|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Unrestricted File upload** | **Risk Rating**: High |
| **Description** | The application fails to restrict the file types that the user uploads. The application accepted the files with the double extension when tried to upload. If tshe uploaded file contains any malicious content such as macros it may cause an adversary result in the server. | |
| **Affected Path(s)** | https://apbudget.apcfss.in/Contactus.do | |
| **Impact** | An attacker can upload the malicious files that can be used as the backdoor for the later attacks in an attempt to compromise the whole server. | |
| **Evidence/Proof of Concept**  Step 1: Access the URL and access the Contact Us:    Step 2: fill all the details and in upload a file tab select a malicious file and click submit:  Contact us.JPG  **Step 3:** After successfully submitting the details it will generate a reference number  **Submit.JPG**  **Step 4:** Now go to check query status tab and enter reference number it will feteh all the details  Submit1.JPG  Step 5: now click on attachment details it will gives the shell    Step 6: we can execute and system commands  Shell.JPG | | |
| **Recommendation** | 1. If there is no need to have Unicode characters, it is highly recommended to only accept alpha-numeric characters and only one dot as an input for the file name and the extension.  2. Don't rely only on client-side validation only.  3. Use the white list of extensions to verify the uploaded files  4. Use magic quotes for file upload validation  **Reference Links:**  https://www.aspforums.net/Threads/291996/Validate-file-extension-with-magic-number-using-C-and-VBNet-in-ASPNet/  https://stackoverflow.com/questions/2780191/how-to-restrict-file-type-in-fileupload-control  https://www.codeproject.com/Questions/886361/Prevent-double-file-Extension-file-upload-in-cshar  https://www.aspforums.net/Threads/291996/Validate-file-extension-with-magic-number-using-C-and-VBNet-in-ASPNet/ | |
| **Management Comments** |  | |