



12th July 2012

Application Security Audit

Site Name : Website of Eastern Coalfields Limited
 Client's Address : Eastern Coalfields Limited
 (A govt. of India Undertaking)
 Sanctoria, Dishergarh, Burdwan
 Pin: 713 333
 Site URL : http://easterncoal.gov.in
 Temporary/Test URL : http://easterncoal.gov.in
 Audit Performed by : STQC IT Services, Kolkata
 Testing Date : 17th June 2011 to 3rd August 2011

Observation :

Sl. No	Web Application Vulnerabilities	Observation	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	No issues	--
A10	Unvalidated Redirects and Forwards	No issues	--

Recommendation:

- The web application may be hosted at the following site URL, with privileges of Read Only permission for the general public:
 - Site URL: http://easterncoal.gov.in
- Hardening of the Web Server and the OS for security need to be done in the production server where the application will be hosted.

Conclusion:

The Web Application is free from OWASP-Top 10 2010 (and any other known) vulnerabilities.

Audited By: *Arup Datta*
 Scientist 'B'

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