|  |
| --- |
| **Security Certificate**  (Unique Ref No: APTS/APCSP/Assurance/13/2019) |
| **Audit Performed by:** Andhra Pradesh Technology Services Ltd.  **Application Description/Name:** Andhra Pradesh Non Resident Telugu Society(APNRT)  **Staging URL :** http://staging.apnrt.com, http://staging.apnrt.com/admin  **Production URL** of the web application: <https://www.apnrt.com/>, <https://www.apnrt.com/admin>  **Audit Performed by:**   1. **Name :**  APTS Security Team 2. **Email :** 3. **Telephone :** 0866-2468102   **Level -01 Assessment date :** 15-Mar-2019  **Level -02 Assessment date :** 01-Jul-2019  **Level -03 Assessment date :** 06-Jul-2019  **Level -04 Assessment date :** 08-Jul-2019  **Level -05 Assessment date :** 10-Jul-2019  **Issue Date :** 11-Jul-2019  **Unique Reference No. :** APTS/APCSP/Assurance/13/2019  APNRT Web Application, auditing is completed on a staging server with URL: http://staging.apnrt.com, http://staging.apnrt.com/admin. During the initial assessment of the web application following vulnerabilities were discovered which have been successfully fixed by the development team:   1. Unrestricted File upload 2. Cross Site Request Forgery 3. Improper Handling of Payment Redirection 4. Cross Site Scripting (XSS) 5. Broken Authentication 6. Default Credentials 7. Data Transmission in GET Method 8. File and Directory Information Exposure 9. User Credentials in Clear Text 10. Configuration File Disclosure 11. Php Info Page Disclosure 12. Admin page Disclosure 13. Default Hosting Pages Found 14. Html Injection 15. Concurrent logins 16. TRACE Method Enabled 17. Insecure Cookie Implementation 18. Improper Session Expiration 19. Improper User Validation 20. Vulnerable Bootstrap Version 21. Account lockout policy not enabled 22. Technology/ Version Disclosure 23. Insufficient Anti Automation 24. Username Auto complete enabled 25. Vulnerable jQuery Version 26. Click Jacking 27. E-mail Address Disclosure 28. Information Leakage and Search Engine Discovery 29. Weak Password Policy 30. Port Misconfiguration 31. SQL Injection 32. Client side validation bypass 33. Sensitive server directories disclosed 34. Privilege escalation 35. Insecure Direct Object References(IDOR) 36. Broken access control 37. Full path disclosure 38. Session Replay     **CONCLUSION:**  Auditing for APNRT Web Application was initiated on 15-Mar-2019 in the staging server URL: http://staging.apnrt.com, http://staging.apnrt.com/admin 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 11.07.2019.  APNRT Web Application meets all the aspects of Open Web Application Security Project (OWASP) and is safe for hosting provided the recommendations are implemented. APNRT 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 APNRT Web Application. This application is free from any known vulnerabilities as on 11.07.2019.  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. 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 ITE&C Invest –Incentive Portal Web Application is done or one year from the date of issue whichever is earlier.   Dr.G. Jacob Victor Date: 11.07.2019  Executive Director  Andhra Pradesh Technology Services Ltd.  Place : Vijayawada |