**Main Objective: Highlight all sensitive information**

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

Both the login.php?-s file and the config.inc.php~ files are both leaking sensitive information about post calls and error messages. In addition to all the database information.

Ensuring we test each php file with a “~” is important as those are usually how IT teams mark backups which they may forget to backup.

Directories sensitive information found:

172.16.1.109/dvwa/login.php?-s

172.16.1.109/dvwa/config.inc.php~

Extra Information:

PHP Credits may provide version information which is beneficial for attackers

A change log can give a attacker an idea of what systems are being used

Step 1: go to site and perform scan

A screenshot of a computer

Description automatically generated

Step 2: perform scan

A screenshot of a computer

Description automatically generated

Step 3: Search all directories

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Step 4: Test php files for ~ after themA screenshot of a computer

Description automatically generated