|  |
| --- |
| **Security Certificate**  (Unique Ref No: APTS/APCSP/Assurance/8/2019) |
| **Audit Performed by:** Andhra Pradesh Technology Services Ltd.  **Application Description/Name:** ITE&C Invest –Incentive Portal  **Production URL** of the web application: <http://itecinvest.ap.gov.in/ITECINC/#/login>, http://itecinvest.ap.gov.in/ITECINC/#/admin/login  **Audit Performed by:**   1. **Name :**  APTS Security Team 2. **Email :** 3. **Telephone :** 0866-2468102   **Level -01 Assessment date :** 04-Jun-2019  **Level -02 Assessment date :** 07-Jun-2019  **Level -03 Assessment date :** 17-Jun-2019  **Level -04 Assessment date :** 20-Jun-2019  **Level -05 Assessment date :** 21-Jun-2019  **Level -06 Assessment date :** 25-Jun-2019  **Level -07 Assessment date :** 26-Jun-2019  **Issue Date :** 26-Jun-2019  **Unique Reference No. :** APTS/APCSP/Assurance/8/2019  ITE&C Invest –Incentive Portal Web Application, auditing is completed on a production server with URL: <http://itecinvest.ap.gov.in/ITECINC/#/login>, <http://itecinvest.ap.gov.in/ITECINC/#/admin/login>. During the initial assessment of the web application following vulnerabilities were discovered which have been successfully fixed by the development team:   1. Stored Cross Site Scripting 2. Broken Access Control 3. Business Logic Bypass 4. Privilege Escalation 5. OTP Bypass 6. Insecure Direct Object Reference (IDOR) 7. Sensitive Information Disclosure 8. Malicious File Upload 9. Weak Password Policy 10. Improper Session Management 11. Forceful browsing 12. Insufficient anti automation 13. Concurrent Logins Possible 14. Password Encoded with Base 64 15. OTP Flooding 16. Improper / No session handling 17. Insecure Response with wildcard '\*' in Access-Control-Allow-Origin 18. Clickjacking Attack 19. HTTP Only Flag Not Implemented 20. Version Disclosure 21. Auto-complete off not enabled 22. CAPTCHA bypass 23. Database error 24. Improper Input validation 25. SQL Injection     **CONCLUSION:**  Auditing for ITE&C Invest –Incentive Portal Web Application was initiated on 04-Jun-2019 in the production server URL: [http://itecinvest.ap.gov.in/ ITECINC/#/login](http://itecinvest.ap.gov.in/%20ITECINC/#/login), <http://itecinvest.ap.gov.in/ITECINC/#/admin/login> 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 26.06.2019.  ITE&C Invest –Incentive Portal Web Application meets all the aspects of Open Web Application Security Project (OWASP) and is safe for hosting provided the recommendations are implemented. ITE&C Invest –Incentive 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 ITE&C Invest –Incentive Portal Web Application. This application is free from any known vulnerabilities as on 26.06.2019.  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 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: 26.06.2019  Executive Director  Andhra Pradesh Technology Services Ltd.  Place : Vijayawada |