|  |
| --- |
| **Security Certificate**  (Unique Ref No: APTS/APCSP/Assurance/14/2019) |
| **Audit Performed by:** Andhra Pradesh Technology Services Ltd.  **Application Description/Name:** Ananthapuramu District Portal  **Staging URL :** http://119.226.216.91:8080/anantapuramu/login.apo  **Production URL** of the web application: [https://www.anantapuramu.ap.gov.in](http://mtrack.me/tracking/raWzMz50paMkCGHkAmplBGVmAmVzMKWjqzA2pzSaqaR9AGLjAwDjAQN0Way2LKu2pG0lZQNkBQN0BGL5ASD)  **Audit Performed by:**   1. **Name :**  APTS Security Team 2. **Email :** 3. **Telephone :** 0866-2468102   **Level -01 Assessment date :** 29-DEC-2018  **Level -02 Assessment date :** 22-FEB-2019  **Level -03 Assessment date :** 29-MAR-2019  **Level -04 Assessment date :** 30-MAR-2019  **Level -05 Assessment date :** 08-MAY-2019  **Level -06 Assessment date :** 09-MAY-2019  **Level -07 Assessment date :** 12-JUN-2019  **Level -08 Assessment date :** 17-JUL-2019  **Level -08 Assessment date :** 23-JUL-2019  **Issue Date :** 23-JUL-2019  **Unique Reference No. :** APTS/APCSP/Assurance/14/2019  Ananthapuramu District Portal, auditing is completed on a staging server with URL: http://119.226.216.91:8080/anantapuramu/login.apo. 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. Cross Site Scripting (XSS) 3. Cross Site Request Forgery (CSRF) 4. Malicious File Upload 5. Insecure Direct Object Reference (IDOR) 6. Local File Inclusion 7. Directory Traversal 8. Concurrent Logins 9. Click jacking 10. HTTP methods enabled (PUT,DELETE) 11. Sensitive Data Disclosure 12. Improper Input Validation 13. Improper Captcha Implementation 14. Internal IP Disclosure 15. Cross Domain Script Include 16. Security Headers Not Implemented 17. Username Disclosure 18. Email Address Disclosure 19. Display Last Login Time 20. Username in Clear text 21. Password in Clear text 22. Apache Tomcat Default Files 23. Technology Version Disclosure 24. Vulnerable JavaScript Library 25. Web server Default Installation Page 26. Microsoft Windows IIS Default Page 27. Apache Struts2 Remote Command Execution 28. HTTP.SYS Remote Code Execution 29. Snoop Servlet Information Disclosure     **CONCLUSION:**  Auditing for Ananthapuramu District Portal Web Application was initiated on 29.10.2018 in the staging server URL: http://119.226.216.91:8080/ anantapuramu/login.apo 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 24.07.2019.  Ananthapuramu District Portal Web Application meets all the aspects of Open Web Application Security Project (OWASP) and is safe for hosting provided the recommendations are implemented. Ananthapuramu District Portal 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 Ananthapuramu District Portal Web Application. This application is free from any known vulnerabilities as on 24.07.2019.  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 Ananthapuramu District Portal Web Application is done or six months from the date of issue whichever is earlier.   Dr.G. Jacob Victor Date: 23.07.2019  Executive Director (FAC)  For Andhra Pradesh Technology Services Ltd.  Place : Vijayawada |