|  |
| --- |
| **Security Certificate**  (Unique Ref No: APTS/APCSP/Assurance/10/2019) |
| **Audit Performed by:** Andhra Pradesh Technology Services Ltd.  **Application Description/Name:** PEOPLE FIRST.  **Staging URL :** <http://www.uat.peoplefirst.ap.gov.in/>  **Production URL** of the web application: <https://www.peoplefirst.ap.gov.in/>  **Audit Performed by:**   1. **Name :**  APTS Security Team 2. **Email :** 3. **Telephone :** 0866-2468102   **Level -01 Assessment date :** 07-JAN-2019  **Level -02 Assessment date :** 18-JAN-2019  **Level -03 Assessment date :** 30-JAN-2019  **Level -04 Assessment date :** 18-FEB-2019  **Level -05 Assessment date :** 22-JUN-2019  **Issue Date :** 08-JUL-2019  **Unique Reference No. :** APTS/APCSP/Assurance/10/2019  People First, auditing is completed on a staging server with URL: <http://www.uat.peoplefirst.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. Improper validation in OTP field 2. Improper API Authentication 3. Blind Sql Injection 4. Cross Site Scripting 5. Admin Page Enumerated 6. Concurrent Logins 7. Improper Input Validation 8. Account Lock out Policy Not Enabled 9. Stored HTML Injection 10. Unencrypted Communication 11. Password Field with auto-complete enabled 12. Technology/Version Disclosure 13. Clickjacking Attack 14. Sensitive Information Disclosure 15. Possible internal IP address disclosure 16. Unrestricted File Upload 17. Authentication Bypass 18. OTP Flooding 19. Improper Captcha Implementation 20. Improper Authentication 21. Improper / No session Handling 22. Broken Access Control 23. No Session timeout 24. Login Brute Force Attack 25. Security Headers not enabled 26. Improper last login time implemented 27. Unreferenced File Found 28. Web Services Information Disclosure     **CONCLUSION:**  Auditing for People First Web Application was initiated on 07.01.2019 in the staging server URL: <http://www.uat.peoplefirst.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 08.07.2019.  People First Web Application meets all the aspects of Open Web Application Security Project (OWASP) and is safe for hosting provided the recommendations are implemented. People First 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 People First Web Application. This application is free from any known vulnerabilities as on 08.07.2019.  The web application is free from all the vulnerabilities and is safe for hosting provided the recommendations are implemented.  **Recommendation:**   1. All SSL/TLS and security header 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 People First Web Application is done or one year from the date of issue whichever is earlier.   Dr. G. Jacob Victor Date: 08.07.2019  Executive Director  Andhra Pradesh Technology Services Ltd.  Place : Vijayawada |