# Threat Analysis

| STRIDE Category | Threat Scenario | Potential Impact | Mitigation |
|---|---|---|---|
| **Spoofing Identity** | A malicious user pretends to be a student or admin to access results or modify data. | Unauthorized access to exam results or admin functions. | Strong authentication (username + password), 2FA for admin, secure session tokens. |
| **Tampering** | An attacker modifies exam results in the database or alters HTTP requests to change data. | Data integrity loss, wrong results shown to students. | Use prepared statements, input validation, database access controls, HTTPS. |
| **Repudiation** | Users or admins deny performing actions, like uploading or changing results. | Accountability loss; difficult to audit. | Maintain secure logs with timestamps and user IDs; digital signatures for admin actions. |
| **Information Disclosure** | Sensitive student data (marks, personal info) is leaked via insecure session or SQL injection. | Privacy breach, potential legal issues. | HTTPS, secure cookies, session expiration, access control checks, input sanitization. |
| **Denial of Service (DoS)** | Flooding login page or result queries to make the portal unavailable. | Students cannot access results; service disruption. | Rate limiting, CAPTCHA, server resource monitoring, scaling with Kubernetes. |
| **Elevation of Privilege** | A student gains admin privileges through flaws (e.g., parameter tampering, session hijacking). | Unauthorized modification of results, data corruption. | Role-based access control, session regeneration, server-side authorization checks. |