|  |
| --- |
| **Security Certificate**  (Unique Ref No: APTS/APCSP/Assurance/32/2019) |
| **Audit Performed by:** Andhra Pradesh Technology Services Ltd.  **Application Description/Name:** Meebhoomi  **Staging URL :** http://10.10.11.88:84/  **Production URL** of the web application: https://meebhoomi.ap.gov.in/  **Audit Performed by:**   1. **Name :**  APTS Security Team 2. **Email :** mgr-apcsp-apts@ap.gov.in 3. **Telephone :** 0866-2468102   **Level -01 Audit date** **:** 08-Nov-2018  **Level -02 Audit date** **:** 03-Jan-2019  **Level -03 Audit date** **:** 08-Feb-2019  **Level -04 Audit date** **:** 31-May-2019  **Level -05 Audit date** **:** 20-Jun-2019  **Level -06 Audit date** **:** 28-Jun-2019  **Level -07 Audit date** **:** 03-Sep-2019  **Issue Date :** 06-Sep-2019  **Unique Reference No. :** APTS/APCSP/Assurance/32/2019  Meebhoomi of Andhra Pradesh Web Application, auditing is completed on a Testing server with URL: http://10.10.11.88:84/.  During the initial Audit of the web application following vulnerabilities were discovered which have been successfully fixed by the development team:   1. Concurrent Logins Possible (Functionality removed while testing) 2. Unencrypted \_\_VIEWSTATE parameter 3. Weak password policy (Functionality removed while testing) 4. User credentials are sent in clear text (Functionality removed while testing) 5. Stack trace disclosure 6. Full Path Disclosure 7. Version/ Technology disclosure 8. Vulnerable JavaScript library 9. Cookie(s) without Secure flag set 10. HTTP TRACE method is enabled 11. Web Server Unconfigured - Default Install Page Present 12. Direct URL Access (Functionality removed while testing) 13. Malicious File Upload 14. vertical privilege escalation (Functionality removed while testing) 15. otp bypass 16. Session Fixation (Functionality removed while testing) 17. Improper session termination (Functionality removed while testing) 18. Browser Cache Weakness (Functionality removed while testing) 19. Improper Captcha Implementation 20. No Session time out (Functionality removed while testing) 21. Last login time not implemented (Functionality removed while testing) 22. Server Error Message 23. No Account Lockout (Functionality removed while testing) 24. Username and Password Fields with auto-complete enabled (Functionality removed while testing) 25. Content Security Policy not implemented 26. Business Logic Validation 27. Unencrypted communication 28. sensitive information disclosure   **CONCLUSION:**  Auditing for Meebhoomi of Andhra Pradesh Web Application was initiated on 08-Nov-2018 in the Testing server URL: http://10.10.11.88:84/ by Andhra Pradesh Technology Services Ltd. The initial and follow-up audits were done on the above mentioned dates and there is no pending nonconformity w.r.t OWASP Top 10, 2017 as on 06.09.2019.  Meebhoomi of Andhra Pradesh Web Application meets all the aspects of Open Web Application Security Project (OWASP) and is safe for hosting provided the recommendations are implemented. Meebhoomi of Andhra Pradesh Web Application in a secure opening environment will create an overall system that is resilient to known patterns of attack.  It is therefore our opinion that a typical user would require a sophisticated level of security attack skill to breach such a system. In this capacity, we are pleased to provide a positive rating on the security posture of Meebhoomi of Andhra Pradesh Web Application. This application is free from any known vulnerabilities as on 06.09.2019.  The web application is free from all the known vulnerabilities and is safe for hosting provided the recommendations are implemented.  **Recommendation:**   1. All SSL/TLS related issues can be addressed on the production server 2. All the above reported issues can be addressed on the production server 3. The entire application should be hosted with read only permission. 4. The application has to be tested quarterly for any vulnerability. 5. Application should be reviewed before any major update is released. 6. Patching of infrastructure and application has to be done on regular basis. 7. Admin login should be accessible through VPN only. 8. The application which is tested by the team should have application version number. 9. This certificate is valid till no modification in Meebhoomi of Andhra Pradesh Web Application is done or **six months** from the date of issue whichever is earlier.   Dr. G. Jacob Victor  Executive Director  Date: 06.09.2019 Andhra Pradesh Technology Services Ltd.  Place : Vijayawada |