Rockwell Road, HMT Colony PO,
Kalamassery, Cochin - 683 503
0484 2550322, 2532890.
ceo.kied@gmail.com
www.kied.info

KIED
Kerala Institute for Entrepreneurship Development

Quotation Notice for conducting the Security Audit of web applications of EDC- **Kerala Institute for Entrepreneurship Development (KIED)**, from CERT-In empanelled agencies.

Quotation No. KIED/SQN/2024/004

Kerala Institute for Entrepreneurship Development (KIED) is an autonomous State level institute promoted by the Government of Kerala. The main objective of the Institute is to provide training in the field of entrepreneurship development and to set up Enterprise Development Centres (EDCs) across Kerala. In this direction a web has been developed with Payment Gateway to enable Easy Monitoring of various activities under EDC project. KIED is inviting quotations from CERT-In Empanelled Agencies for Security audit of below mentioned applications. These applications need to obtain the "safe-to-host" certificates from CERT-In empanelled agencies before hosting the same on State Data Centre. The applications is - **www.edckerala.org**

Bidders are advised to study the document carefully. The Cost estimates may please be provided in the **sealed envelope** and should reach by **SPPED/REGISTERED POST** to the **below mentioned address latest by 07/06/2024, 1500 Hrs (3.PM).** (Please see Annexure-IV)

The **sealed quotation** is to be raised in the name of following –

Chief Executive Officer and Executive Director,
Kerala Institute for Entrepreneurship Development (KIED),
Rockwell Road, HMT Colony P.O, Kalamasserry, Ernakulam-683503

Quotation document with other details is also available on KIED website i.e. www.kied.info

CEO & Executive Director,

KIED

Place for opening of thebid	Conference Room K**erala Institute for Entrepreneurship Development (KIED)**,Rockwell Road, HMT Colony P.O, Kalamasserry, Ernakulam-683503.
Last Date & Time of Submission of Bid	07/06/2024, 1500 Hrs (3 PM)
Date & Time of Opening of Bid	07/06/2024, 1600 Hrs (4 PM)

Name of the Bidding Firm:	**Kerala Institute for Entrepreneurship Development (KIED)**, Rockwell Road, HMT Colony P.O, Kalamasserry, Ernakulam, PIN-683503
Contact Person	K. P. Sreesarath Assistant Manager (Insight)
Correspondence Address:	**Kerala Institute for Entrepreneurship Development (KIED)**, Rockwell Road, HMT Colony P.O, Kalamasserry, Ernakulam-683503
Mobile No: **Telephone:**	9633050143 0484-2550322 0484-2532890
Website	www.edckerala.org
Official E-mail Address	1. ceo.kied@gmail,com 2. am.insight@kied.in.

ANNEXURE-I

(A) General Conditions

1. The web applications will be hosted at State Data Centre after Security audit, so the security audit certificate should be in compliance with the Cert-In standards and as per the guidelines issued by the Government vide Order GO.(MS).No.8/2019/ITD dated 22/04/2019 and subsequent orders in force.
2. The envelope shall be marked on top with **"QUOTATION FOR CONDUCTING THE SECUIRTY AUDIT OF WEB APPLICATIONS OF EDC- KIED"**. The envelop should be properly sealed.
3. The quotations should reach this office by 07/06/2024, 1500 Hrs (3PM).
4. The price bids of those firms will be opened who fulfils the terms and conditions.
5. The main objective of this quotation is to obtain mandatory "Safe to host Certification "from a CERT-In empaneled Security Auditing Agency.
6. Only those Organizations/firms registered with the CERT-in-empaneled are eligible for submitting the quotation.
7. Incomplete or conditional quotation will not be entertained.
8. No quotation will be accepted after closing date and time
9. The first security audit report should be submitted to KIED within 3 weeks from the date of receipt of the work order issued by the KIED and consecutive report if any, should be submitted within 8 working days of receiving the patched application for re-test.
10. The offer or authorized representative may remain present at the time of opening the quotation.
11. Any firm/organization blacklisted by a Government/Semi Government Department shall not be considered for this quotation and quotation will be rejected straightway.
12. The payment will be made only after submitting the final security audit certificate on completion of Audit of website.
13. No claim for interest or charges of any other nature in case of delayed audit work completion will be entertained by the KIED.
14. Quotation must be submitted in prescribed format given in Annexure-IV
15. The KIED reserves the right to relax any terms and condition in the Public/Government interest.
16. All disputes are subject to the jurisdiction of the Courts in the Ernakulam District.

