|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **SQL Injection** | **Risk Rating**: High |
| **Description** | SQL Injection is an attack technique used to exploit applications that construct SQL statements from user supplied input. When successful, the attacker is able to change the logic of SQL statements executed against the database. | |
| **Affected Path(s)** | https://apobmms.cgg.gov.in/contactUs.do?status=track | |
| **Impact** | A wide range of damaging attacks can be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database and taking control of the database server. | |
| **Evidence/Proof of Concept**  Step 1: Access the below URL .  URL: https://apobmms.cgg.gov.in/contactUs.do?status=track any reference number and capture the request after submitting t as shown in image.  1.png  2.png  Step 2: Now inject the SQL injection payload in the reference number feild and submit request as shown in image:  3.png  Step 2: After injecting the payload instead of retrieving one record all the records has been retrieved as shown in image:  Screenshot_2019-12-16 Andhra Pradesh State OBMMS - CGG.png | | |
| **Recommendation** | 1. This is a critical vulnerability to have on a web application and should be addressed immediately. User controllable data should be validated before any queries are performed on the database using the data. Blacklisting is an approach which consists of checking the input data for malicious characters but a more effective approach is whitelistng. Whitelistng consists of only allowing certain characters to be submitted. For example checking if data submitted is alphanumeric and rejecting the request if it is not. Many libraries exist, such as built-in libraries for programming languages and open-source libraries, which can assist you in preventing this vulnerability. | |
| **Management Comments** |  | |