सत्यमेव जयते

# Application Security Audit Report

## Citizen Portal Application, Employee Portal Application & CRM Application Of Department of Post

**24th September, 2015**

**STQC IT Services Delhi**
STQC Directorate, Department of Electronics & Information Technology,
Ministry of Communication & Information Technology,
S- Block, Okhla Industrial Area Phase – II
New Delhi – 110020

# STQC IT – Delhi
## Application Security Audit Report

| Application Security Audit Report Number | Date | Page No. |
|---|---|---|
| STQC - IT Services/DOP/ CSI/ASAR-01 | 24/09/2015 | Page 1 of 1 |

**Web Application Tested:** 1. Citizen Portal Application
2. Employee Portal Application & CRM Application

**Test URL:** https://bqdbssswmv01.indiapostdev.gov.in/VAS/Pages/dophome.aspx
https://btepptv1.indiapostdev.gov.in/irj/portal

**Host URL :** https://portal.indiapost.gov.in ( For Citizen Portal)

**Not Specified ( For Employee Portal Application & CRM Application)**

**Test /Audit Agency:** STQC IT - ERTL (North) New Delhi

**Testing/ Audit Date(s):** 11th & 22nd September 2015

**Test/ Audit Result Summary:**

| 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. Security Testing & Audit of CSI applications of Department of Post was done on 11th & 22nd September 2015 , as per the OWASP Top 10 2013 by STQC IT, ERTL (N) and there is no known vulnerability observed w.r.t OWASP Top 10 2013 as on 22/09/2015.
2. These are ASPX based web applications which can be hosted with Read and Script Execute permissions.
3. User credentials and sensitive portal data must be suitably protected.
4. Before deploying the Web Applications 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) vulnerabilities and is safe for hosting.

| **Audited by:** | **Approved by:** |
|---|---|
| **Sanjeev Kumar &**<br>**M. K. Saxena** | **Suresh Chandra** |