|  |
| --- |
| **Security Certificate**  (Unique Ref No: APTS/APCSP/Assurance/7/2019) |
| **Audit Performed by:** Andhra Pradesh Technology Services Ltd.  **Application Description/Name:** AP Content Corporation.  **Staging URL :** http://www.uat.apcc.ap.gov.in  **Production URL :** https://www.apcc.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 Assessment date :** 27-Dec-2018  **Level -02 Assessment date :** 04-Jan-2019  **Level -03 Assessment date :** 18-Jan-2019  **Level -04 Assessment date :** 23-Feb-2019  **Level -05 Assessment date :** 26-Mar-2019  **Level -06 Assessment date :** 13-Apr-2019  **Level -07 Assessment date :** 09-May-2019  **Level -08 Assessment date :** 30-May-2019  **Issue Date :** 24-Jun-2019  **Unique Reference No. :** APTS/APCSP/Assurance/7/2019  AP Content Corporation Web Application, auditing is completed on a staging server with URL: http://www.uat.apcc.ap.gov.in. During the initial assessment of the web application following vulnerabilities were discovered which have been successfully fixed by the development team:   1. Sensitive Information like Aadhaar, Credentials & OTP disclosure in response 2. OTP Bypass 3. Improper OTP Validation 4. Privilege Escalation 5. Concurrent Logins Possible 6. Broken Access Control 7. Sensitive Information Disclosure 8. Cross Site Request Forgery 9. User credentials are sent in clear text 10. Admin Account Credentials Enumerated 11. Unauthenticated API 12. Weak Password Policy 13. Improper Session Management 14. No account lockout policy 15. Input fields are not validated 16. No Session timeout 17. Technology/Version Disclosure 18. Cookie(s) without Secure flag 19. Clickjacking Attack 20. Internal IP Disclosure 21. Insufficent Anti-Automation 22. Improper Captcha Implementation 23. Internal File Path Disclosure 24. Database schema Disclosed 25. Improper Aadhaar ID Validation 26. User Id Disclosed in plain text 27. Improper Session Termination 28. Account lockout bypass 29. OTP flooding 30. Bypassing CAPTCHA validation 31. Password Bypass 32. Ability forge requests 33. Security Headers not enabled 34. Script src Integrity Check 35. Improper account lockout 36. Improper last login time implemented 37. Internal ip disclosure in login request     **CONCLUSION:**  Auditing for AP Content Corporation Web Application was initiated on 27.12.2018 in the staging server URL: http://www.uat.apcc.ap.gov.in 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 24.06.2019.  AP Content Corporation Web Application meets all the aspects of Open Web Application Security Project (OWASP) and is safe for hosting provided the recommendations are implemented. AP Content Corporation 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 AP Content Corporation Web Application. This application is free from any known vulnerabilities as on 24.06.2019.  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 AP Content Corporation Web Application is done or one year from the date of issue whichever is earlier.   Dr.G. Jacob Victor Date: 24.06.2019.  Executive Director  Andhra Pradesh Technology Services Ltd.  Place : Vijayawada |