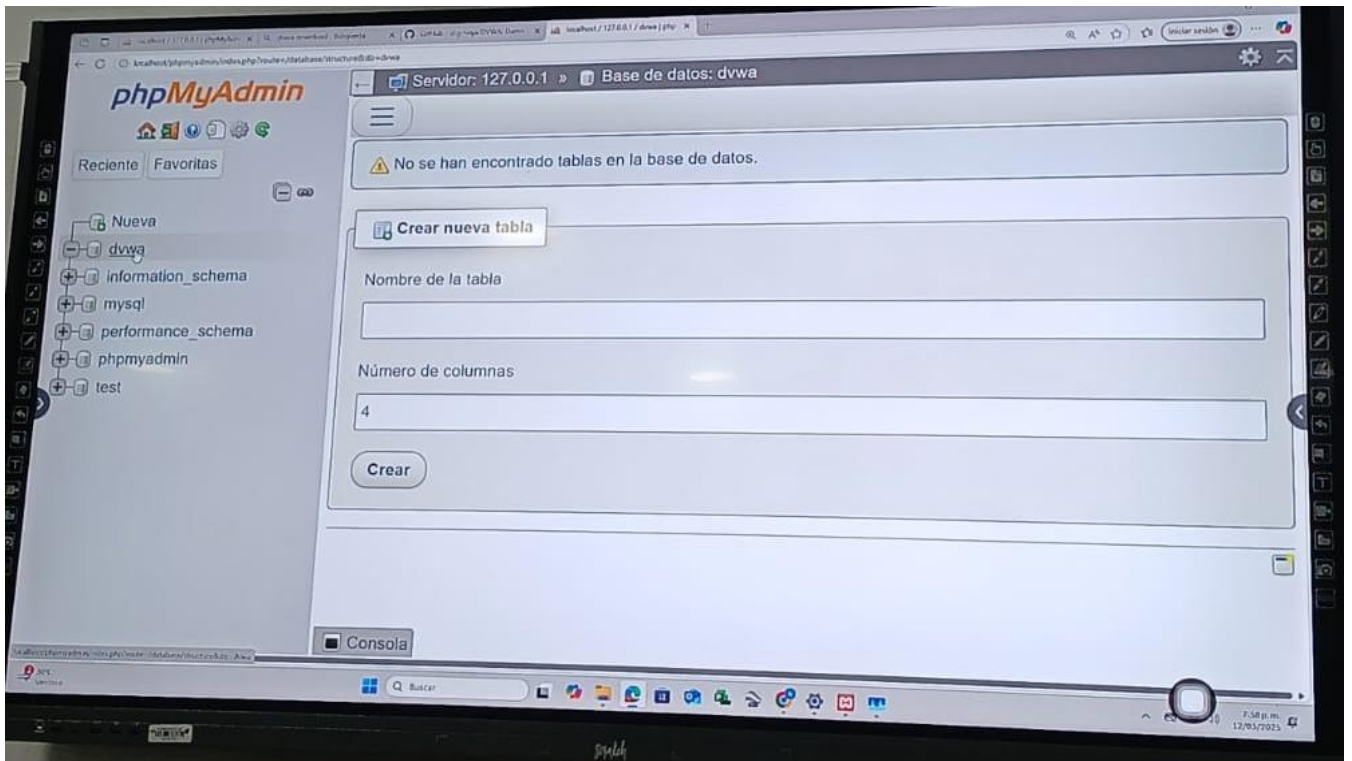


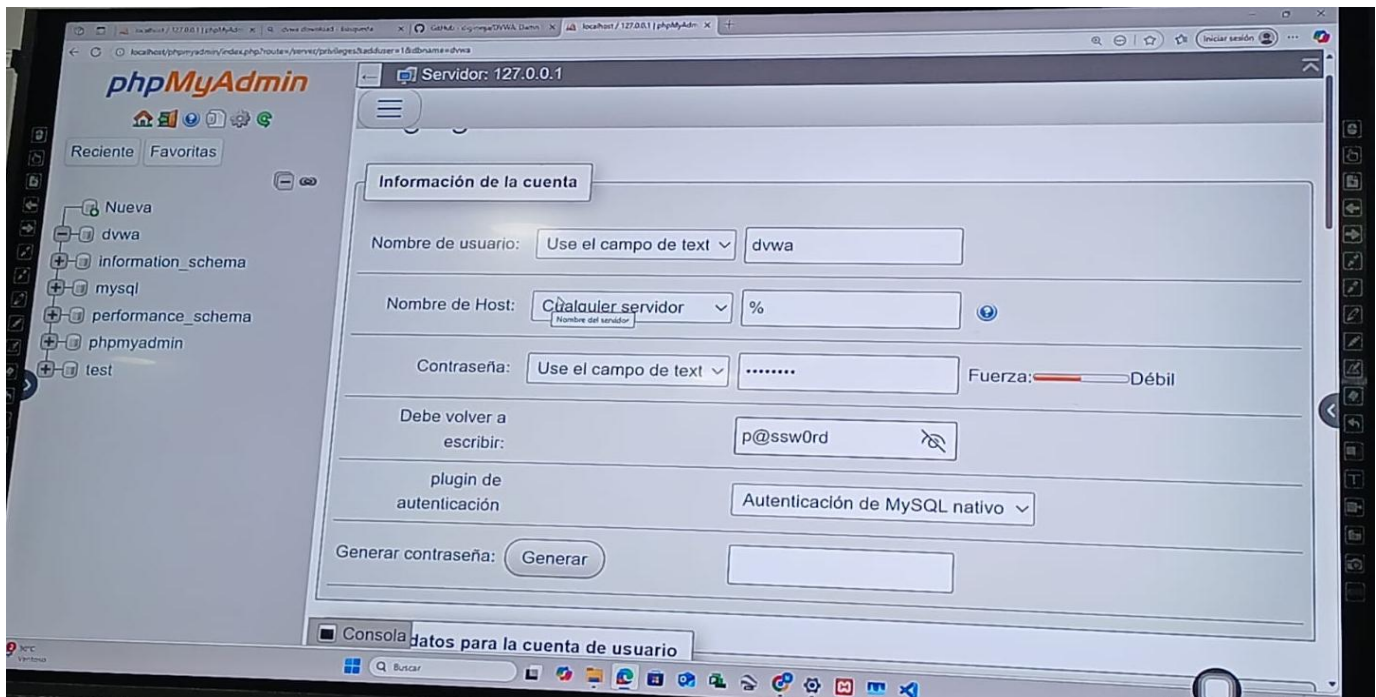
Si nos sale este error debemos crear una base de datos en XAMPP



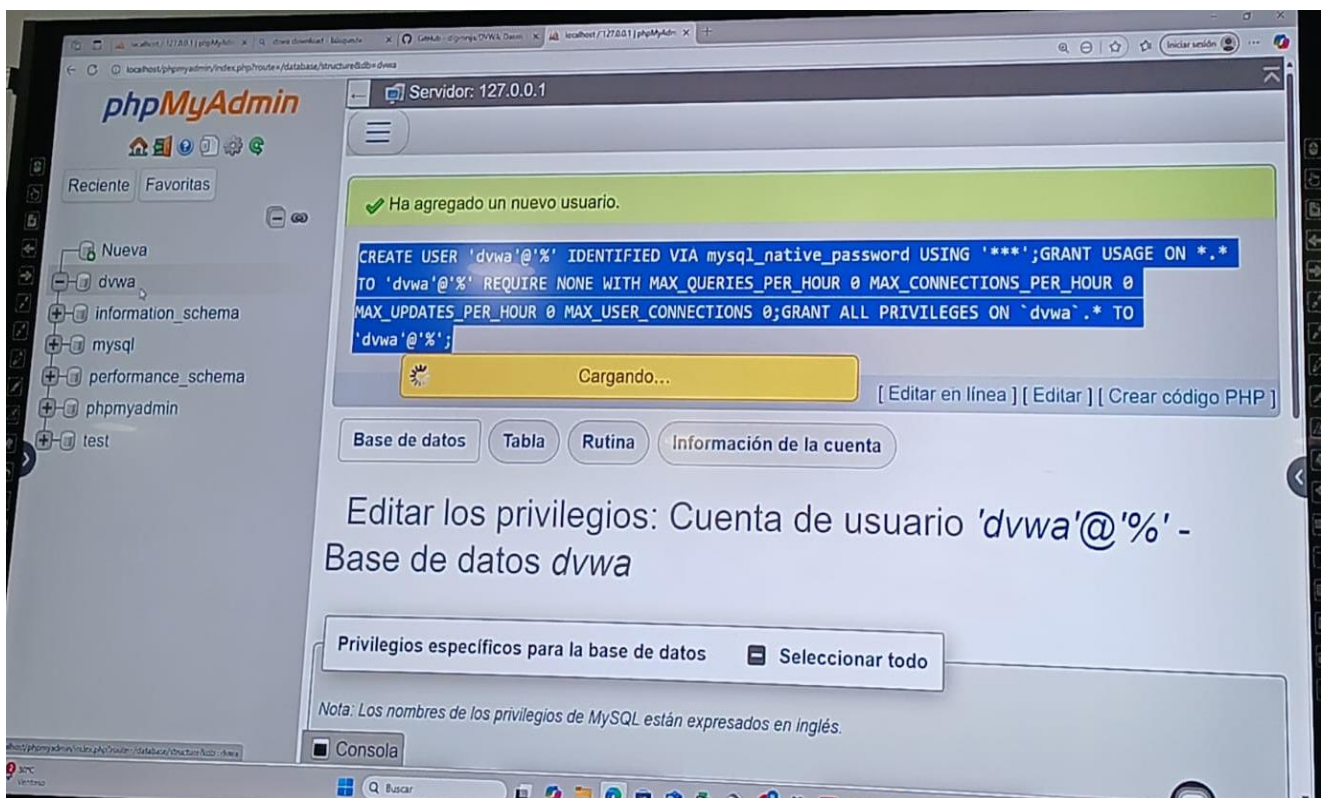
Ahora debemos crear una nueva cuenta de usuario, le