(B) DOCUMENTS REQUIRED TO BE ATTACHED WITH BID:

1. Copy of GST Registration Certificate and PAN Card.
2. Copy of authorization with current CERT-in empanelment.
3. All the firms participating in the Quotation must submit a list of their owners/partners etc. and ***a Certificate to the effect that the firm is neither blacklisted by any Government Department or Public***

Sector Units nor any Criminal Case is registered against the firm or its owner or partners anywhere in India.

4. All Other supporting documents as required in the quotation shall be attached

(C) Quotation should be in the format given at Annexure-IV

ANNEXURE-II

KIED is in the process of building capacity in the area of Enterprise Development and training and therefore efforts are being made to put in place a robust and reliable online facility, which would assist the trainees and entrepreneurs to submit applications required for training programmes and co-working space allotment with online fees/rent payment facility. This application is developed to monitor and collect the data related to various training and activities conducted by the EDC-KIED.

Primary objective of the security audit exercise is to identify major vulnerabilities in the web application from internal and external threats. Once the threats are identified and reported the auditors should also suggest possible remedies.

Technical Details of the applications are as follows:

Web software has been developed to enable Easy Monitoring of various activities at EDC-KIED. Currently, the following modules have been implemented in AIMS:

i. Events/Training Programmes Information Management System.
ii. Finance Information Management System integrating Payment Gateway.
iii. Document Sharing System
iv. Payment gateway etc.

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

1. Identify the application level vulnerabilities on applications hosted in a test site /production site based on the latest top 10 OWASP vulnerabilities

2. On demand application scans

3. An audit of the environment along with the application to ascertain any vulnerability in the environment where the application is hosted.

4. Password strength on authentication pages

5. Scan Java Script for security vulnerabilities

6. File inclusion attacks

7. Web server information security

8. Malicious File Uploads

9. 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.

10. Follow a specific format for reports.

11. Certify the applications/ websites tested as "Safe for Hosting" and in times if Electronic Payment Gateway Operators request to provide it in their format.

12. Accept responsibility for declaring the websites / URLs/mobile applications free from known vulnerabilities

13. Payment Gateway integration and security.

14. Any other activity concerning security audit related aspects.

15.The parameters, terms, conditions, scope, activities, guidelines, and directives of the security audit encompass all facets, inclusive but not exhaustively limited to the Government guidelines in GO.(MS).No.8/2019/ITD dated 22/04/2019 and GO.(MS).No44/2021/ITD dated 22/12/2021 and subsequent orders in vogue.

(B) Scope of work and deliverables

I) Security audit for Web or browser based application and Website 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
4. Physical Access Control
5. Network security Review as part of Application Security
6. Compliance Review

II) 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

III) Scope of security audit for Desktop based application

1. Test user's rights and roles-authorized person should allow to login

2. Test security of data or information stored in application

3. Role based Security (Privilege Escalation)

4. Authentication Bypass or Unauthorized Access

5. Improper Error handling

6. Buffer Overflow

7. Denial of Services

8. Insecure Communications

9. Insecure Cryptographic Storage

(C) Information about the application has been given in Annexure-III

(D) TERMS AND CONDITIONS

1. For audit engagement, 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 organization.

2. The vendor shall provide the first audit report to the KIED 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.

3. 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.

4. The vendor may be terminated from audit engagements for reasons such as dishonoring 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.

5. The audit report provided by the auditor shall have details of corrective action to be taken and steps to remove the identified vulnerabilities.

6. 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.

7. The vendor shall adhere to all terms and conditions as per agreement with CERT-India.

8. The vendor shall not sub contract any part of work assigned to another vendor or engage non-employees to perform the work.

9. 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-In and any other authorized Government entity. Any audit data should be wiped out from the vendor's domain after any engagement.

10. 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

11. The vendor shall provide any audit report or data as required by KSITM with respect to audits performed for the KIED.

