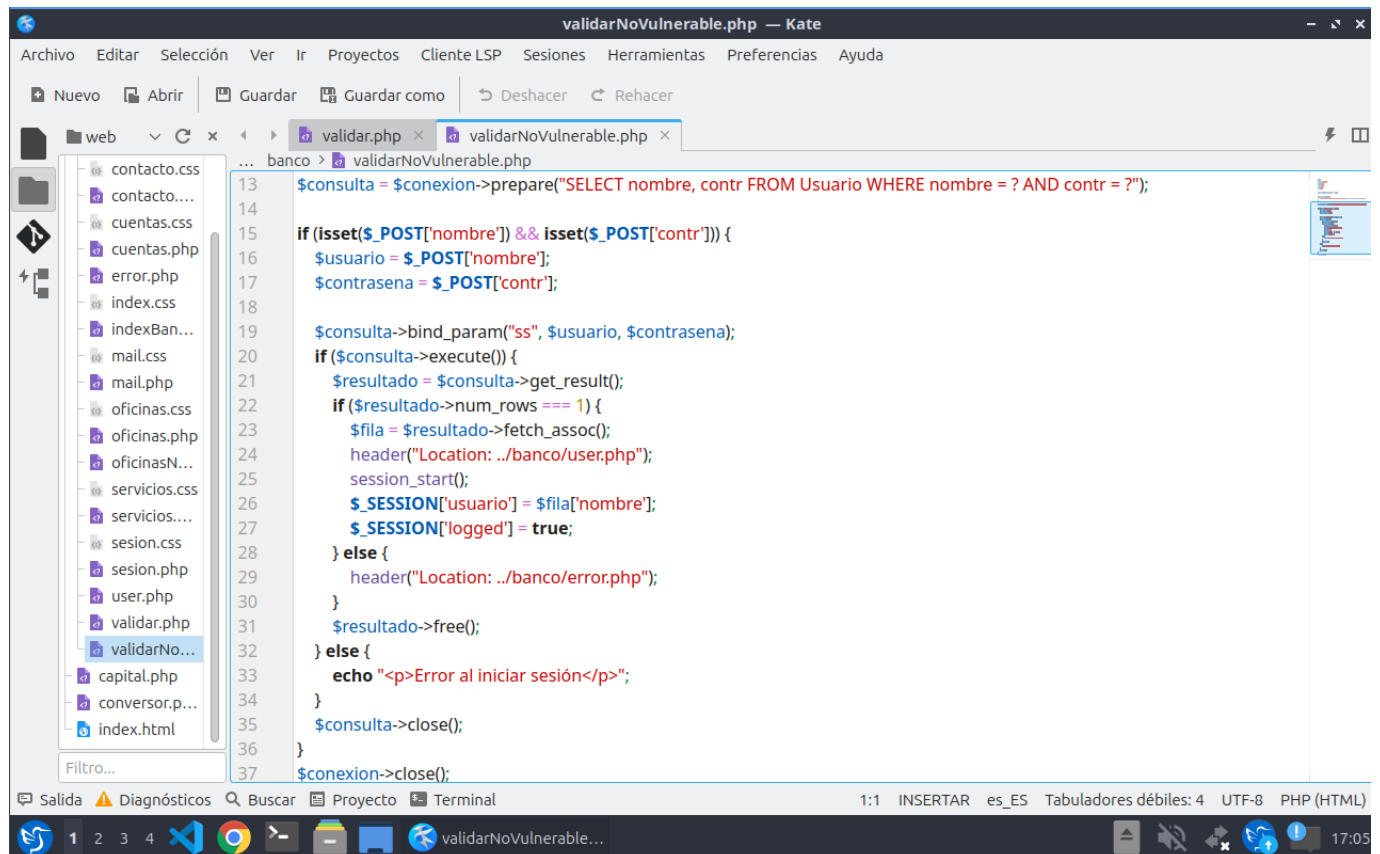


Práctica 14 - "Sanitizando"

Mediante información obtenida en Internet, etc.; realizad las tareas y contestad las preguntas que se plantean.

