|  |
| --- |
| **Security Certificate**  (Unique Ref No: APTS/APCSP/Assurance/4/2019) |
| **Audit Performed by:** Andhra Pradesh Technology Services Ltd.  **Application Description/Name:** Ban Relief Fund Web Application.  **Staging URL :** https://brf.vassarlabs.com  **Production URL :** http://brf.fisheries.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 :** 13-DEC-2018  **Level -02 Assessment date :** 13-FEB-2019  **Level -03 Assessment date :** 19-MAR-2019  **Level -04 Assessment date :** 10-APR-2019  **Level -05 Assessment date :** 23-APR-2019  **Level -06 Assessment date :** 25-APR-2019  **Level -07 Assessment date :** 26-JUN-2019  **Level -08 Assessment date :** 28-JUN-2019  **Issue Date :** 02-JUL-2019  **Unique Reference No. :** APTS/APCSP/Assurance/4/2019  Ban Relief Fund Web Application auditing is completed on a staging server with URL: https://brf.vassarlabs.com. During the initial assessment of the web application following vulnerabilities were discovered which have been successfully fixed by the development team:   1. OTP Bypass 2. Port Configuration 3. Concurrent Logins 4. Improper implementation of account lockout security feature 5. Last login time not implemented 6. Weak Password Policy 7. Horizontal Privilege Escalation 8. User Credentials are sent in clear text 9. Session Hijacking 10. Possible SQL Injection 11. Username field submitted using GET method 12. Sensitive Information Disclosure 13. Improper Captcha Implementation 14. Captcha Bypass 15. Default Credentials 16. Clear text storage of credentials in browser cache 17. Improper Input Validation 18. Application Logic Bypass 19. Sensitive Information is stored inside the Cookie 20. Possible DOS Attack 21. Clickjacking Attack 22. Username and Password Fields with auto-complete enabled 23. Cross-origin resource sharing(CORS) 24. Vertical Privilege Escalation 25. Insecure Direct Object Reference(IDOR) 26. Usernames Enumerated 27. Unauthenticated API 28. Technology/Version Disclosure 29. Security Headers not Implemented 30. Cookie without Secure Flag 31. SSL Vulnerabilities 32. User Id Disclosure in Source Code 33. Improper Error Handling 34. Application running on multiple ports 35. Improper Session Time Out   **CONCLUSION:**  Auditing for Ban Relief Fund Web Application was initiated on 13.12.2018 in the staging server URL: https://brf.vassarlabs.com 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 02.07.2019.  Ban Relief Fund Web Application meets all the aspects of Open Web Application Security Project (OWASP) and is safe for hosting provided the recommendations are implemented. Ban Relief Fund 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 Ban Relief Fund Web Application. This application is free from any known vulnerabilities as on 02.07.2019.  The web application is free from all the vulnerabilities and is safe for hosting provided the recommendations are implemented.  **Recommendation:**   1. SSL/TLS should be implemented 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 Ban Relief Fund Web Application is done or one year from the date of issue whichever is earlier.   Dr. G. Jacob Victor Date: 02.07.2019.  Executive Director  Andhra Pradesh Technology Services Ltd.  Place : Vijayawada |