STQC IT SERVICES
ERTL(E), Kolkata
Ministry of Communications and Information Technology
Government of India

29th November 2011

Application Security Audit

Site Name : Website of Excise Department
Excise Directorate, Govt. of West Bengal

Site URL : http://wbexcise.gov.in

Test URL/Temporary URL : http://wbdemo3.nic.in/default.aspx

Audit Performed by : STQC IT Services, Kolkata

Testing Date : 22nd September 2011 to 9th November 2011

Observation :

Top 10 (2010)	Web Application Vulnerabilities	Outcome	Remarks
A1	Injection	No issues	--
A2	Cross-site Scripting	No issues	--
A3	Broken Authentication and Session Management	No issues	--
A4	Insecure Direct Object Reference	No issues	--
A5	Cross-site Request Forgery	No issues	--
A6	Security Misconfiguration	No issues	--
A7	Insecure Cryptographic Storage	No issues	--
A8	Failure to Restrict URL Access	No issues	--
A9	Insufficient Transport Layer Protection	SSL is not used for authentication pages.	Login parameters should be transmitted over encrypted channel (Refer Recommendation-2).
A10	Unvalidated Redirects and Forwards	No issues	--

Recommendation:

1. The web application may be hosted at the following site URL, with privileges of Read and Script Execute permission for the general public:
   a. Temp URL:http://wbdemo3.nic.in/default.aspx
   b. Site URL: http://wbexcise.gov.in
2. The corresponding pages in the production site to the following pages in temporary site are to be deployed over SSL:
   a. http://wbdemo3.nic.in/UserLogIn/login.aspx
   b. http://wbdemo3.nic.in/UserLogIn/Portal_Login.aspx
3. Web Server and OS level hardening need to be in place in the production server.

Conclusion:

The Web Application is free from OWASP-Top 10 2010 (and any other known) vulnerabilities and is safe for hosting, except the issue related to insufficient transport layer protection (A9).The issue should be taken care of in the production environment as mentioned above.

29.11.2011

Audited By: **Arpita Datta**
Scientist 'D'

Approved By: **B.K.Mondal**
Gp Director &
Head, e-Security

Block DN, Sector V, Salt Lake, Kolkata - 700 091, Phone : (9133) 2367 9825/5114/0772
Fax : (9133) 2367 5113/9472
E-mail : stqc-it@ertleast.org, Website : www.stqc.nic.in