12. To ensure that web based applications is free from the vulnerabilities of any nature. The audit exercise will need to undertake the following activities:

i) Identify the security vulnerabilities, which may be discovered during website security audit including cross-site scripting, Broken links/Weak session management, Buffer Overflows, Forceful browsing, Form/ hidden field manipulation, Command injection, Insecure use of cryptography, Cookie posing, SQL injection, Server miss- configuration, Well known platform vulnerabilities, Errors triggering sensitive information, leak etc.

ii) Identification and prioritization of various risks to the KIED online web applications

iii) Identify remedial solutions and recommendations for making the web applications secure.

iv) Undertake user profiling and suggest specific access methodologies and privileges for each category of the users identified.

v) The auditors will have to carry out an assessment of the vulnerabilities, threats and risks that exist in web application through Internet Vulnerability Assessment and Penetration Testing. This will include identifying remedial solutions and recommendations for implementations of the same to mitigate all identified risks, with the objective of enhancing the security of the system.

vi) Applications should be audited as per the CERT-in Standards. The auditor is expected to submit the final audit report after the remedies/recommendations are implemented and confirmed with retest.

vii) The Audit Firm/company has to submit a summary compliance report at the end of the assessment phase and the final Report will certify that EDC-KIED web applications are incompliance with the standards.

Deliverables and Audit Reports

The successful bidder will be required to submit the following documents in printed format (2 copies each) after the audit of above mentioned web application:

(i) A detailed report with security status and discovered vulnerabilities weakness and mis-configurations with associated risk levels and recommended actions for risk mitigations especially with respect to payment gateway.

(ii) Summary and detailed reports on security risk, vulnerabilities and audit with the necessary counter measures and recommended corrective actions to be undertaken by KIED.

(iii) The vendor will be required to submit the deliverables as per terms and conditions of this document.

ANNEXURE-III

	Client Details	
	Name of Organisation	**Kerala Institute for Entrepreneurship Development**
	Address	**HMT Colony, Rockwell Road, Kalamassery, Kochi**
	Billing Address	**CEO & Executive Director - KIED**
	Contact Person	9633050143
	Contact Number	9633050143
	E-mail	ceo.kied@gmail.com
	GSTN	**32AAATK4049H1ZV**
Web Application Scoping Sheet for Security Assessment		
Sl.No.	**Web Application Assessment Details**	**Description**
1	Web Application Name & Description	**EDC website and cms** : Experience seamless engagement with our integrated platform. Users effortlessly log in, register for exclusive events and programs, and stay informed with curated news and articles from KIED. Admins wield control through a dedicated portal, managing content updates, event registrations, and user approvals with precision and efficiency. Elevate your interaction experience with us.
2	Type of application Web/Application/ Mob/Rest / Thick / Thin instance to assesses & number of Application (s)	Web Application
3	How many login systems to assesses?	9 users, 5 admin
4	How many static pages to assesses? (Approximate)	20 + user side , 10 admin
5	How many dynamic pages to assesses? (Approximate)	35 + User Side, 40 + admin
6	Do you need want role-based testing performed against this application?	yes

7	Do you need want credentialed scans of web applications performed?	yes
8	Back-end Database (MS-SQL Server, PostgreSQL, Oracle, etc.)	Maria db
9	Authorization No. of roles & types of privileges for the different roles	9 users + 5 admin roles roles :
10	Whether the application contains any content management module (CMS) (If yes then which?) If its is Portal do mention please	yes, portal
11	Is it a hybrid application?	no
12	Whether the application was security audited earlier? If so, please mention details.	no
13	Front-end Tool [Server side Scripts] (i.e. c++, J2eee, ASP, Asp.NET, JSP, PHP, etc.) – PHP	php
14	Operating System Details (i.e.Windows-2003, Linux, AIX, Solaris, etc.)	linux
15	Application Server with Version (i.e. IIS 5.0.Apache, Tomcat, etc.)	Apache – 2.4.58
16	Total No. (Approximate) of Input Forms	More than 10
17	Total No. of input field	More than 100
18	Total No. of login modules	9 +5
19	Number of Web Services, if any	More than 100
20	Number of methods in all web services ?	4
21	Number of URL's require to assesses ?	1 for user side, 1 for admin panel
22	Is this REST /SOAP based Application	REST
23	Is it Thick or Thin Client Application	Thin
24	Is this Applications is ERP/ Enterprised based App	No
25	Does the application has or proposed to have payment gateway integration? Please specify	yes, HDFC (cc avenue)
26	Is Application hosted in Cloud ? If yes which under cloud provider private & others (Govt SDC)	Govt SDC

