



Project No. ES/HCLK/181901

11<sup>th</sup> September 2018

## Web Application Security Audit

**Application Name** : Web Portal of Hindustan Copper Limited  
**Customer's Address** : Hindustan Copper Limited  
: Tamra Bhavan  
: 1, Ashutosh Chowdhury Avenue, P.B. No. 10224, Kolkata - 700 019  
**Site URL** : <https://www.hindustancopper.com>  
**Temporary URL** : <http://www.hindustancopper.com>  
**Audit Performed by** : STQC IT Services, Kolkata  
**Testing Date** : 26<sup>th</sup> July 2018 to 24<sup>th</sup> August 2018 (Cycle-1)  
: 3<sup>rd</sup> September 2018 to 10<sup>th</sup> September 2018 (Cycle-2)

### OWASP Top 10 (2017) Vulnerabilities

Sl. No	Web Application Vulnerabilities	Observation	Remarks
A1	Injection	No issues	--
A2	Broken Authentication	No issues	--
A3	Sensitive Data Exposure	No issues	--
A4	XML External Entities	No issues	--
A5	Broken Access Control	No issues	--
A6	Security Misconfiguration	Unnecessary HTTP methods like OPTIONS etc. are enabled in the web server.	Web server should be configured so that it allows GET and POST methods only (Recommendation-2).
A7	Cross-Site Scripting	No issues	--
A8	Insecure Deserialization	No issues	--
A9	Using Components with Known Vulnerabilities	No issues	--
A10	Insufficient Logging and Monitoring	No issues	--

### Recommendation:

1. The web portal may be hosted at <https://www.hindustancopper.com>, with Read and Script Execute permission.
2. Hardening / proper secured configuration of the Web Server and Operating System need to be done in the production environment where the application will be hosted. Vulnerability assessment of the critical servers and perimeter devices should be done at regular intervals.

### Conclusion:

The Web Application is free from OWASP-Top 10 (2017) vulnerabilities and is safe for hosting.

Audited By: **Arup Datta**  
Scientist 'B'

Approved By: **Arpita Datta**  
Scientist 'E'

