I/23879/2023

Government of Kerala
Department of Electrical Inspectorate
Office of the Chief Electrical Inspector
Housing Board Buildings, Shanthi Nagar
Thiruvananthapuram 695 001
Phone: 0471 2330558 , 0471 2331104
Email : cei.kerala@kerala.gov.in, ceikerala@gmail.com
Web site: www. ceikerala.gov.in

An IS 15700 : 2018 Certified Department

No:CEI/5572/2023-G1 Dated: 04-09-2023

Request for Proposal

Proposal is invited for the security audit of the web application (SURAKSHA) developed for Department of Electrical Inspectorate with scope of work as spe cified below.

Scope of Work

Application Security Audit covers some or all but not limited to the following activities:

- Identify the application level vulnerabilities on applications hosted in a test site / production site based on the latest top 10 OWASP vulnerabilities
- On demand application scans
- An audit of the environment along with the application to ascertain any vulnerability in the environment where the application is hosted.
- Password strength on authentication pages
- Scan Java Script for security vulnerabilities
- File inclusion attacks
- Web Server Information security
- Malicious File Uploads
- Provide recommendations for remediation of identified vulnerabilities. The report should contain discovered vulnerabilities and description of
- vulnerabilities and mitigation or remediation recommendations for fixing and patching of existing and found vulnerabilities as a part of solution.
- Follow a specific format for reports.
- Certify the applications / websites tested as “Safe for Hosting” and in times of Electronic Payment Gateway Operators request to provide it in their format.
- Accept responsibility for declaring the websites / URLs / mobile applications free from known vulnerabilities
- Any other activity conceding security audit related aspects; not essentially covered by work-areas outlined above.
- The selected vendor may cover the below mentioned tests for the application or website provided for testing:

1. Application Security Audit
2. Penetration Testing

3. Vulnerability Testing
4. Database Server Controls
5. Physical Access Control
6. Network security Review as part of Application Security
7. Compliance Review

- Black box testing for Security Audit should follow OWASP guidelines covering to the testing below:

1. Cross-site scripting (XSS)
2. Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.
3. Input Validation flaws
4. Malicious file execution
5. Insecure direct object references
6. Cross-site request forgery (CSRF)
7. Information leakage and improper error handling
8. Broken authentication and session management
9. Insecure cryptographic storage
10. Insecure Communications
11. Failure to restrict URL access
12. Denial of Service

- Audit shall cover all requirements specified in the Government Order GO (Ms) No 8/2019/ITD dated 22.04.2019.
- Rate of service shall be as specified in the Government Order GO (Ms) No 8/2019/ITD dated 22.04.2019

Details of Web Application to be assessed

Sl.No	Assessment Details	Description
Web Application		
1	How many web application instance to assesses?	1
2	How many login systems to assesses?	2
3	How many static pages to assesses? (Approximate)	2
4	How many dynamic pages to assesses? (Approximate)	60
5	Do you need fuzzing performed against this application?	No

6	Do you need want role-based testing performed against this application?	Yes
7	Do you need want credentialed scans of web applications performed?	No
8	Back-end Database(MS-SQL Server, PostgreSQL, Oracle, etc.)	PostgreSQL
9	Authorization No. of roles & types of privileges for the different roles	1. Public Users 2. Office Users
10	Whether the application contains any content management module (CMS) (If yes then which?) If its is Portal do mention please	1. Letter Generation Pages (Ck Editor) 2. Certificate Generations pages (Ck Editor)
11	Front-end Tool [Server side Scripts] (i.e. ASP, Asp.NET, JSP, PHP, etc.) – PHP	PHP - Laraval
12	Operating System Details(i.e.Windows-2003, Linux, AIX, Solaris, etc.)	Ubuntu 20.04 LTS
13	Application Server with Version (i.e. IIS 5.0.Apache, Tomcat, etc.)	Apache
14	Total No. (Approximate) of Input Forms	80
15	Total No. of input field (Approximate)	250
16	Total No. of login modules	2
17	Number of Web Services, if any	1
18	Number of methods in all web services ?	20
19	Number of URL requires to assess	One

20	Application Type – REST/SOAP based	REST

Other Terms and conditions for compliance by the vendors

The acceptance of the proposal will be subject to the following conditions:

