|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Threat** | **Impact** | **Security Policies compromised** | **Vulnerability** | **Asset and consequences** | **Risk (Low, Moderate, and High)** | **Counter measure** |
| Spoofing Indentity | Website spoofing | Authentication | Having an easily forgotten domain name and simplistic UI design that can be copied easily | Website.  The emails and passwords of customers and operators can be stolen and used to manipulate data in the airline reservation system while masquerading as the stolen customer or operator | Moderate | Two-factor authentication with the user’s email |
| Man-in-the-middle attack | Authentication, Confidentiality | Exchanging public keys instead of using certificate authority | Data  The threat agent can listen to data such as account information (email and password), ticket information, and so on | Moderate | Use certificate authority |
| Tampering | Password cracking | Integrity | No password limits and no captcha during login. | User accounts  Accounts can be stolen | High | Add captcha for login page and advise a stronger password during registration |
| URL query strings | Integrity | Sensitive information is displayed in the URL such as ids. | User information  User information can be displayed in the URL and accessed by typing in the URL | Moderate | Encode the sensitive information in the URL |
| Denial of Service | DDoS attack | Availability | Firewall is not properly configured to prevent DDoS attacks | Website  The website will be unavailable | High | Configure the firewall to prevent DDoS attacks and monitor the firewall |
| Tampering, Information Disclosure, Elevation of Priveleges | SQL injection | Integrity Confidentiality, Authorization | Preventions for SQL injections were applied | Database  The database can be manipulated | High | Keep the query separate from the database and use prepared statements |