सत्यमेव जयते
महाराष्ट्र शासन

Directorate of Technical Education

Maharashtara State, 3, Mahapalika Marg,
Post Box No.1967, Mumbai- 400 001.
Telephone No0 022-68597470/411/431,
E-mail–desk11@dtemaharashtra.gov.in, Web: https://dte.maharashtra.gov.in

स्वातंत्र्याचा अमृत महोत्सव

No: 11/DTE/Security Audit /2024-25/57

Date: 30/04/2024

Invitation for quotation (2 Envelope)

Sealed quotations (2 envelope system)are invited from authorised supplier's / service providers to **engage CERT-IN empanelled security auditing agency to conduct security audit of Directorate of Technical Education's website** https://dte.maharashtra.gov.in **(DTE, M.S., Mumbai)**. The quotation in specified format, along with necessary supporting documents should be sealed in an envelope and submitted to this office on or before the prescribed time and date mentioned in this invitation letter.

You are requested to quote your best rates as offered to the Government organisations **in a sealed cover** indicating "COMMERCIAL BID FOR CONDUCTING THE SECUIRTY AUDIT OF DTE WEBSITE" addressed to the undersigned to reach **on or before 10/5/2024** (Address: Directorate of Technical Education, 3, Mahapalika Marg, Mumbai 400 001) and submitted sealed quotation will be opened on 10/05/2024 at 11.30 am.

Sr. No	Enquiry Number	Name of item*	Qty.	Consignee	Estimated cost/unit (Rs.)
1	11/DTE/Security Audit/2024-25/	To Complete all levels of Security Audit of DTE website with Report Generation, recommendations and issue a Security Clearance Certificate. (As per scope of work & deliverables at Annexure I & II)	Lump sum as per this document and Annexures thereof	*DTE, M.S., Mumbai*	82,600/- (incl.of Taxes)

*Technical specifications are given in Annexure I and II of this document.

Last date for submission of above quotations in sealed envelope(Envelope 1 and Envelope 2 to be packed and sealed in Third Bigger Envelope) to this office is 10/05/2024 till 5.00pm

Instructions to bidders and Terms & Conditions

1. The price bids of those firms will be opened who fulfil the terms and conditions.
2. Only those Organizations/firms registered with the CERT-in-empanelled for information security audit are eligible for submitting the quotation.

3. Incomplete or conditional quotation will not be entertained.
4. No quotation will be accepted after closing date and time.
5. Quotations by email /fax / online will not be accepted.
6. The selected agency will not outsource any activity to other agency.
7. The selected agency will maintain confidentiality of the findings of security audit and ensure that the findings and corrective actions are shared with concerned stake holders of the project
8. Schedule: The first round of website audit report should be submitted to DTE within10 days after the work order issued by DTE and consecutive round report if any, should be submitted within 5 days.
9. The bidder may remain present himself /herself or his/her authorized representative at the time of opening the quotation.
10. Any firm/organization blacklisted by a Govt./Semi Govt. Deptt. shall not be considered for his bid and bid will be rejected straightway.
11. A copy of terms & conditions attached as and Scope of work attached as duly signed by the bidder, as a token of acceptance of the same should be attached along-with the this enquiry.
12. DTE reserves the right to relax any terms and condition in the Govt. interest, with the approval of competent authority.
13. All disputes are subject to the jurisdiction - Mumbai.
14. Prices should be indicated in Indian Rupees only and in the respective units indicated at each row.
15. Calculations against each row as specified in the price schedule should be carried out carefully both for the total of each row and the Grand Total. Furnishing of any miscalculation etc. shall be at the bidder's risk and cost and the bid may be liable for summary rejection.
16. Payment Terms: 100% payment will be made only after submitting the final security audit certificate on completion of Audit of DTE website.
17. Under no circumstances any extra/ additional taxes, duties, levies etc. shall be payable to the bidder by DTE unless such a tax, duty or levy has been newly introduced and notified by the State Government or Government of India.
18. The bidder shall be the single point of contact for DTE till the completion of audit process.
19. Penalty Clause:
    a. Failure to complete the audit along with deliverables on or before the stipulated date will entail a penalty equal to 0.5% of the value of the contract price per week / part their of subject to maximum of 5 % of total contract value.
    b. In case of delay in compliance with the order beyond 15 days of the stipulated time period, DTE have right to cancel the order.

Sr.No.	Type of document to be attached in bid offer Envelop -1
1	covering letter with details of bidders, address, telephone number, mobile number, email ID, name , signature and seal
2	Type of Business Entity; manufacturer/ authorised dealer, any other (to be specified).
3	PAN card photocopy
4	sales tax /VAT /GST TIN number and proof of GST paid for the last quarter.
5	Offer letter on bidders letterhead stating make and model quoted(THIS OFFER LETTER SHULD BE SEPERATE FROM OTHER DOCUMENTS mentioned therein).
6	Technical Literature of the item quoted. (details of treatment to be done , nature of chemicals which will be used by the vendor)
	Type of document to be attached in bid offer Envelop -2
7	Price quote alongwith taxation, inclusions and exclusions, if any
8	Undertaking the bidder has not been blacklisted or debarred from supplying previously.

