|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Cross site Scripting(XSS)** | **Risk Rating**: High |
| **Description** | The application is affected with this vulnerability which occurs at the client side due to the improper input validation supplied by the user. This is a code injection that includes client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. | |
| **Affected Path(s)** | https://apbcl.ap.gov.in/ap/index.php/site/login# | |
| **Impact** | An attacker can insert malicious JavaScript code that has access to cookies and local storage, which are often used to store session tokens. If an attacker can obtain a user's session cookie, they can then impersonate that user. | |
| **Evidence/Proof of Concept**  Step 1: Access the URL and click on bot symbol to open chat as shown below:  Step 2: enter the payload and submit the query as show in image.  Step 3:the pop will displayed as shown in image. | | |
| **Recommendation** | 1. • Input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain 2. • User input should be HTML-encoded at any point where it is copied into application responses. All HTML meta characters, including < > " ' and =, should be replaced with the corresponding HTML entities (&lt; &gt; etc). | |
| **Management Comments** |  | |