SIAKAD

1. DASAR

```
<?php
function gagal() {
   echo $_err = ErrorMsg("Login Gagal", "Login dan Password yang Anda masukkan tidak valid.<br>
      Hubungi Administrator untuk informasi lebih lanjut.<hr size=1 color=black>
      Pilihan: <a href='?nme=$_REQUEST[nme]&mnux=login&lid=$_REQUEST[lid]&lgn=frm'>Login</a> | <a
href='?mnux='>Kembali</a>");
}
function berhasil() {
  global $_ProductName, $_Version;
// Tampilkan welcome
  TampilkanJudul("Selamat Datang");
  echo Konfirmasi("Selamat Datang", "Selamat datang di $_ProductName<hr size=1 color=silver>
    Nama : <b>$_SESSION[_Nama]</b><br>
    LevelID : <b>$_SESSION[_LevelID]</b><br>
    Institusi : <b>$_SESSION[_KodeID]</b><br>
    <hr size=1>
    Pilihan: <a href='?slnt=loginprc&slntx=lout'>Logout</a>");
}
function cek() {
  global $arrID;
  $_tbl = GetaField('level', 'LevelID', $_REQUEST['lid'], 'TabelUser');
  $Institusi = $_REQUEST['institusi'];
  $s = "select * from $_tbl where Login='$_REQUEST[Login]' and KodeID = '$_REQUEST[institusi]' and NA = 'N' and
Password=LEFT(PASSWORD('$_REQUEST[Password]'),10) limit 1";
  $r = _query($s);
  $_dat = _fetch_array($r);
  if (empty($_dat)) {
    $_SESSION['mnux'] = 'login';
    $_REQUEST['lgn'] = 'gagal';
  }
  else {
    $sid = session_id();
    // Set Parameter
    $_SESSION['_Login'] = $_REQUEST['Login'];
    $_SESSION['_Nama'] = $_dat['Nama'];
    $_SESSION['_TabelUser'] = $_tbl;
    $_SESSION['_LevelID'] = $_REQUEST['lid'];
    $_SESSION['_Session'] = $sid;
    $_SESSION['_Superuser'] = $_dat['Superuser'];
    $_SESSION['_ProdiID'] = $_dat['ProdiID'];
    $_SESSION['KodeID'] = $Institusi;
    $_SESSION['_KodeID'] = $Institusi;
    $_SESSION['mnux'] = 'login';
    $_REQUEST['lgn'] = 'berhasil';
  }
}
function lout() {
  ResetLogin();
  $_SESSION['mnux'] = 'logout';
}
?>
```

2. Kelemahan

```
$s = "select * from $_tbl where Login='$_REQUEST[Login]' and KodeID = '$_REQUEST[institusi]'
and NA = 'N' and Password=LEFT(PASSWORD('$_REQUEST[Password]'),10) limit 1";
$r = _query($s);
$_dat = _fetch_array($r);
if (empty($_dat)) {
$_SESSION['mnux'] = 'login';
$_REQUEST['lgn'] = 'gagal';
}
```

3. Cara mengatasi

a. Hindari penggunaan tanda petik tunggal (‘) dengan menggunakan fungsi REPLACE, seperti dibawah ini:

p_strUsername = Replace(Request.Form(“txtUsername”), “‘”, “””)
p_strPassword = Replace(Request.Form(“txtPassword”), “‘”, “””)

b. Mengganti Error message (yang default)
c. Batasi hak akses