DVWA Local Setup Project

Project Overview:

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to aid security professionals in testing their skills and tools in a legal environment.

Setup Environment:

- OS: Kali Linux
- Web Server: Apache2
- Database: MariaDB/MySQL
- Language: PHP 8.4.5
- Tools: DVWA, git, phpmyadmin (optional)

Steps Taken:

1. Installed necessary packages (apache2, mariadb-server, php, php-mysqli, git)
2. Cloned DVWA from GitHub: https://github.com/digininja/DVWA.git
3. Copied and configured config.inc.php with database credentials
4. Created database and user with necessary privileges:
   - Database: dvwa
   - User: dvwauser
   - Password: p@ssw0rd
5. Enabled required PHP settings and Apache modules
6. Restarted Apache2 and accessed DVWA via http://localhost/DVWA
7. Clicked 'Create / Reset Database' on DVWA setup page

Configuration Example (config.inc.php):

```
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'dvwauser';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';
```

Troubleshooting:

- Fixed "mysqli_connect(): Connection refused" by correcting DB credentials and permissions
- Resolved "Access denied for user" by granting privileges and flushing them
- Verified Apache and PHP configurations (mod_rewrite, display_errors, etc.)
- Ensured MySQL was listening on the correct port

Next Steps:

- Integrate DVWA logs with Splunk for monitoring
- Add Wazuh agent to the system for threat detection
- Explore vulnerabilities through DVWA modules (SQLi, XSS, etc.)