सत्यमेव जयते

Application Security Test Report
Of
Government e-Marketplace (GeM)

(http://uat.gemorion.org/)

21th December, 2018

STQC IT - ERTL (North)

STQC Directorate,

Ministry of Electronics & Information Technology

ERTL (North), S- Block, Okhla Industrial Area Phase – II

New Delhi – 110020

Executive Summary:

The Application Security testing of Government e-Marketplace (GeM) web application was undertaken by STQC. The scope of testing covered only website application security testing of Government e-Marketplace (GeM) and did not include any attempts to exploit Network or Host System level vulnerabilities. As the scope was limited to application security only, the configuration settings of host systems & network devices and operational aspects including security processes/ controls at hosting site were not verified.

The key aim of application security testing was to verify that itcomplies with the security requirements of OWASP top 10, 2013. The website application security testing was performed to assess the adequacy & effectiveness of various security controls such as input validation, authentication, authorization, session management, data protection during transmission and in storage, error handling, audit logs etc. and identify the vulnerabilities (if any).

The Application Security testing was performed only for the web application and the test setup was provided on a staging server. The application was accessed remotely by using test URL: http://uat.gemorion.org/.

Security testing was performed for following roles i.e. Buyer, Seller, HoD, Consignee & PAO.
The Website Application security testing was carried out using Black Box approach based on test scenarios & test cases derived from the requirements of the application without any knowledge of the internals. Security testing was conducted without launching any attack; however tests were conducted to determine whether the Website is susceptible to security vulnerabilities. The security testing involved an active analysis of Website to identify any weaknesses, technical flaws and vulnerabilities. The Website was tested as per the security requirements of OWASP Top 10, 2013.
Major concerns observed during testing are as follows:

1. **During testing, test environment was not completely freeze and it seems site was under continuous upgradation process. UAT was unstable during testing period.**
2. **During testing, credentials were changing very frequently, due to which testing was interrupted many times.**
3. **During automated testing for the Seller, Consignee and PAO role, only http://uat.gemorion.org/ URL is accessible to the AppScan tool. AppScan was unable to discover other sub URLs like https://mkp.gemorion.org, http://admin-mkp.gemorion.org/, http://fulfilment.gemorion.org/, http://bidplus.gemorion.org/, https://sso.gemorion.org/ etc during testing because of the GeM side restriction.**

The first cycle of security testing was conducted from 06th to 14th September, 2018. The vulnerabilities observed were reported to GeM team vide Security Test Report, Ref. no. STQC IT ERTL (N)/GeM/AS/09/2018/139 dated 25th September 2018, for corrective action on the observed vulnerabilities. Main issues observed are as follows:
The closure verification/ Final test cycle was conducted on 19th December 2018.
All of the Thirty Five (35) vulnerabilities are verified for closure actions & found as satisfactorily closed during second/final cycle. No new vulnerability was found in the final test cycle.

Details of security vulnerabilities observed in the various cycles & their closure status after final cycle, Compliance against OWASP Top 10, 2013 and Recommendations for deployment of the Web site in production environment are given in section 4.0 of this report.