1. roposal shall be submitted two weeks from the date of RFQ. Proposals received after cutoff date will not be considered.
2. The bidder should be a CERT-IN empaneled or Government approved security auditing form.
3. For security auditing of Government assets, the vendor shall not Charge cost exceeding the rates finalized by the Government.
4. The vendor shall conduct a pre-assessment to understand the audit requirements of the organization/Department and shall provide the draft scope of work in detail at free of cost, if requested by the department.
5. The vendor shall provide the first audit report not later than 3 weeks from receiving the work order. Subsequent interim reports shall be issued not later than 8 working days of receiving the patched application for re-test.
6. For any audit engagement, besides the original first audit, the vendor shall do any number of re-tests at no additional cost till all issues are cleared by the user department within 90 working days of providing the first audit report. It should also ensure no new vulnerabilities are introduced as part of code changes to fix the reported vulnerabilities.
7. The vendor may be terminated from audit engagements for reasons such as dishonouring audit commitments or violating these terms and conditions, degradation of auditor's performance or competence to meet expectations or if empanelment at CERT-India ceases.
8. The audit report provided by the auditor shall have details of corrective action to be taken and steps to remove the identified vulnerabilities.
9. For any audit engagement, the vendor shall provide support to the auditee technical team in fixing the security issues reported in first audit or any subsequent audit in terms of handholding and training. The support should include a minimum of 1 day onsite or remote training or handholding on how to fix the issues.
10. The vendor shall adhere to all terms and conditions as per agreement with CERT-India.
11. The vendor shall not sub contract any part of work assigned to another vendor or engage non-employees to perform the work.
12. A formal Confidentiality & Non-Disclosure Agreement should be signed by the vendor to keep confidential all the information that it has access to during the course of its actions. Employees at the vendor Organization should sign individual NDAs. As per CERT-In advisory, the empanelled vendor must ensure that data collected during audit work and reports prepared are not taken out of the auditee organization’s premises/ network and/ or shared to anyone except the auditors, auditee Organization, CERT-ln and any other authorised Government entity. Any audit data should be wiped out from the vendor’s domain after any engagement.
13. In the case of Application Vulnerability Assessment/ Penetration Testing (VAPT), the Auditor will be required to audit and test the website on the staging server/testing environment provided

by hosting Service provider before issuing the audit certificate.

14. The vendor shall provide any audit report or data as required by KSITM with respect to audits perfumed for Government of Kerala.
15. Withdrawal from the proposal after it is accepted or failure to service within a specified time or according to specifications will entail cancellation of the order and purchases being made at the offerer's expenses from elsewhere, any loss incurred thereby being payable by the defaulting party. In such an event the Government reserves also the right to remove the defaulter's name from the list of Government suppliers permanently or for a specified number of years.
16. No representation for enhancement of price once accepted will be considered during the currency of the contract.
17. Any attempt on the part of tenderers or their agents to influence the Officers concerned in their favour by personal canvassing will disqualify the tenderers.
18. If any license or permit is required, tenderers must specify in their proposal and also state the authority to whom application is to be made.
19. Any sum of money due and payable to the contractor (including Security Deposit returnable to him) under this contract may be appropriated by the Purchasing Officer or Government or any other person authorized by Government and set-off against any claim of the Purchasing Officer or Government for the payment of a sum of money arising out of or under any other contract made by the contractor with the Purchasing officer or Government or any other person authorized by Government.
20. The prices quoted should be inclusive of all taxes, duties, cesses, etc., which are or may become payable by the contractor under existing or future laws or rules of the country of origin/supply or delivery during the course of execution of the contract.
21. Process of procurement will be as per the conditions mentioned in GO (Ms) No 8/2019/ITD dated 22.04.2019. Payment will be released only after issue of the final audit report and Security Audit Certificate.
22. Any sum of money due and payable to the successful tenderer or contractor from Government shall be adjusted against any sum of money due to Government from him under any other contracts.
23. Special conditions, if any, printed on the proposal sheets of the tenderer or attached with the tender will not be applicable to the contract unless they are expressly accepted in writing by the purchases.

Signed by Vinod G
Date: 04-09-2023 11:45:19
Chief Electrical Inspector In Charge