1. Sanitizad la aplicación WEB de la práctica 12 utilizando consultas parametrizadas.

- *Consulta parametrizada Validar*



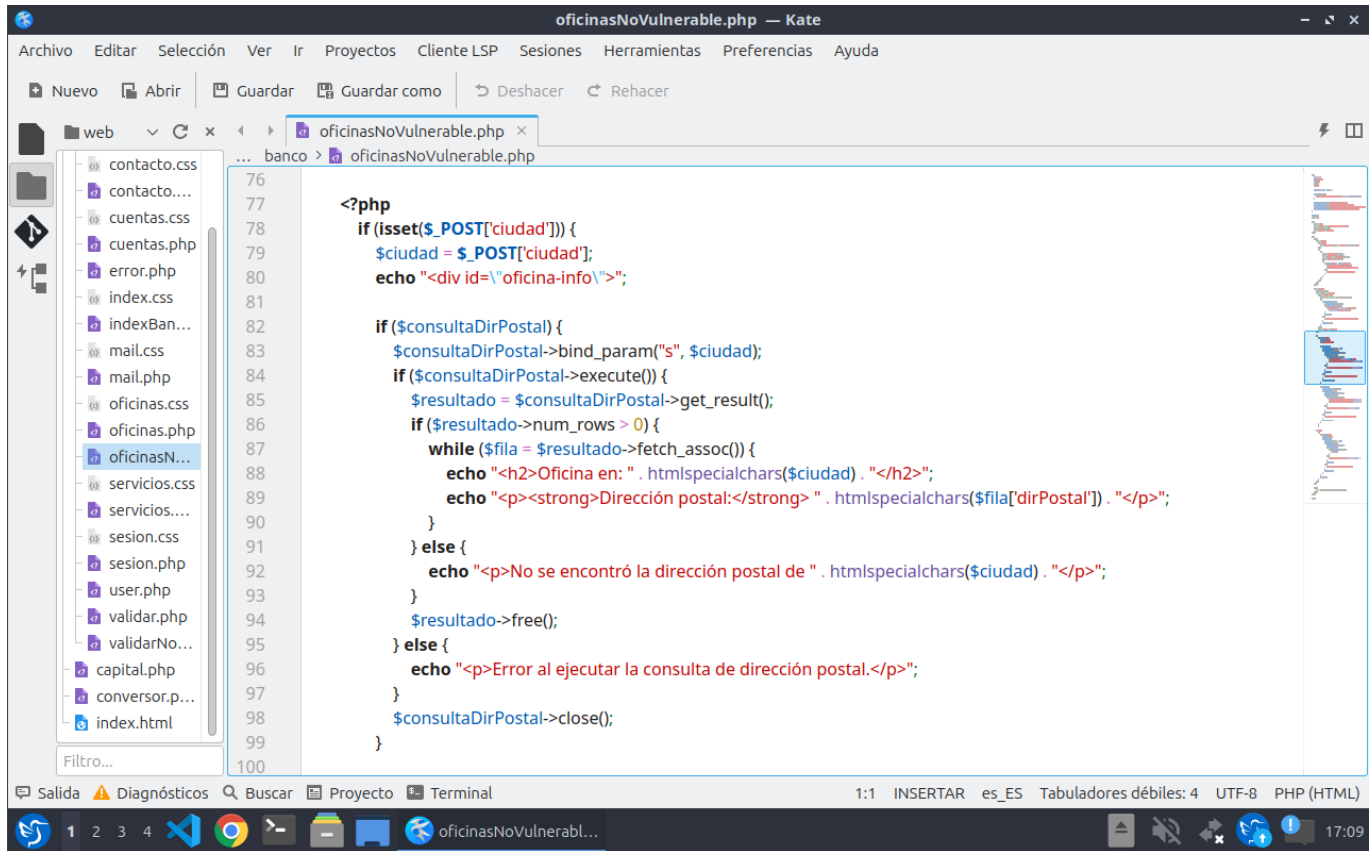
The screenshot shows a code editor window titled "validarNoVulnerable.php — Kate". The editor displays a PHP script for validating a user login. The script uses a parametrized query to prevent SQL injection. The code is as follows:

```
13 $consulta = $conexion->prepare("SELECT nombre, contr FROM Usuario WHERE nombre = ? AND contr = ?");
14
15 if (isset($_POST['nombre']) && isset($_POST['contr'])) {
16     $usuario = $_POST['nombre'];
17     $contrasena = $_POST['contr'];
18
19     $consulta->bind_param("ss", $usuario, $contrasena);
20     if ($consulta->execute()) {
21         $resultado = $consulta->get_result();
22         if ($resultado->num_rows === 1) {
23             $fila = $resultado->fetch_assoc();
24             header("Location: ../banco/user.php");
25             session_start();
26             $_SESSION['usuario'] = $fila['nombre'];
27             $_SESSION['logged'] = true;
28         } else {
29             header("Location: ../banco/error.php");
30         }
31         $resultado->free();
32     } else {
33         echo "<p>Error al iniciar sesión</p>";
34     }
35     $consulta->close();
36 }
37 $conexion->close();
```

The script includes a menu bar with options like Archivo, Editar, Selección, Ver, Ir, Proyectos, Cliente LSP, Sesiones, Herramientas, Preferencias, and Ayuda. A sidebar on the left shows a file explorer with various files and folders. The bottom status bar indicates the current line (1:1), column (INSERTAR), encoding (es_ES), tab settings (Tabuladores débiles: 4), and file encoding (UTF-8, PHP (HTML)).

