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.

1.0	**Client Details:**	
1.1	**Client**	Government e-Marketplace (GeM)
1.2	**Address**	Mr. Sanjay Joseph GeM Hall, 2nd Floor, Jeevan Tara Building, Near Patel chowk, New Delhi , Contact Number : 011-23348469 E-mail: sanjay.joseph@gem.gov.in
2.0	**Details of the Web Application Under Test:**	
2.1	**Web Application**	Government e-Marketplace (GeM)
2.2	**Version No.**	3.0
2.3	**Date of Release**	Not Specified
2.4	**Description**	GeM is the platform which provides procurement of goods and service required by central and state government organization.
2.5	**Developing Organization**	Not Specified
2.6	**Applicable References**	OWASP Top 10, 2013
2.7	**Web Application Access**	http://uat.gemorion.org/
2.8	**Documents Submitted**	Website Application Security Questionnaire
3.0	**Test Description:**	
3.1	**Testing Organization**	STQC IT – ERTL (North), STQC Directorate, Ministry of Electronics &Information Technology, ERTL (North), S- Block, Okhla Industrial Area Phase – II , New Delhi – 110020
3.2	**Test Objective(s)**	The key aim of security testing was to verify that the GeM Web application complies with the security requirements as per OWASP top 10, 2013. The Application Security testing was performed to assess the adequacy & effectiveness of various software application security controls such as input validation, authentication, authorization, session management, denial of service, data protection during transmission and in storage, error handling, audit logs etc. and identify vulnerabilities (if any).
3.3	**Scope of Testing**	The scope of testing was limited to the application security testing of GeM web application only and did not cover any Network or Host System level vulnerabilities assessment.

3.4	**Type of Testing**	Independent third party Application Security Testing.
3.5	**Test Approach & Methodology**	Application security testing involved an active analysis of the web application to identify any weaknesses, technical flaws and vulnerabilities by emulating attacks. Automated test tool- IBM Rational AppScan and BurpSuite used to detect the vulnerabilities.
3.6	**Test Data**	The test data used for testing was generated based on test scenarios for both valid as well invalid cases.
3.7	**Test Standards**	1. IEEE Std 29119 for test documentation 2. OWASP Top 10, 2013
3.8	**Test Environment**	The client side test environment used for security testing comprised of following hardware & software Test configurations:
	Hardware & Software Configurations	System Model: Dell System Type : Latitude E5440 Processor : Intel Core i7 4600U CPU @2.10 GHz 2.70 GHz RAM : 8 GB HDD : 500 GB
		OS Name : Microsoft Windows 8.1 Pro Microsoft Office 2007 IBM Rational AppScan 9.0.3.7 Burp Suite version 1.7.30 Mozilla Firefox 62.0
	Test Tools	IBM Security AppScan Standard 9.0.3.7 Burp Suite version 1.7.30
3.9	**Test Location**	STQC IT-ERTL(N) STQC Directorate, Ministry of Electronics & Information Technology ERTL (North), S- Block, Okhla Industrial Area Phase – II New Delhi – 110020
3.10	**Test Team**	1. Sanjeev Kumar, Scientist, "F" 2. Praveen Kumar Singh, Scientist, "B"
3.11	**Period of Testing**	06th to 14th September, 2018 (First Round for Buyer and HoD role) 05th to 09th November, 2018 (First Round for PAO and Consignee role) 26th to 27th November, 2018 (First Round for Seller role) 03th to 04th December, 2018 (Second Round Confirmation Testing for all role) 19th December 2018 (Final Round)

4.0. Application Security Test Summary:

4.1 Closure Status of the vulnerabilities observed in Various Test Cycles:

The status of closure of vulnerabilities observed in Final cycle of testing is as follows:

S. NO.	Vulnerability Details	Closure Status (Final Cycle)
1.	**Apache Multiviews Attack:** It seems test response indicates that the server reveals some of its pages names in the response. It may be possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application.	**Verified & Closed**
2.	**Cacheable SSL Page Found:** It seems sensitive information might have been cached by the browser. The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache"). Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache". It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations.	**Verified & Closed**
3.	**Check for SRI (Subresource Integrity) support:** In application there is no support for Subresource Integrity. The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised. Add to each third-party script/link element support to SRI (Subresource Integrity). In case the third-party server is compromised, the content/behavior of the site will change.	**Justification accepted. Clarification from GEM: On Google analytics link, it is not possible to implement "integrity" attribute.**
4.	**Compressed Directory Found:** It is possible to retrieve the source code of server-side scripts, which may expose the application logic. Due to insecure web application programming or configuration, AppScan received a response status 200 OK, with a Content-Type that matches the requested file extension.	**Verified & Closed**
5.	**Cross-Site Request Forgery:** The test results confirm this vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referrer' header. Validate the value of the "Referrer" header, and use a one-time-nonce for each submitted form.	**Verified & Closed**