damos a privilegios y a agregar cuenta de usuario







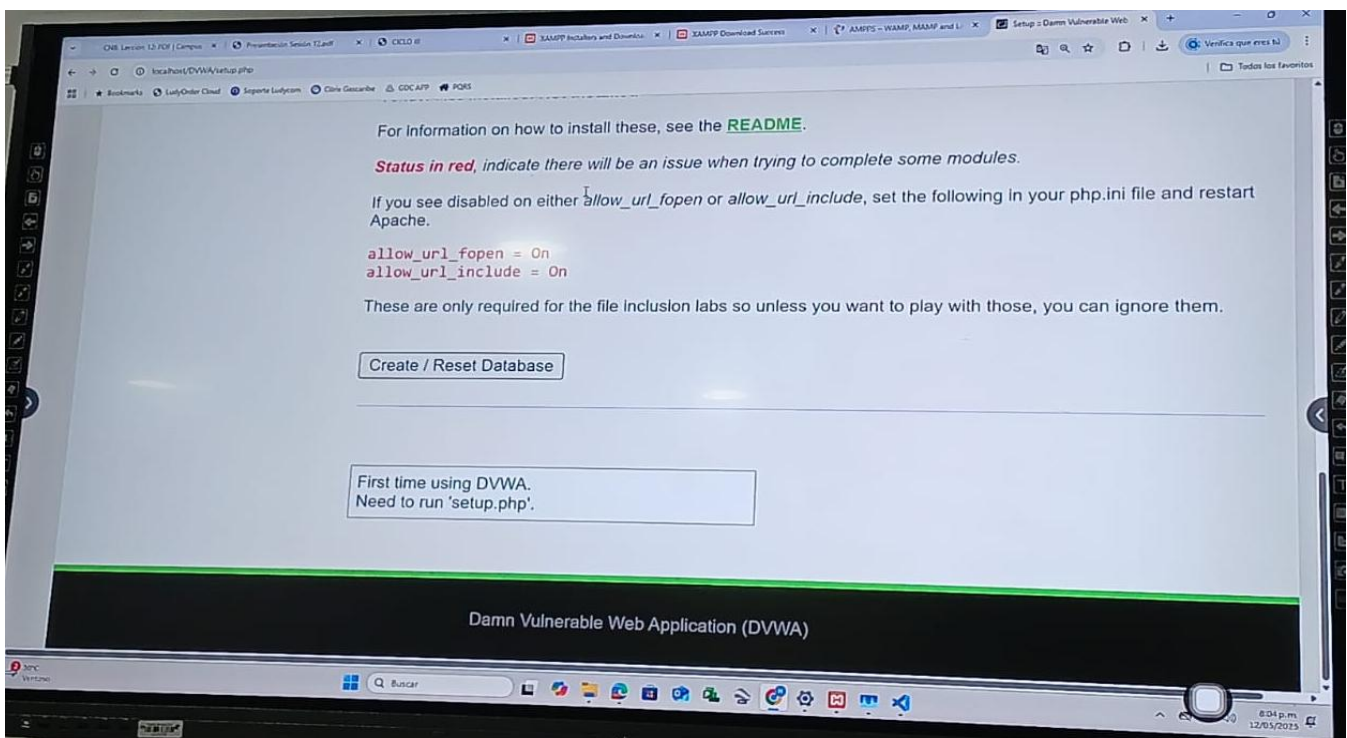
Ahora comprobamos si el usuario ya se ha creado

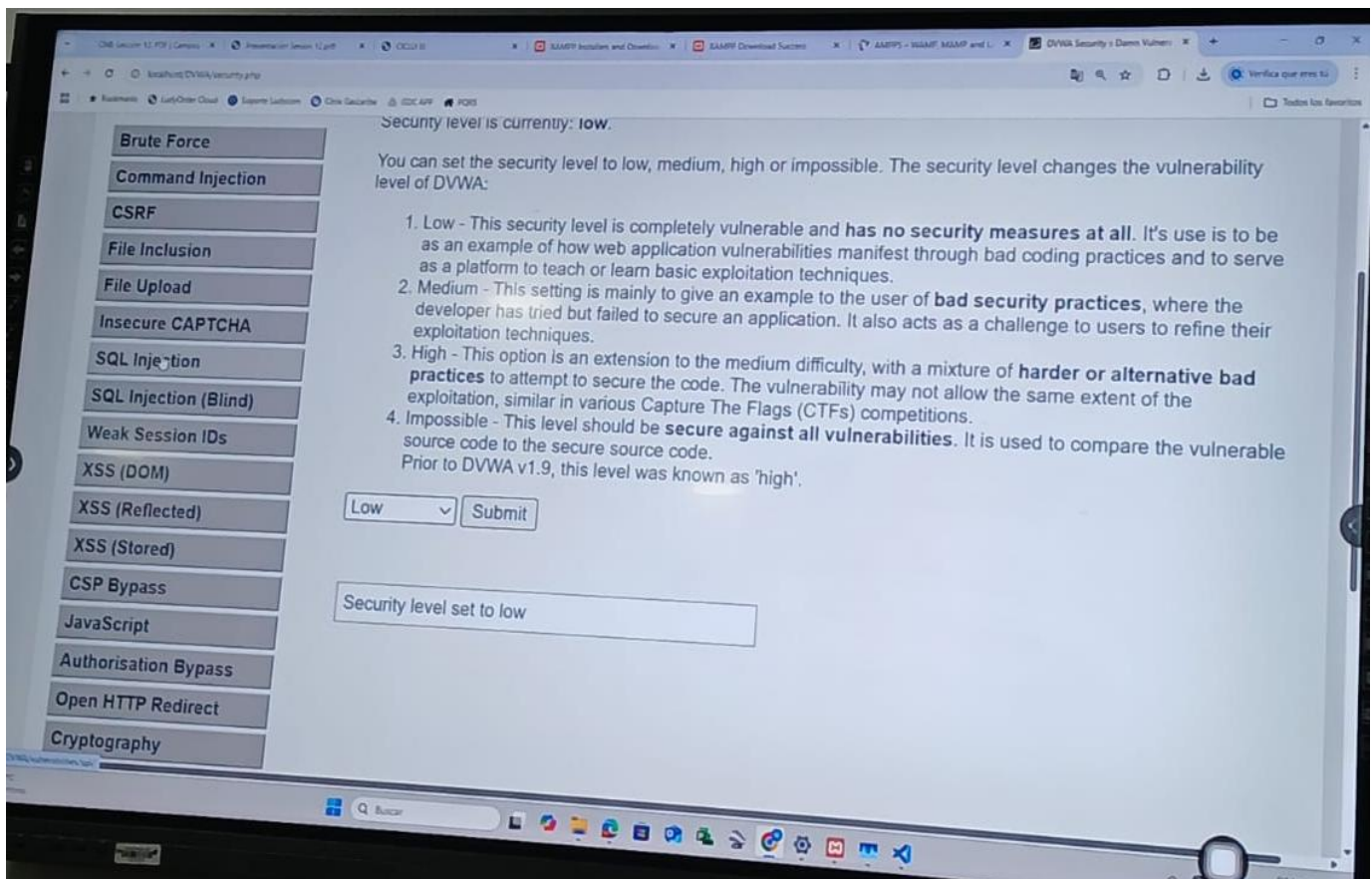
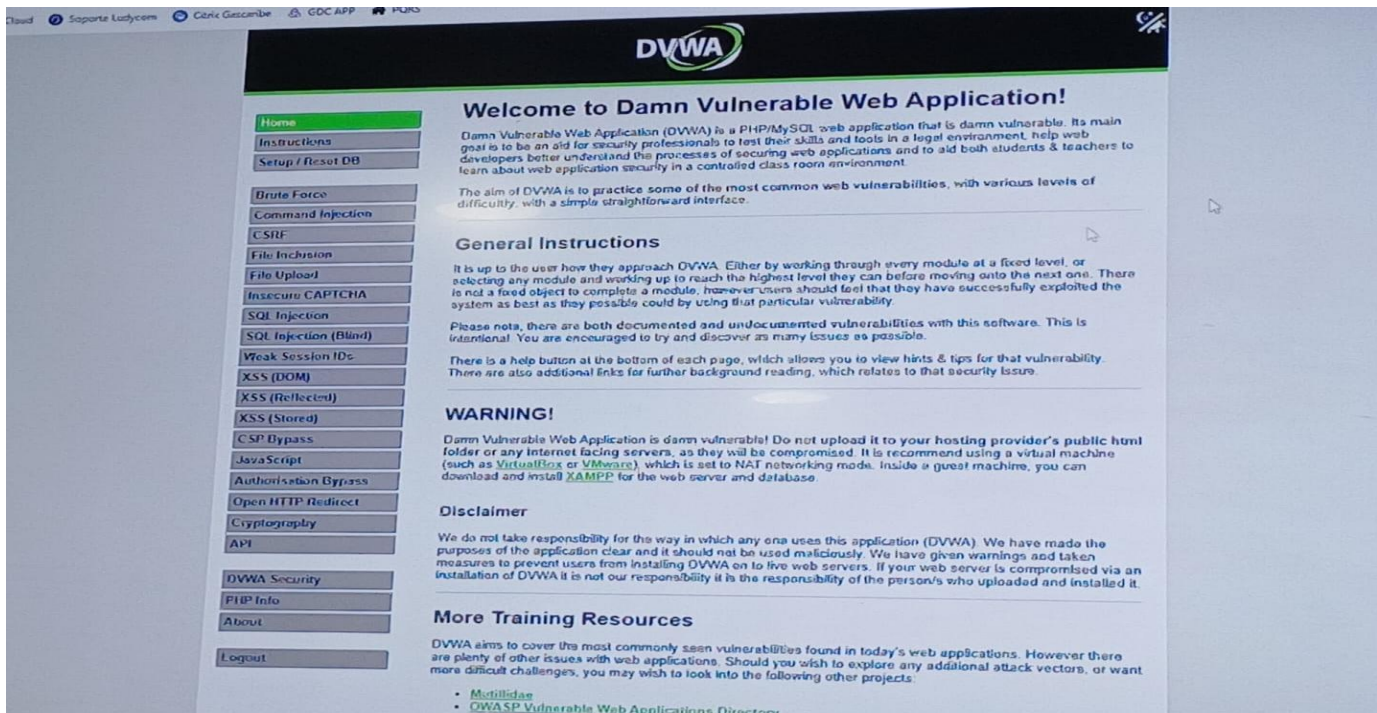


