|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **SQL injection** | **Risk Rating**: High |
| **Description** | SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server. | |
| **Affected Path(s)** | <http://labour.ap.gov.in:8080/misreportslogin.php>  <http://labour.ap.gov.in:8080/inspectionportal/get_view_details.php>  <http://labour.ap.gov.in:8080/jointinspectionslist.php>  http://labour.ap.gov.in:8080/jointinspectionslist.php | |
| **Impact** | An attacker can use SQL injection it to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQLi can also be used to add, modify and delete records in a database, affecting data integrity. Under the right circumstances, SQLi can also be used by an attacker to execute OS commands, which may then be used to escalate an attack even further. | |
| **Evidence/Proof of Concept**  **Step 1:**By injecting the payload in the username field the sql error is generating  sql injection 1.png  **Step 2:** By giving the command order by, we can confirm the number of columns.  **sql injection1.png**  **sqlinjection2.png** | | |
| **Recommendation** | Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allows the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection  Reference Links:  https://dzone.com/articles/aspnet-preventing-sql-injectio  https://www.aspsnippets.com/Articles/SQL-Injection-Attack-its-examples-and-Prevention-mechanisms-and-Techniques-in-ASPNet.aspx  https://stackoverflow.com/questions/305044/how-can-i-avoid-sql-injection-attacks-in-my-asp-net-application | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Directory Listing** | **Risk Rating**: Medium |
| **Description** | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. | |
| **Affected Path(s)** | /(web server) | |
| **Impact** | A user can view a list of all files from this directory possibly exposing sensitive information. | |
| **Evidence/Proof of Concept:**  **Step 1:** Directories are being enumerated for the application as shown below.  **directorylisting.png** | | |
| **Recommendation** | **Type 1:**  For Apache you need to edit the Apache configuration file (usually named httpd.conf) or create an .htaccess file. In the configuration file you will have the definition of the directory. Something like  <Directory /directory name/subdirectory> Options Indexes FollowSymLinks ... </Directory>  To disable directory listing for that directory you need to remove the 'Indexes' option.  **Type 2:**  Disable directory browsing by using web.Config  Reference Links:  Refer:  https://stackoverflow.com/questions/9806446/disable-directory-listing-in-iis  https://forums.asp.net/t/1338177.aspx?How+can+I+disable+directorylisting | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Improper Error Handling** | **Risk Rating**: Low |
| **Description** | 1. The application is not configured to display any generic error message rather it displays the application version details. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker | |
| **Affected Path(s)** | http://labour.ap.gov.in:8080/insp\_mediumrisk\_est\_excel.php  http://labour.ap.gov.in:8080/getjointinspectiondata.php  http://labour.ap.gov.in:8080/individualworkerdetails.php  http://labour.ap.gov.in:8080/insp\_check\_gen\_pwd.php  http://labour.ap.gov.in:8080/insert\_compli\_action.php | |
| **Impact** | An attacker makes use of the details found to perform the concentrated attacks based on the vulnerabilities present in the current version. | |
| **Evidence/Proof of Concept**  **Step 1:**By accesing the url <http://labour.ap.gov.in:8080/inspectionportal/insp_insert_details.php> it is displaying the php error messages  improper error handling.png | | |
| **Recommendation** | Verify that this page is disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.  **Reference Links:**  https://www.c-sharpcorner.com/blogs/handling-verbose-error-messageimproper-errorhandling-in-webconfig https://stackoverflow.com/questions/4363941/asp-net-customerrors-mode-off-error-when-tryingto-access-working-webpage | |
| **Management Comments** |  | |