6.	**Cross-Site Scripting :** Sanitation of hazardous characters was not performed correctly on user input. The test results confirm this vulnerability because AppScan successfully embedded a script in the response, which will be executed when the page loads in the user's browser. It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user.	**Verified & Closed**
7.	**Directory Listing:** Directory browsing is enabled. The response contains the content of a directory (directory listing). This indicates that the server allows the listing of directories, which is not usually recommended. It is possible to view and download the contents of certain web application virtual directories, which might contain restricted files	**Verified & Closed**
8.	**Hidden Directory Detected:** The test detects hidden directories on the server. The 403 Forbidden responses reveal the existence of the directory, even though access is not allowed. It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site.	**Verified & Closed**
9.	**HTTP Response Splitting:** It is possible to deface the site content through web-cache poisoning. Sanitation of hazardous characters was not performed correctly on user input. The response contained a new header, inserted by the successful HTTP Response Splitting test. It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user.	**Verified & Closed**
10	**Missing HttpOnly Attribute in Session Cookie:** The web application sets session cookies without the HttpOnly attribute. AppScan detects that a session cookie is used without the "HttpOnly" attribute. It is recommended to add the 'HttpOnly' attribute to all session cookies.	**Verified & Closed**
11	**Missing or insecure "Content-Security-Policy" header:** Insecure web server configuration. It is observed that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks. It is recommended to Config your server to use the "Content-Security-Policy" header with secure policies. It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations.	**Verified & Closed**

12	**Missing or insecure "X-Content-Type-Options" header:** Due to insecure web application programming or configuration, AppScan detected that the "X-Content-Type-Options" response header is missing or has an insecure value, which increases possibility to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations.	**Verified & Closed**
13	**Missing or insecure "X-XSS-Protection" header:** Due to insecure web application programming or configuration, AppScan detected that the X-XSS-Protection response header is missing or with an insecure value, which may allow possibility to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations.	**Verified & Closed**
14	**Missing or insecure Cross-Frame Scripting Defense:** Due to insecure web application programming or configuration, AppScan detected that the X-Frame-Options response header is missing or with insecure value, which increases possibility to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations.	**Verified & Closed**
15	**Overly Permissive CORS Access Policy:** Due to insecure web application programming or configuration, AppScan detected that the "Access-Control-Allow-Origin" header is too permissive. It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations.	**Verified & Closed**
16	**Stored Cross-Site Scripting:** Sanitation of hazardous characters was not performed correctly on user input. The test result seems to indicate vulnerability because the Global Validation feature found an embedded script in the response, which was probably injected by a previous test. It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user.	**Verified & Closed**
17	**Temporary File Download:** It seems that temporary files were left in production environment. The test tried to retrieve a source code file. The fact that the response did not yield an error, and contained non-HTML contents, indicates that the source code retrieval succeeded. It is possible to download temporary script files, which can expose the application logic and other sensitive information.	**Verified & Closed**

18	**Temporary Directory Found:** The test result seems to indicate a vulnerability because the test response is similar to the Original Response, indicating that a somewhat different version of the resource was received using an alternate name. It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site.	**Verified & Closed**
19	**Unsafe third-party link (target="_blank"):** The rel attribute in the link element is not set to "noopenernoreferrer". The third-party links with target="_blank" attribute and no rel="noopenernoreferrer" attribute allows linked page partial access to the linking page window object. It is recommended to add the attribute rel = "noopenernoreferrer" to each link element with target="_blank".	**Justification accepted. Clarification from GEM: Rel= ”noopener noreferrer” cannot be set on “drive.google” link as it is the business requirement of GeM.**
20	**Web Application Source Code Disclosure Pattern Found:** The response contains source code of script files, which may expose sensitive information about the site and the application logic. It is possible to retrieve the source code of server-side scripts, which may expose the application logic. Remove source code files from your web-server and apply any relevant patches.	**Verified & Closed**
21	**Application Error:** Proper bounds checking were not performed on incoming parameter values. No validation was done in order to make sure that user input matches the data type expected. The application has responded with an error message, indicating an undefined state that may expose sensitive information.	**Verified & Closed**
22	**Application Test Script Detected:** Temporary files were left in production environment. AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.	**Verified & Closed**
23	**Email Address Pattern Found:** The response contains e-mail addresses that may be private. Remove e-mail addresses from the website which are not required.	**Verified & Closed**

