|  |
| --- |
| **Security Certificate**  (Unique Ref No: APTS/APCSP/Assurance/11/2019) |
| **Audit Performed by:** Andhra Pradesh Technology Services Ltd.  **Application Description/Name:** Society for Andhra Pradesh Network.  **Staging URL :** <https://www.competitiveindia.com/dynamic/sapnet/>home.php,  [https://www.competitiveindia.com/dynamic/dashboard/authentication](https://www.competitiveindia.com/dynamic/sapnet/)  **Production URL** of the web application: https://sapnet.gov.in,  https://sapnet.gov.in/dashboard  **Audit Performed by:**   1. **Name :**  APTS Security Team 2. **Email :** 3. **Telephone :** 0866-2468102   **Level -01 Assessment date :** 13-MAR-2019  **Level -02 Assessment date :** 28-MAR-2019  **Level -03 Assessment date :** 01-APR-2019  **Level -04 Assessment date :** 08-APR-2019  **Level -05 Assessment date :** 23-APR-2019  **Level -06 Assessment date :** 07-MAY-2019  **Level -07 Assessment date :** 11-MAY-2019  **Level -08 Assessment date :** 21-MAY-2019  **Issue Date :** 08-JUL-2019  **Unique Reference No. :** APTS/APCSP/Assurance/11/2019  Society for Andhra Pradesh Network, auditing is completed on a staging server with URL: <https://www.competitiveindia.com/dynamic/sapnet/>home.php, [https://www.competitiveindia.com/dynamic/dashboard/authentication](https://www.competitiveindia.com/dynamic/sapnet/). During the initial assessment of the web application following vulnerabilities were discovered which have been successfully fixed by the development team:   1. Malicious File Upload 2. Time Based Blind SQL Injection 3. Stored XSS (Cross Site Scripting) 4. Error Based SQL Injection 5. Cross Site Request Forgery (CSRF) 6. Improper Session Management 7. HTML Injection 8. Improper Input Validation 9. Directory Listing 10. Weak Password Policy 11. Account lockout policy not implemented 12. Cookie Attributes not implemented 13. Technology / Version Disclosure 14. Email Addresses Disclosure 15. Insufficient Anti Automation 16. Concurrent Logins possible 17. Cleartext storage of credentials in browser cache 18. Last Login Time not implemented 19. Subresource Integrity (SRI) not implemented 20. Autocomplete all forms 21. Username And Password stored in post request with page after login 22. Broken access control   **CONCLUSION:**  Auditing for Society for Andhra Pradesh Network Web Application was initiated on 13.03.2019 in the staging server URL: <https://www.competitiveindia.com/dynamic/sapnet/>home.php, [https://www.competitiveindia.com/dynamic/dashboard/authentication](https://www.competitiveindia.com/dynamic/sapnet/) 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.  Society for Andhra Pradesh Network Web Application meets all the aspects of Open Web Application Security Project (OWASP) and is safe for hosting provided the recommendations are implemented. Society for Andhra Pradesh Network 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 Society for Andhra Pradesh Network 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 Society for Andhra Pradesh Network 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 |