|  |
| --- |
| **Security Certificate**  (Unique Ref No: APTS/APCSP/Assurance/22/2019) |
| **Audit Performed by:** Andhra Pradesh Technology Services Ltd.  **Application Description/Name:** Learning Management System  **Staging URL :** http://172.19.135.184/  **Production URL** of the web application: http://www.ccelms.ap.gov.in/rusa  **Audit Performed by:**   1. **Name :** APTS Security Team 2. **Email :** mgr-apcsp-apts@ap.gov.in 3. **Telephone :** 0866-2468102   **Level -01 Audit date :** 06-NOV-2018  **Level -02 Audit date :** 05-Mar-2019  **Level -03 Audit date :** 22-Mar-2019  **Level -04 Audit date :** 08-APR-2019  **Level -05 Audit date :** 18-APR-2019  **Level -06 Audit date :** 29-APR-2019  **Level -07 Audit date :** 06-JUN-2019  **Issue Date :** 30-JUL-2019  **Unique Reference No. :** APTS/APCSP/Assurance/22/2019  Learning Management System, auditing is completed on a staging server with  URL: http://172.19.135.184/. During the initial audit of the web application following vulnerabilities were discovered which have been successfully fixed by the development team:   1. SQL Injection 2. Sensitive Information Disclosure 3. No Password Policy 4. User Credentials are sent in clear text 5. Database Files Found 6. Concurrent Logins Possible 7. Cross Site Request Forgery 8. Broken Access Control (Open) – (Exception mail has been received from Dept on 30-07-2019) 9. Browser Cache Weakness(back button) 10. Stored XSS 11. Clickjacking 12. Directory Listing 13. Backup Files Found 14. File Path Disclosure 15. Spoofed the Client IP Address 16. Application Error Page 17. Potentially Harmful Trace Method Enabled 18. Error Message on Page 19. HTML Injection 20. Insufficient Anti Automation 21. No Account Lockout Policy 22. Cookie(s) without HTTP Only flag set 23. Cookie(s) without Secure flag set 24. Technology/Version disclosure 25. Jquery Vulnerable Version 26. Duplicate cookie set 27. File Upload Functionality 28. Robots.txt 29. Host Header reflected in Href Response 30. Missing Security headers 31. Sub Resource Integrity (OSS.MAX.CDN) 32. Internal IP Disclosure 33. Config Files Found 34. Email Address Disclosure 35. Cross Origin Resource Sharing 36. Last Login Time Not implemented 37. AutoComplete On     **CONCLUSION:**  Auditing for Learning Management System Web Application was initiated on 26.10.2018 in the staging server URL: http://172.19.135.184/ 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 30.07.2019.  Learning Management Web Application meets all the aspects of Open Web Application Security Project (OWASP) and is safe for hosting provided the recommendations are implemented. Learning Management System 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 Learning Management System Web Application. This application is free from any known vulnerabilities as on 30.07.2019.  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 Guntur District Portal Web Application is done or **six months** from the date of issue whichever is earlier.   Dr.G. Jacob Victor Date: 30.07.2019  Executive Director  For Andhra Pradesh Technology Services Ltd.  Place : Vijayawada |
|  |