S. No.	Required service information	Description
1	What services do you expose to the internet? (Examples: Web, database, FTP, SSH, etc.)	Web
2	What type of authentication do you use for your web services? (Examples: PubCookie, Windows Integrated, htaccess, etc.)	ht access
3	What languages do you use for your web services? (Examples: PHP, Perl, Ruby, ASP, etc.)	php
4	What antivirus application (s) do you use?	nil
5	Is your antivirus application implemented using a "managed" client/server architecture, or in a stand-alone configuration?	no
6	What Enterprise Resource Planning (ERP/MIS) application (s) does your organization use? (Examples – SAP, Peoplesoft, Oracle, JD Edwards), Any Other Vender Applications.	NA
7	Please include a brief description of each.	
8	What E-commerce application (s) does your organization use? Please include a brief description of each.	
9	What database technologies does your organization use? (Examples – Oracle, Microsoft SQL, IBM DB2, MySQL) . Please include a brief description of the purpose for each.	MY SQL
10	What services do you expose to the end users in internet?	

S.No	Details About Business Applications and related database system-	Please fill it up wherever require necessary or appropriate
1	Application Name and Description detailed	Edc website and cms : Experience seamless engagement with our integrated platform. Users effortlessly log in, register for exclusive events and programs, and stay informed with curated news and articles from KIED. Admins wield control through a dedicated portal, managing content updates,

		event registrations, and user approvals with precision and efficiency. Elevate your interaction experience with us.
2	Primary programming language used to develop the application	PHP, React js
3	Additional components, used in the application, which are developed in the programming languages other than the primary language.	
4	Is the architecture document of the application available? (Yes/No)	No
5	Does the application process any data which falls under the PCI-DSS, HIPPA, etc. international standards/regulations? If yes, then Please specify.	No
6	Is security incorporated in the SDLC of the application? (Yes/No)	Yes
7	Backend database used in the application.	Maria db
8	Type of the application.	
	●CMS based application	**yes**
	●Custom developed application	Yes
9	Any third party library used in the application? (Yes/No)	Yes
10	How is access control enforced in the application e.g. database role mapping, per page access checks?	database role mapping, per page access checks
11	How data access layer is implemented?	
	●Dynamic SQL strings	yes
	●Stored Procedures	
	●Prepared Statements	
12	What authentication mode is implemented?	
	●SSO	
	●Form based login	yes
	●LDAP authentication	

	●Other	
13	No of user roles in the application	9 users + 5 admin roles roles :
14	No of application users	200
15	Any protocols other than HTTP or HTTPS used in the application.	no
16	Is the application accessible over the internet? (Yes/No)	yes
17	Total number of web servers and their details.	Apache , Nginx
18	Total number of application servers and their hardware details.	
19	Total number of database servers and their hardware details	Maria db
20	No of total code files in the application	More than 200
21	At what instance of the application this security assessment will be conducted?	
	●Production	
	●UAT	Yes
22	Is web application firewall used to protect the application? (Yes/No)	No
23	Is load balancer/ Application firewall used to analyze and balance the traffic? (Yes/No)	no
24	Details About Current Application layout and Architecture	
	●Diagram	
	●Work Flow	Yes
	●Any issues you faced in past, current on security aspect in your applications.	

For each Application whether its web or mobile please fill in different sheet

If mobile applications requirement is there then kindly fill it up

S. No.	Mobile Applications - Android Parameters	Details
1	Number of Screens in Mob app	
2	Total No. of Input Forms	
3	Total No. Parameters in API	
4	Total No of Input fields	
4	Total No of User Roles such as admin, manager, user	
5	Type of App such as Native apps or Mobile web Apps, or Hybrid Apps	
6	Technologies such as HTML, CSS, asp.net, Java, PHP or any details	
7	Backend web Services & Database	
S. No.	**Mobile Applications - iOS Parameters**	**Details**
1	Number of Screens in Mob app	
2	Total No. of Input Forms	
3	Total No. Parameters in API	
4	Total No of Input fields	
4	Total No of User Roles such as admin, manager, user	
5	Type of App such as Native apps or Mobile web Apps, or Hybrid Apps	
6	Technologies such as HTML, CSS, asp.net, Java, PHP or any details	
7	Backend web Services & Database	

ANNEXURE-IV

QUOTATION FOR CONDUCTING THE SECUIRTY AUDIT OF WEB APPLICATION OF EDC- KIED

QUOTATION / BID (On Company Letter Head)

1. Name of the Bidder :

2. Address for Correspondence :

3. Contact number :

4. e-mail :

I/we hereby submit the quote for conducting Security Audit of web application of EDC-KIED as per the Scope of work given and within the time specified and in accordance with the terms and conditions of Quotation Notice.- **KIED/SQN/2024/004** Dated:23-05-2024.

