|  |
| --- |
| **Security Certificate**  (Unique Ref No: APTS/APCSP/Assurance/9/2019) |
| **Audit Performed by:** Andhra Pradesh Technology Services Ltd.  **Application Description/Name:** Chief Commissioner of Land Administration.  **Staging URL :** http://ccla.ap.gov.in/CCLATEST/  **Production URL** of the web application: http://ccla.ap.gov.in/CCLA/  **Audit Performed by:**   1. **Name :**  APTS Security Team 2. **Email :** 3. **Telephone :** 0866-2468102   **Level -01 Assessment date :** 20-DEC-2018  **Level -02 Assessment date :** 08-FEB-2019  **Level -03 Assessment date :** 15-APR-2019  **Level -04 Assessment date :** 18-APR-2019  **Level -05 Assessment date :** 23-APR-2019  **Level -06 Assessment date :** 02-MAY-2019  **Issue Date :** 01-JULY-2019  **Unique Reference No. :** APTS/APCSP/Assurance/9/2019  Chief Commissioner of Land Administration, auditing is completed on a staging server with URL: http://ccla.ap.gov.in/CCLATEST/. During the initial assessment of the web application following vulnerabilities were discovered which have been successfully fixed by the development team:   1. Blind SQL Injection 2. Sensitive File Disclosure 3. Default Credentials 4. Cross-site Scripting 5. Privilege Escalation 6. Cleartext Submission of Credentials 7. File Upload with Unexpected File Type 8. Concurrent Logins Possible 9. Unencrypted \_\_VIEWSTATE parameter 10. Login Brute Force Attack 11. Partial Source Code Revealed 12. Full Path Disclosure 13. Cookie(s) without Secure flag set 14. Technology/Version Disclosure 15. Click jacking Attack 16. Vulnerable HTTP Methods 17. Information Leakage and Search Engine Discovery 18. Weak Password Policy 19. Vulnerable JQuery Version 20. Vulnerable Bootstrap Version 21. Auto Complete Off is NOT Enabled 22. Insufficient Anti Automation 23. E-mail Address Disclosure     **CONCLUSION:**  Auditing for Chief Commissioner of Land Administration Web Application was initiated on 20.12.2018 in the staging server URL: http://ccla.ap.gov.in/CCLATEST/ 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 01.07.2019.  Chief Commissioner of Land Administration Web Application meets all the aspects of Open Web Application Security Project (OWASP) and is safe for hosting provided the recommendations are implemented. Chief Commissioner of Land Administration 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 Chief Commissioner of Land Administration Web Application. This application is free from any known vulnerabilities as on 01.07.2019.  The web application is free from all the 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. The entire application should be hosted with read only permission. 3. The application has to be tested quarterly for any vulnerability. 4. Application should be reviewed before any major update is released. 5. Patching of infrastructure and application has to be done on regular basis. 6. Admin login should be accessible through VPN only. 7. The application which is tested by the team should have application version number. 8. This certificate is valid till no modification in Chief Commissioner of Land Administration Web Application is done or one year from the date of issue whichever is earlier.   Dr. G. Jacob Victor Date: 01.07.2019  Executive Director  Andhra Pradesh Technology Services Ltd.  Place : Vijayawada |