**Risk Assessment-**

**Identified Risks**

1. **Registration Form**- **Lack of CAPTCHA or Rate Limiting:**

Automated bots can flood the registration system, potentially leading to denial of service (DoS) attacks or the creation of fake registrations. This can disrupt the availability of the system and lead to resource exhaustion. Automated tools for such attacks are readily available and easy to deploy.

1. **Schedule Access**- **Publicly Accessible Information:**

Unauthorised users might access the conference schedule, though this is generally low risk. The conference schedule typically does not contain sensitive information. Most users do not benefit significantly from unauthorised access to the schedule.

1. **Session Materials- Predictable URL Patterns:**

Unauthorised users can easily guess URLs and download session materials without registration. Intellectual property and exclusive content might be freely accessible. Predictable URLs make it easy for unauthorised users to guess and access files.

1. **Admin Panel- Basic Login Form:**

The admin panel is only protected by a username and password, making it vulnerable to brute force attacks. Unauthorised access to the admin panel can lead to significant data breaches, manipulation of registration data, and disruption of the conference schedule. Without additional security measures, brute force attacks can easily be automated.

**Security Improvement-**

**Recommendations**

1. **Registration Form- Implement CAPTCHA:**

Add CAPTCHA (e.g., Google reCAPTCHA) to the registration form to prevent automated bot submissions. Reduces the risk of automated registrations and DoS attacks. Implement rate limiting to restrict the number of registrations attempts from a single IP address. Mitigates the risk of brute force attacks and resource exhaustion.

1. **Schedule Access**

The risk associated with schedule access is low, and no sensitive information is typically exposed.

1. **Session Materials- Secure URLs:**

Implement token-based access to session materials. Each registered user receives a unique, time-limited token to access materials. Prevents unauthorised access by ensuring only registered users can download materials. Ensure that session materials are stored in a directory that requires authentication for access. Adds an additional layer of security, ensuring materials are not publicly accessible.

1. **Admin Panel-**

* **Multi-Factor Authentication (MFA):**

Implement MFA for the admin login to require an additional verification step. Significantly increases security by making it more difficult for attackers to gain access with stolen credentials.

* **Rate Limiting:**

Apply rate limiting to the admin login attempts to prevent brute force attacks. Reduces the likelihood of successful brute force attacks.

* **IP Whitelisting:**

Restrict access to the admin panel by whitelisting trusted IP addresses. Limits access to the admin panel to only known and trusted IP addresses.

* **Secure Password Policies:**

Enforce strong password policies (minimum length, complexity requirements, regular password changes). Reduces the risk of compromised passwords.

By following these recommendations, the security of the online conference registration system can be significantly improved, reducing the risk of unauthorised access and potential data breaches. Implementing these measures will protect both the users' personal information and the conference's intellectual property.