# Exploitation Guide for Vulnerable Dash Application

## SQL Injection Exploitation

1. Navigate to the SQL Injection page.  
2. Enter the following payload in the username field: ' OR '1'='1  
3. Enter any password and click the login button.  
4. Observe that the application logs in without verifying credentials.

## Cross-Site Scripting (XSS) Exploitation

1. Navigate to the XSS page.  
2. Enter the following payload in the comment field: <script>alert('XSS');</script>  
3. Click the submit button.  
4. Observe that the alert box is triggered, indicating successful XSS.

## File Upload Exploitation

1. Navigate to the File Upload page.  
2. Upload a malicious file (e.g., a file with .exe extension or containing a payload).  
3. Observe that the application accepts the file without validation.

## Notes

Ensure to run this application in a controlled environment. Do not deploy this application in a production environment due to the presence of vulnerabilities.