No. VSEZ-DC0G/5/2023-SEZ VIZAG

Date: 03-08-2023

Notice Inviting Quotations for Security Audit of VSEZ Website

Visakhapatnam Special Economic Zone under Ministry of Industry & Commerce, Department of Commerce, Govt. of India has developed Website to provide information to the various stake holders.

Sealed quotations are invited from the interested and willing Security Audit Agencies empanneled with Cert-in, to get the complete Security Audit of VSEZ Website. The quotations exclusive of GST for security audit of VSEZ Website along with the empanelled letter from Cert-in must be sent to the "Development Commissioner, Visakhapatnam Special Economic Zone, Administrative Building, Duvvada, Visakhapatnam-530049 latest by **24-08-2023 by 11.00 AM**. The sealed quotations will be opened on **24-08-2023 at 12.00 PM** in the office of the Development Commissioner, VSEZ, Administrative Building, Duvvada, Visakhapatnam. The authorised representatives of the quotationers may be present during the opening of the quotations. Quotations received after the scheduled date and time will not be entertained and no request in this regard will be considered.

The scope of work for Security Audit of VSEZ Website is given in Annexure-I. The details of Web application of VSEZ is attached as Annexure-II.

Security Audit of Website should be completed within **7 (seven) days** of the request made for the same.

The Department reserves the right to cancel the published notice done without any assigning any reasons on administrative grounds.

In case of any further query, the concerned may contact Shri K. V. Prasanna Kumar, Asst. Development Commissioner at Cell No.9866499929.

The Notice is also available at VSEZ Website www.vsez.gov.in

(K. SRINIVAS)
Asst. Development Commissioner

Scope of Work : Security Audit of VSEZ Website

1. Quotationers would be expected to perform the following tasks for websites to analyse and review the website. The auditors will have to carry out an assessment of the vulnerabilities that exist in website through Internet vulnerability assessment and penetrating testing.

2. This will include indentifying remedial solutions and recommendations for implementation of the same to mitigate all identified risks, video objective of enhancing the security of the website. The quotationer will also be expected to propose risk mitigation strategy as well give specific recommendation to tackle the residual risks emerging out of identified vulnerabilities assessment. The website should be audited as per the industry standards and the Govt. of India guidelines. The auditor is expected to submit the final audit report after the remedies/recommendations are implemented. The final report will certify the Website"Certified for Security". The scope of the proposed audit tasks is given below. The audit firm/company will be required to prepare the checklist/reports.

Task : 1

To check various web attacks. The various checks/attacks/vulnerabilities should cover the following or any type of attacks which are vulnerable to the website.

- Vulnerabilities
- Authentication Hacking/attacks
- Password strength on authentication pages
- File inclusion attacks
- Remotely exploitable vulnerability
- Web server information security
- Cross site scripting
- HTTP injection
- Phishing a website
- Buffer overflow, invalid inputs, insecure storage etc
- Any other vulnerable attack
- Additional mandatory or voluntary standards or regulations.

The quotationer will be responsible to provide a detailed recommendations report for the vulnerabilities observed in Task - 1

Task : 2 - Re-audit based on the Recommendations Report from Task -1

The quotationer will be responsible to provide a detailed recommendations report for the vulnerabilities observed in Task - 2

Task -3 : - Re-audit, if required based on the Recommendation Report from Task – 2

If vulnerabilities are observed from the re-audit, the vendor has to provide a detailed recommendations report on the vulnerabilities observed or found from Re-audit/Task-2. The Audit firm has to submit a summary compliance report at the end of each task and the

final report should certify that the website (should mention the name of the Website) is "Certified for Security".

The audit of the website should be conducted in conformity with guidelines of National Informatics Centre (NIC) for website security audit. After successful audit of the website, the security audit report from the auditor should clearly state that all web pages along with respective linked data files (in pdf/doc/xlsetc formats), all scripts and image files are free from any vulnerability or malicious code, which could be exploited to compromise and gain unauthorised access with escalated privileges into the webserver system hosting the said website.

Technical Details of the application are as follows:

Sl. No.	Parameters/ Information about the website	Description
1.	Web application name & URL	VSEZ www.vsez.gov.in
2.	Operating system details	Windows 2008 R2
3.	Application server with Version	Web Root
4.	Development platform for application:	ASPX
5.	Back-end Database	No Database
6.	Authorization No. of roles & types of privileges for the different roles	NIL
7.	Whether the site contains any content management module (CMS)	No
8.	No. of input forms	No input forms
9.	No. (Approximate) of input fields	Zero
10.	No. of login modules	NIL
11.	How many application roles/privilege levels of users?	NIL
12.	Does the application provide a file download features (Yes/No)	Yes
13.	Does the application use Client-side certificate (Yes/No)	No
14.	Is there a CMS (Content Management System) present to maintain the public portal/login module/	No
15.	Tentative Testing environment (Development/Staging/Production Box)?	Staging
16.	Does the application has SMS integration (Yes/No)	No
17.	Does the application has E-Mail integration (Yes/No)	No
18.	Does the application has Payment Gateway integration (Yes/No)	No
19.	Does the application provide a file upload feature (Yes/No)	No
20.	Detail of total number of pages (Static/Dynamic and separate counting for separate platform/front end used) – Count	
	Static Pages (Name of Platform used to design)	0
	Dynamic Pages (Name of Front End tool used to design and develop)	45 Pages approximately
	Total Pages	45 Pages approximately