Description	**Price Quoted (in Rs)**	**Tax (if any)**	**Total Cost (Rs.)**
(i)	**(ii)**	**(iii)**	**(iv)**
Security Auditing of website www.edckerala.org			

Thus the total amount quoted including GST and applicable all other charges is Rs……./-

(Rupees…… …… ……...)

The rate quoted rate must be valid for the period of contract fromthe date of opening of financial bid.

Place- Signature-

Date- Name of the authorized Signatory.

(Seal of the Company /Firm)

I/513857/2024

Quotation Notice for conducting the Security Audit of web applications of EDC- **Kerala Institute for Entrepreneurship Development (KIED)**, from CERT-In empanelled agencies.

Quotation No. KIED/SQN/2024/004 **25-05-2024**

Kerala Institute for Entrepreneurship Development (KIED) is an autonomous State level institute promoted by the Government of Kerala. The main objective of the Institute is to provide training in the field of entrepreneurship development and to set up Enterprise Development Centres (EDCs) across Kerala. In this direction a web has been developed with Payment Gateway to enable Easy Monitoring of various activities under EDC project. KIED is inviting quotations from CERT-In Empanelled Agencies for Security audit of below mentioned applications. These applications need to obtain the "safe-to-host" certificates from CERT-In empanelled agencies before hosting the same on State Data Centre. The applications is - **www.edckerala.org**

Bidders are advised to study the document carefully. The Cost estimates may please be provided in the **sealed envelope** and should reach by **SPPED/REGISTERED POST** to the **below mentioned address latest by 07/06/2024, 1500 Hrs (3.PM)**. (Please see Annexure-IV)

The **sealed quotation** is to be raised in the name of following –

Chief Executive Officer and Executive Director,
Kerala Institute for Entrepreneurship Development (KIED),
Rockwell Road, HMT Colony P.O, Kalamasserry, Ernakulam-683503

Quotation document with other details is also available on KIED website i.e. www.kied.info

CEO & EXECUTIVE DIRECTOR

CEO & Executive Director,
KIED

Place for opening of the bid	Conference Room K**erala Institute for Entrepreneurship Development (KIED)**, Rockwell Road, HMT Colony P.O, Kalamasserry, Ernakulam-683503.
Last Date & Time of Submission of Bid	07/06/2024, 1500 Hrs (3 PM)
Date & Time of Opening	07/06/2024, 1600 Hrs (4 PM)

of Bid	

Name of the Bidding Firm:	**Kerala Institute for Entrepreneurship Development (KIED)**, Rockwell Road, HMT Colony P.O, Kalamasserry, Ernakulam, PIN-683503
Contact Person	K. P. Sreesarath Assistant Manager (Insight)
Correspondence Address:	**Kerala Institute for Entrepreneurship Development (KIED)**, Rockwell Road, HMT Colony P.O, Kalamasserry, Ernakulam-683503
Mobile No: **Telephone:**	9633050143 0484-2550322 0484-2532890
Website	www.edckerala.org
Official E-mail Address	1. ceo.kied@gmail,com 2. am.insight@kied.in.

ANNEXURE-I

(A) General Conditions

1. The web applications will be hosted at State Data Centre after Security audit, so the security audit certificate should be in compliance with the Cert-In standards and as per the guidelines issued by the Government vide Order GO.(MS).No.8/2019/ITD dated 22/04/2019 and subsequent orders in force.
2. The envelope shall be marked on top with **"QUOTATION FOR CONDUCTING THE SECUIRTY AUDIT OF WEB APPLICATIONS OF EDC- KIED"**. The envelop should be properly sealed.
3. The quotations should reach this office by 07/06/2024, 1500 Hrs (3PM).
4. The price bids of those firms will be opened who fulfils the terms and conditions.
5. The main objective of this quotation is to obtain mandatory "Safe to host Certification "from a CERT-In empaneled Security Auditing Agency.
6. Only those Organizations/firms registered with the CERT-in-empaneled are eligible for submitting the quotation.
7. Incomplete or conditional quotation will not be entertained.
8. No quotation will be accepted after closing date and time
9. The first security audit report should be submitted to KIED within 3 weeks from the date of receipt of the work order issued by the KIED and consecutive report if any, should be submitted within 8 working days of receiving the patched application for re-test.

