Sure! Let’s go through this code line-by-line so you fully understand what’s happening:

**✅ Full Code Breakdown**

<?php

* Opens the PHP tag to start scripting.

include '../includes/auth.php';

* This includes the authentication script.
* It likely contains functions for verifying logged-in users or roles.

checkRole('admin');

* This function ensures **only users with the "admin" role** can access this script.
* If a non-admin tries to run it, they’ll probably be redirected or shown an error.
* This is **role-based access control** – very important for protecting sensitive actions like deletions.

include 'config.php';

* This includes your **database configuration file**.
* It usually contains the connection setup like:
* $conn = new mysqli("localhost", "username", "password", "database");

if (isset($\_GET['id']) && is\_numeric($\_GET['id'])) {

* Checks if there is a GET parameter named id **AND** it is numeric.
* is\_numeric() helps prevent malicious string input (like SQL injection).
* Example safe URL: delete\_student.php?id=7

$id = $\_GET['id'];

* Stores the student ID in a variable.

$stmt = $conn->prepare("DELETE FROM students WHERE student\_id = ?");

* Prepares a **parameterized SQL query**.
* The ? is a placeholder for the actual value.
* This prevents **SQL injection** by separating the query from the data.

$stmt->bind\_param("i", $id);

* Binds the $id variable to the ? placeholder.
* "i" means the parameter is an **integer**.
* If it was a string, you'd use "s" instead.

$stmt->execute();

* Executes the SQL statement, which deletes the student with the matching student\_id.

$stmt->close();

* Closes the prepared statement to free up resources.

}

* Ends the if block – no deletion will happen unless id is present and numeric.

header("Location: manage\_students.php");

exit();

* After the operation, the user is **redirected** to the student management page.
* exit() ensures no further code is run after the redirect.

**🔐 Security & Best Practices Used**

| **Technique** | **Purpose** |
| --- | --- |
| checkRole('admin') | Prevents unauthorized access |
| isset() & is\_numeric() | Basic input validation |
| prepare() + bind\_param() | Prevents SQL injection |
| header() redirect | Keeps user experience smooth and avoids double submissions |

**❓ Want to Improve Further?**

* ✅ Add a **confirmation prompt** before deletion (in the frontend).
* ✅ Add **logging** (e.g., log which admin deleted which student).
* ✅ Add a flash message like: Student deleted successfully ✅ after redirect.

Let me know if you want to implement those!