|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **WordPress Admin Console Available to End user** | **Risk Rating**: High |
| **Description** | The application discloses Word Press admin console to end-user and Word Press doesn’t limit the number of login attempts, so brute force attacks can be very effective. | |
| **Affected Path(s)** | 1. http://aparchmuseums.nic.in/wp-login.php | |
| **Impact** | Brute force attacks can be possible on the login page which may lead to the complete takeover of the website and can also change the design and layout of the website | |
| **Evidence/Proof of Concept**  Step1: By Accessing the URL https://www.apcob.org/wp-login.php the word press login page can be accessed as shown in the image.  Step2: Click on Register page    Step3: Enter the user name and email ID click on register user can able to register.    Step4: once successful registration user can get the email alert for the password set    Step5: Click on the link and set the password and try to login into the application. Below screenshot shows the user successfully login into the application. | | |
| **Recommendation** | 1. Disable the wordpress login page and allow only to whitelisted IPs. | |
| **Management Comments** |  | |