9	Undertaking about compliance of terms and conditions mentioned in this quotation
10	Bill of Material / Bill of quantity (BoM/BoQ/Packing list)
11	Envelope 3 - Envelope 1 and Envelope 2 are to sealed and packed in Envelope 3. Envelope 3 should be super scribed with enquiry number and date and addressed to the Director Technical Education,Maharashtra ,Mumbai. This envelope should be submitted on or before the last date and time mentioned in this document.

20. The sealed offers should be dropped in the Tender box at Desk11 of this office (Directorate of Technical Education,MS, 3, Mahapalika Marg, Opp Metro Cinema, Dhobi Talao, Mumbai -400 001. Phone - 022-68597431/411.)
21. This office reserves the right to reject any quotation(/s) without asigning the reasons thereof.

(Dr. Vinod M.Mohitkar)
Director, Technical Education, M.S. Mumbai

Copy to: - 1) Notice Board, Desk11, DTE HO
2) IT cell, DTE for publishing on website

Annexure – I

Objectives:

1. To conduct security audit to assess vulnerabilities to the DTE Website as per the ISO standards and OWASP top 10 vulnerabilities (Web &Mobile). The audit shall be conducted to review the intent and vulnerabilities to the organisations website.
2. Security Audit is intended to give developers and security teams the resources they need to build and maintain secure website. Through the project, our goal is to classify security risks and provide developmental controls to reduce their impact or likelihood of exploitation.
3. To identify the vulnerabilities, present in the RECPDCL website.
4. To identify the corrective measures and rectification of the vulnerabilities in DTE website.

Deliverables:

- The audit report provided by the agency should have details for corrective action and steps to remove identified vulnerabilities.
- The agency should provide support to the development team for changes in coding to remove the vulnerabilities.
- Vulnerability Assessment Report, Penetration Test Report.
- Compliance review should be done after ensuring that changes to remove the vulnerabilities are completed by the development team.
- Compliance audit should be done not only to check for removal of previously identified threats but to ensure that the application or website has no vulnerabilities as a result of changes done in the code
- One-day training session on the security for – No. of participants to also cover facilitation for closure of audit findings.

Annexure- II

The proposed scope of work

A. Audit of the DTE website:

1. The audit has to be done on the following parameters
    - To Assess Flaws in the Design of the website.
    - Attempting to guess passwords using password-cracking tools.
    - Validations of various data inputs.
    - Exception handling and logging.
    - Logical access control and authorization.
    - Evaluate the environment under which the website /application runs.
    - An unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system.
    - Malicious modification of data.
    - Website/ Application Security Audit
    - Penetration Testing
    - Vulnerability Testing
    - Compliance Review
2. Checking if commonly known holes in the website exist.
3. DTE website should be audited as per the Industry Standards and also as per the latest OWASP (Open Web Application Security Project) (refer table 6.1).
4. The auditor is expected to submit the recommendation, final audit report after the remedies/recommendations are implemented. The final report will certify the particular Website "Certified for Security".
5. Auditor must test website for attacks. The various checks/attacks /Vulnerabilities should cover the following or any type of attacks, which are vulnerable to website/application.
    - Vulnerabilities to SQL Injections
    - CRLF injections
    - Directory Traversal
    - Authentication hacking/attacks
    - Password strength on authentication pages
    - Scan Java Script for security vulnerabilities
    - File inclusion attacks
    - Exploitable hacking vulnerable
    - Web server information security
    - Cross site scripting
    - PHP remote scripts vulnerability
    - HTTP Injection
    - Phishing a website
    - Buffer Overflows, Invalid inputs, insecure storage etc.
    - Any other attack that can be a vulnerability to the website or web applications.
6. The Top 10 Web application security vulnerabilities, which are given below, should also be checked, but not restricted to the following. The best practices in the industry must be followed.

6.1- Top Ten Most Critical Web Application Security Vulnerabilities		
A1	**Injection**	Injection flaws, such as SQL, No SQL, OS, and LDAP injection, occur when un-trusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2	**Broken Authentication**	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
A3	**Sensitive Data Exposure**	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
A4	**XML External Entities (XXE)**	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
A5	**Broken Access Control**	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
A6	**Security Misconfiguration**	Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.
A7	**A7 Cross-Site Scripting (XSS)**	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A8	**Insecure Deserialization**	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

A9	**Using Components with Known Vulnerabilities**	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defences and enable various attacks and impacts.
A10	**Insufficient Logging & Monitoring**	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

7. Auditor to test vulnerabilities in Website as per Industry practices/OWASP.

B. Audit Report

The website security audit report is a key audit output and must contain the following:

1. Identification of Auditee (Address & contact information)
2. Dates and Location(s) of audit
3. Terms of reference (as agreed between the Auditee and Auditor), including the standard for Audit, if any.
4. Audit plan.
5. Additional mandatory or voluntary standards or regulations applicable to the Auditee.
6. Audit Standards should be followed.
7. Summary of audit findings including identification tests, tools used and results of tests performed (like vulnerability assessment, application security assessment, password cracking and etc.)
    i. Tools used
    ii. List of vulnerabilities identified
    iii. Description of vulnerability
    iv. Risk rating or severity of vulnerability
    v. Test cases used for assessing the vulnerabilities
    vi. Illustration if the test cases to provide the vulnerability
    vii. Applicable screen dumps
8. Analysis of vulnerabilities and issues of concern.
9. Recommendations for action.
10. Personnel involved in the audit.

The auditor may further provide any other required information as per the approach adopted by the demand which they feel is relevant to the audit process.