

Application PHP vulnérable (détection injection sql)

```
<?php
$conn = new mysqli("localhost", "root", "", "vulnapp");

if ($conn->connect_error) {
    die("Connexion échouée : " . $conn->connect_error);
}

if (isset($_GET['username'])) {
    $username = $_GET['username'];

    // Requête SQL vulnérable sans échappement ni guillemets autour de la
variable
    $sql = "SELECT * FROM users WHERE username = $username";

    $result = $conn->query($sql);

    if ($result && $result->num_rows > 0) {
        echo "Utilisateur trouvé !";
    } else {
        echo "Aucun utilisateur trouvé.";
    }
} else {
    echo "Utilisez /login.php?username=...";
}

$conn->close();
?>
```