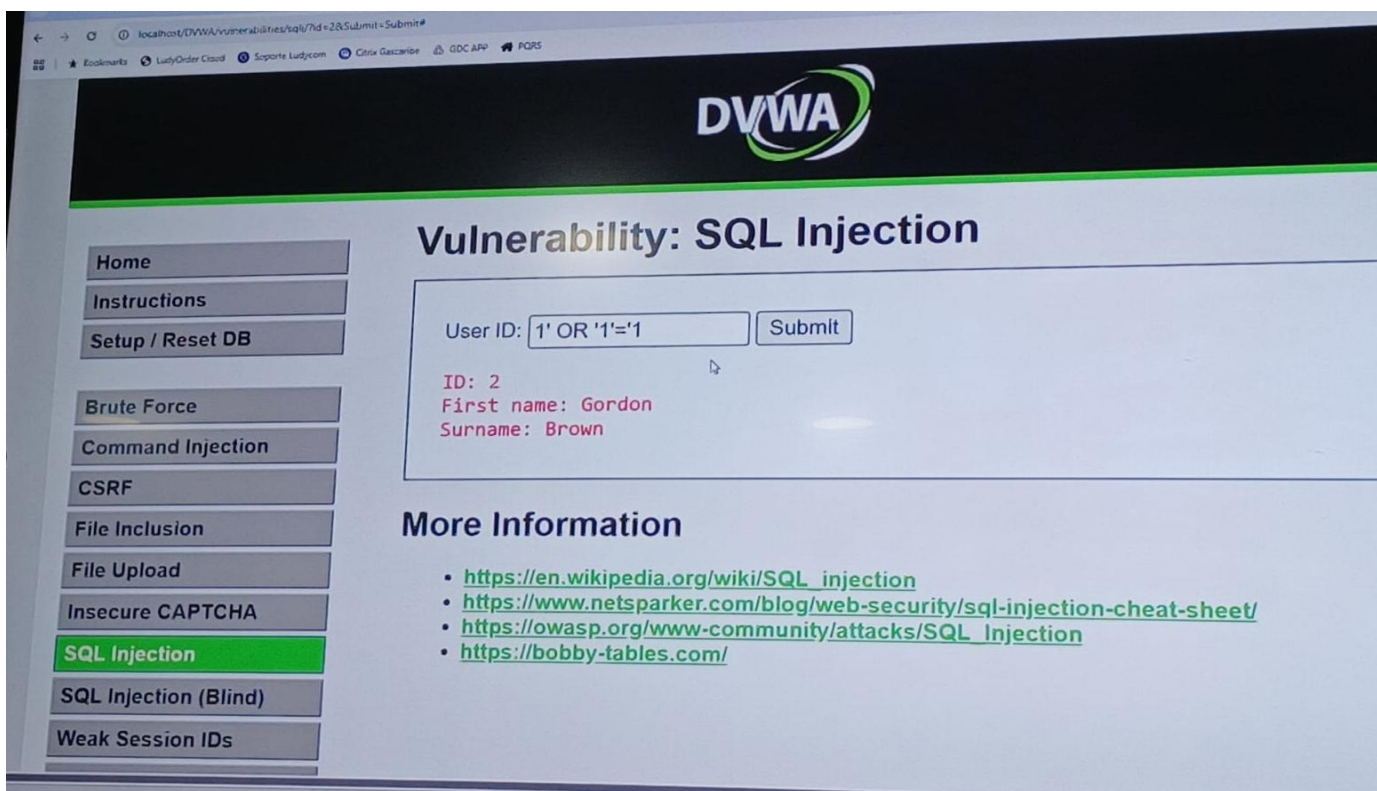
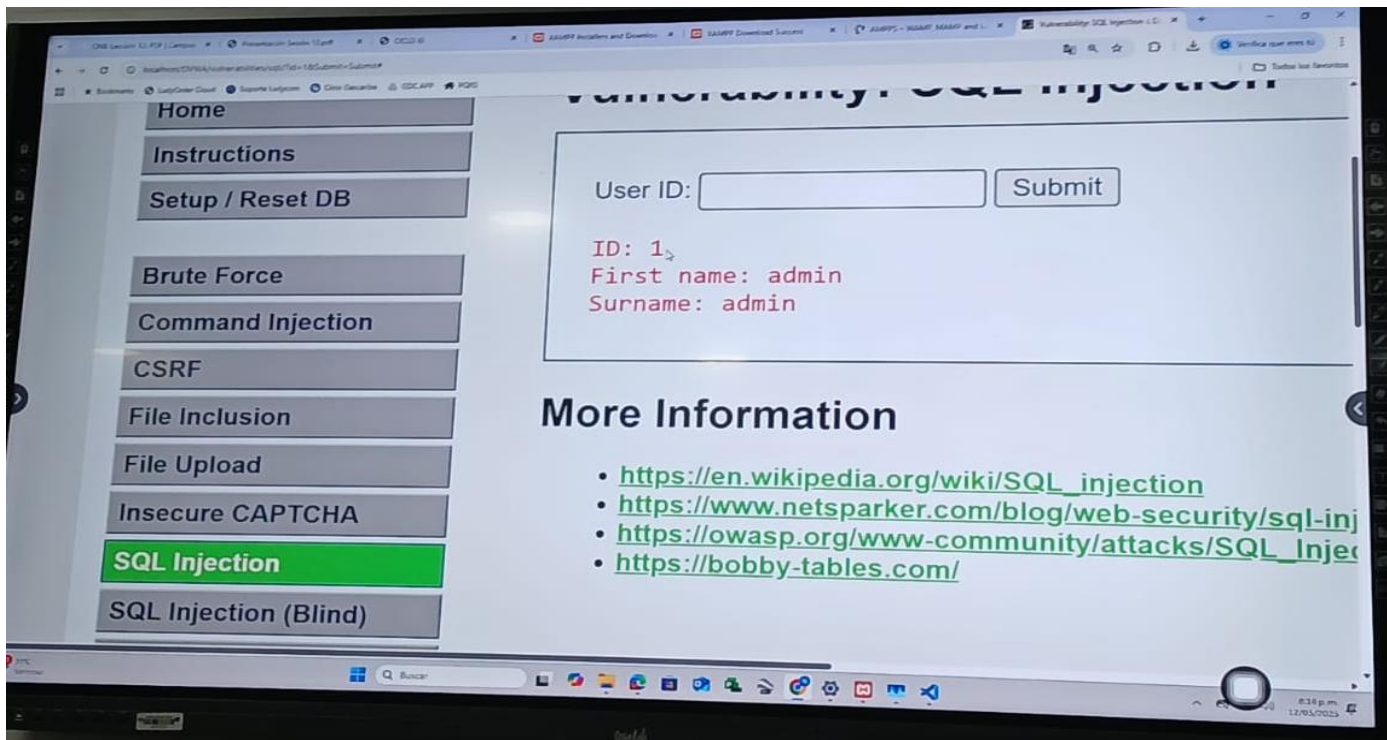
Ahora vamos a la pagina de DVWA para ingresar

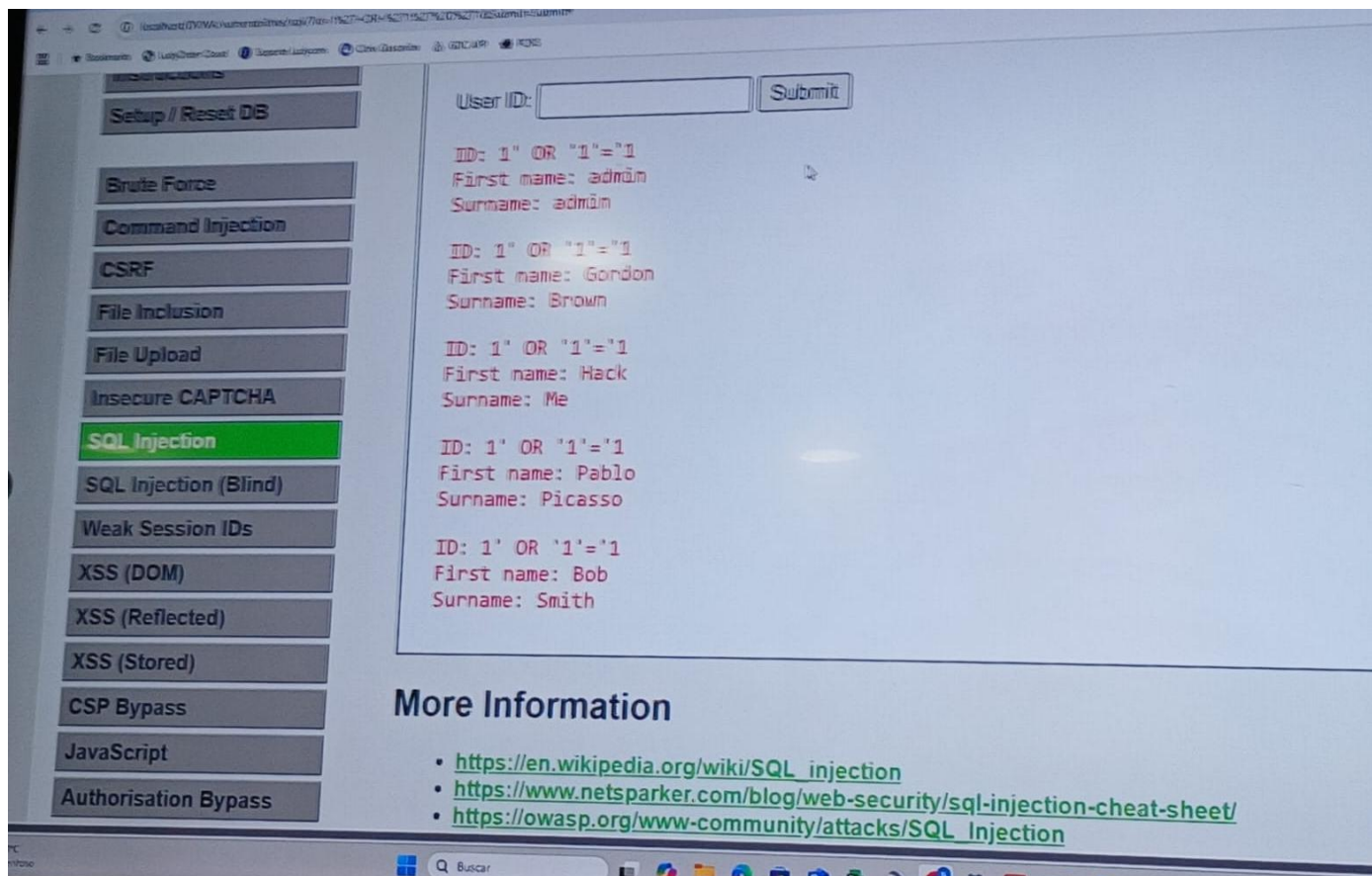


El usuario es admin y la contraseña es password









CONCLUSIÓN

La realización de este laboratorio representó una experiencia fundamental para afianzar mis conocimientos prácticos en ciberseguridad, específicamente en el área de identificación y análisis de vulnerabilidades. Trabajar con herramientas como XAMPP y DVWA me permitió configurar un entorno de pruebas funcional y seguro, ideal para explorar de manera controlada cómo se presentan, detectan y mitigan diversas fallas de seguridad en aplicaciones web.

Uno de los aspectos más valiosos de este laboratorio fue poder visualizar cómo un atacante real podría aprovecharse de fallas comunes que, muchas veces, se pasan por alto en el desarrollo o mantenimiento de aplicaciones. Además, discutir e investigar sobre posibles medidas de mitigación me ayudó a tener una visión más completa del ciclo de seguridad: desde la detección hasta la solución de las vulnerabilidades.

También pude reflexionar sobre la importancia de mantener actualizado el software, aplicar buenas prácticas de codificación segura y establecer políticas de seguridad claras y aplicables en una organización. El laboratorio no solo reforzó mis habilidades técnicas, sino también mi capacidad de análisis, razonamiento ético y toma de decisiones enfocadas en la prevención.