24	**HTML Comments Sensitive Information Disclosure:** Debugging information was left by the programmer in web pages. AppScan discovered HTML comments containing what appears to be sensitive information. It is possible to gather sensitive information about the web application	**Verified & Closed**
25	**Integer Overflow:** Proper bounds checking were not performed on incoming parameter values. No validation was done in order to make sure that user input matches the data type expected. The application has responded with an error message, indicating an undefined state that may expose sensitive information.	**Verified & Closed**
26	**Possible Server Path Disclosure Pattern Found:** The response contains the absolute paths and/or filenames of files on the server. It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application	**Verified & Closed**
27	**SHA-1 cipher suites were detected:** The web server or application server are configured in an insecure way. AppScan determined that the site uses weak cipher suites by successfully creating SSL connections using each of the weak cipher suites listed here. It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user.	**Verified & Closed**
28	**Unsanitized user input reflected in JSON:** Sanitation of hazardous characters was not performed correctly on user input. The test result seems to indicate vulnerability because the Global Validation feature found an embedded script in the response, which was probably injected by a previous test. It may be possible to steal or manipulate customer session and cookies.	**Verified & Closed**
29	**Default user name** Default user name i.e. network and user1 are valid username and system permits to login with password "Gem@12345" into the application.	**Verified & Closed**
30	**Password Length** Minimum length of password should have to be 8 characters long for public web application, however in application minimum length of password are 6 characters only.	**Verified & Closed**
31	**Disabling Browser Auto complete Feature** Auto complete is not set to false for password and username field. It is necessary to disable browser auto complete feature in the application.	**Verified & Closed**

32	**Privilege Escalation:** HoD user who is not authorized to access "Order" link, is able to escalate its privilege by using below mentioned URL "https://fulfilment.gemorion.org/fulfilment/home#WORKSPACE_ID=ORDERS_WS" Some other issues of privilege escalation may be possible in the application. It is recommended to restrict privilege escalation all over in the application.	**Verified & Closed**
33	**Session Handling:** Session handling is not properly configured. On clicking Logout link, result in the session needs to expire from server side. Session Id mentioned in "_site_session" attribute is not expired from server side. User can replace current session id with previous session id. Along with that server is accepting any value (user defined) in "_site_session" attribute instead of server assigned session id.	**Justification accepted because Rail Framework is used as development platform.**
34	**Command injection** After login with seller credentials, on entering ">|;%date>|;% " in bid search box field. Instead of generic error whole page gone blank.	**Verified & Closed**
35	**Cookie Contains Sensitive Information:** The web application stores sensitive session information in cookie. BurpSuite found that sensitive information like username, email id, post name and server name are passing in plain text in "Request" header. Either sensitive information need not to be mention in the cookie or need to pass them with strong encryption.	**Verified & Closed**

4.2 OWASP Compliance Status:

The compliance status against different vulnerability categories as per OWASP top 10, 2013 is as follows:

OWASP Top Ten (2013)	Web Application Vulnerabilities	Compliance	Remark
A1	Injection	Satisfactory	Nil
A2	Broken Authentication and Session Management	Satisfactory	Nil
A3	Cross Site Scripting (XSS)	Satisfactory	Nil
A4	Insecure Direct Object References	Satisfactory	Nil
A5	Security Misconfiguration	Satisfactory	Nil
A6	Sensitive Data Exposure	Satisfactory	Nil
A7	Missing Function Level Access Control	Satisfactory	Nil
A8	Cross Site Request Forgery (CSRF)	Satisfactory	Nil
A9	Using Known Vulnerable components	Satisfactory	Nil
A10	Unvalidated Redirects and Forwards	Satisfactory	Nil

Recommendations:

1. Auditing for Government e-Marketplace (GeM) 3.0 was done from 06th to 14th September 2018 for Buyer and HoD role, 05th to 09th November 2018 for PAO and Consignee role, 26th to 27th November 2018 for Seller role as per the OWASP Top 10 2013 by STQC IT, ERTL (N). The follow-up testing/ auditing was done from 03th to 04th December 2018 and 19th December 2018 (Final Cycle) and there is no pending nonconformity w.r.t OWASP Top 10 2013 as on 19th December 2018.
2. This is a php, jsp, ruby and gwt based application. It can be hosted with Read permissions only.
3. It is recommended to implement Two Factor authentication.
4. Sensitive data must be suitably protected in storage & transit.
5. User access log & transaction log of the Web application should be enabled and stored on a separate secure server.
6. Before deploying the Website in the production environment, the hardening of IT infrastructure (Network, Hosts and OS) must be ensured.

Conclusion:

The Website is free from OWASP Top 10, 2013 and any other known vulnerability and is safe for hosting.

5.0: Approved & Released By:

A. K. Upadhaya
Scientist "F"

K. S. Samant
Scientist "E"

STQC IT Delhi
Dated: 21st December, 2018