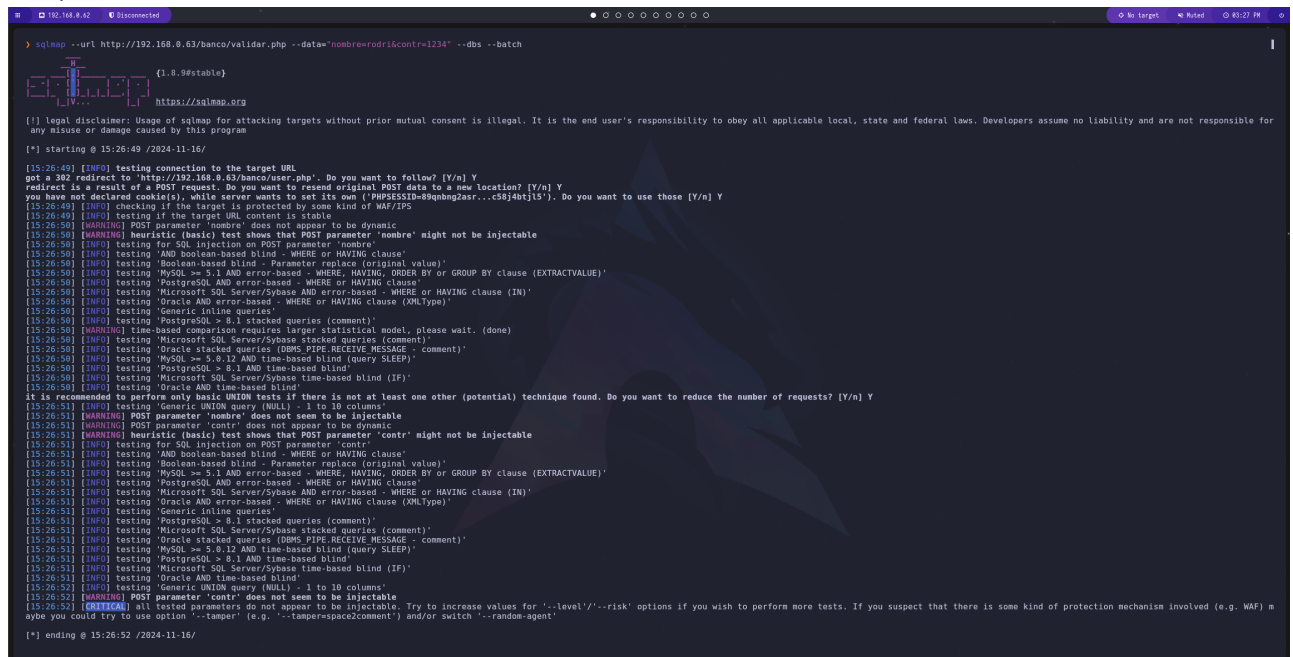
- *Consulta parametrizada Oficinas*

```
$consultaNombre = $conexion->prepare("SELECT nomCiudad FROM Oficinas");
$consultaMapa = $conexion->prepare("SELECT mapa FROM Oficinas WHERE nomCiudad = ?");
$consultaHorario = $conexion->prepare("SELECT horarioApertura, horarioCierre FROM Horario WHERE nomCiudad = ?");
$consultaDirPostal = $conexion->prepare("SELECT dirPostal FROM Oficinas WHERE nomCiudad = ?");
```



2. Comprobad el resultado de la sanitización con SQLmap.

• Ataque Validar



3. En cuanto al despliegue de la base de datos se recomienda que pertenezca a un usuario que tenga acceso sólo a dicha base de datos.

• Creación de usuario

```
CREATE USER 'areaClientes'@'localhost' IDENTIFIED BY 'areaClientes1234';
```

```
mysql> CREATE USER 'areaClientes'@'localhost' IDENTIFIED BY 'areaClientes1234';
```

- *Concesión de permisos*

```
GRANT SELECT ON BANCO.Usuario TO 'areaClientes'@'localhost';  
GRANT SELECT ON BANCO.Cuentas TO 'areaClientes'@'localhost';
```

```
mysql> GRANT SELECT ON BANCO.Usuario TO 'areaClientes'@'localhost';  
Query OK, 0 rows affected (0,00 sec)
```

```
mysql> GRANT SELECT ON BANCO.Cuentas TO 'areaClientes'@'localhost';  
Query OK, 0 rows affected (0,00 sec)
```

- *Conexión con el usuario creado*

