



Certificate of Approval

This is to certify that "Website of eTender/eProcurement of NIC –
has been tested in line with "OWASP Top 10 2013 Web Application Security Risks".

Web site Details:

- Site Name: eTender/eProcurement
- Test URL/Temporary URL:
1. <https://164.100.129.65/nicgep/app>
- Audit Performed by: STQC-IT, Chennai
- Testing Date: 26/12/2018 to 11/02/2019
- Hash value (MD5) of Application: MD5 Checksum: 0a43f3e609ddd4a7ccd94fa0982ddc84
- REPORT NO: ETDC(CN)/IT/2018-19/444/3rd Cycle

Observations: NIL

Conclusion: Site is free from OWASP Top 10 2013 Vulnerabilities and is safe for hosting except, Vulnerabilities related to A5 (5.1) of OWASP 2013 as they are not tested due to limitation of scope of testing. Hence it is recommended to carry out the same on the live server. (Refer web application security report for more details)

Recommendation:

1. Site may be hosted with appropriate privileges of read or execute permission for the general public.
2. Ensure that "Write / Read "appropriate Permission is provided to the folders concerned with the uploading of files.
3. Ensure "Write" permission is provided to the folder containing the database.
4. Ensure appropriate protection for Application logs, user logs and establish necessary clock synchronization with international time sources.
5. The equivalent of the below listed URL to be deployed over TLS Version 1.2 :
<https://eprocure.gov.in/eprocure/app>
6. Web server and OS level hardening need to be in place for the production server.
7. The application owner(s) must conduct a reaudit in case of any addition/change in the dynamic content of the application.



(Authorised Signatory)

K. SANKARASUBRAMANIAN
SCIENTIST 'F'
ELECTRONICS TEST & DEVELOPMENT CENTRE
STQC DIRECTORATE,
MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA
THIRUVANMIYUR, CHENNAI - 600 041.

NABL Accredited Laboratory

तिरुवान्मियूर, चेन्नै - ६०० ०४१ / THIRUVANMIYUR, CHENNAI - 600 041.

Phone : 24547700 / 01 / 02 Fax : 24543713

E-mail : etdccn@stqc.gov.in Website : <http://www.stqc.gov.in>



Certificate of Approval

This is to certify that "Website of Open Auction & eAuction –
has been tested in line with "OWASP Top 10 2013 Web Application Security Risks".

Web site Details:

- Site Name: Open Auction & e-Auction
- Test URL/Temporary URL:
 1. <http://164.100.129.63/openauction/#/>
 2. <https://164.100.129.63/eAuction/app>
- Audit Performed by: STQC-IT, Chennai
- Testing Date: 01/01/2019 to 16/01/2019
- Hash value (MD5) of Application: MD5 Checksum:
 1. eAuction (Department Side): 5b74ab11af93c1639615eaef4b34ca57
 2. Open Auction: 9ceb5f8e2d56d48c214d22f5ab166f90
- REPORT NO: ETDC(CN)/IT/2018-19/448/2nd Cycle

Observations: NIL

Conclusion: Site is free from OWASP Top 10 2013 Vulnerabilities and is safe for hosting except, Vulnerabilities related to A5 (5.1 & 5.2) of OWASP 2013 as they are not tested due to limitation of scope of testing. Hence it is recommended to carry out the same on the live server. (Refer web application security report for more details)

Recommendation:

1. Site may be hosted with appropriate privileges of read or execute permission for the general public.
2. Ensure that "Write / Read "appropriate Permission is provided to the folders concerned with the uploading of files.
3. Ensure "Write" permission is provided to the folder containing the database.
4. Ensure appropriate protection for Application logs, user logs and establish necessary clock synchronization with international time sources.
5. The equivalent of the below listed URL to be deployed over TSL Version 1.2 :
<https://pmmementos.gov.in>.
6. Web server and OS level hardening need to be in place for the production server.
7. The application owner(s) must conduct a reaudit in case of any addition/change in the dynamic content of the application.


(Authorised Signatory)

N. PADMINI
SCIENTIST 'D'

NABL Accredited Laboratory

ELECTRONICS TEST & DEVELOPMENT CENTRE
STQC DIRECTORATE, DeitY,
MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA
THIRUVANMIYUR, CHENNAI - 600 041.