I/513857/2024

10. The offer or authorized representative may remain present at the time of opening the quotation.
11. Any firm/organization blacklisted by a Government/Semi Government Department shall not be considered for this quotation and quotation will be rejected straightway.
12. The payment will be made only after submitting the final security audit certificate on completion of Audit of website.
13. No claim for interest or charges of any other nature in case of delayed audit work completion will be entertained by the KIED.
14. Quotation must be submitted in prescribed format given in Annexure-IV
15. The KIED reserves the right to relax any terms and condition in the Public/Government interest.
16. All disputes are subject to the jurisdiction of the Courts in the Ernakulam District.

(B) DOCUMENTS REQUIRED TO BE ATTACHED WITH BID:

1. Copy of GST Registration Certificate and PAN Card.
2. Copy of authorization with current CERT-in empanelment.
3. All the firms participating in the Quotation must submit a list of their owners/partners etc. and ***a Certificate to the effect that the firm is neither blacklisted by any Government Department or Public Sector Units*** nor any Criminal Case is registered against the firm or its owner or partners anywhere in India.
4. All Other supporting documents as required in the quotation shall be attached

(C) Quotation should be in the format given at Annexure-IV

ANNEXURE-II

KIED is in the process of building capacity in the area of Enterprise Development and training and therefore efforts are being made to put in place a robust and reliable online facility, which would assist the trainees and entrepreneurs to submit applications required for training programmes and co-working space allotment with online fees/rent payment facility. This application is developed to monitor and collect the data related to various training and activities conducted by the EDC-KIED.

Primary objective of the security audit exercise is to identify major vulnerabilities in the web application from internal and external threats. Once the threats are identified and reported the auditors should also suggest possible remedies.

Technical Details of the applications are as follows:

Web software has been developed to enable Easy Monitoring of various activities at EDC-KIED. Currently, the following modules have been implemented in AIMS:

i. Events/Training Programmes Information Management System.
ii. Finance Information Management System integrating Payment Gateway.
iii. Document Sharing System
iv. Payment gateway etc.

I/513857/2024

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

1. Identify the application level vulnerabilities on applications hosted in a test site /production site based on the latest top 10 OWASP vulnerabilities

2. On demand application scans

3. An audit of the environment along with the application to ascertain any vulnerability in the environment where the application is hosted.

4. Password strength on authentication pages

5. Scan Java Script for security vulnerabilities

6. File inclusion attacks

7. Web server information security

8. Malicious File Uploads

9. 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.

10. Follow a specific format for reports.

11. Certify the applications/ websites tested as "Safe for Hosting" and in times if Electronic Payment Gateway Operators request to provide it in their format.

12. Accept responsibility for declaring the websites / URLs/mobile applications free from known vulnerabilities

13. Payment Gateway integration and security.

14. Any other activity concerning security audit related aspects.

15.The parameters, terms, conditions, scope, activities, guidelines, and directives of the security audit encompass all facets, inclusive but not exhaustively limited to the Government guidelines in GO.(MS).No.8/2019/ITD dated 22/04/2019 and GO.(MS).No44/2021/ITD dated 22/12/2021 and subsequent orders in vogue.

(B) Scope of work and deliverables

I) Security audit for Web or browser based application and Website 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
4. Physical Access Control
5. Network security Review as part of Application Security
6. Compliance Review

II) 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

III) Scope of security audit for Desktop based application

1. Test user's rights and roles-authorized person should allow to login
2. Test security of data or information stored in application
3. Role based Security (Privilege Escalation)
4. Authentication Bypass or Unauthorized Access
5. Improper Error handling
6. Buffer Overflow
7. Denial of Services
8. Insecure Communications
9. Insecure Cryptographic Storage

(C) Information about the application has been given in Annexure-III

(D) TERMS AND CONDITIONS

1. For audit engagement, 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 organization.

2. The vendor shall provide the first audit report to the KIED 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.

3. 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.

4. The vendor may be terminated from audit engagements for reasons such as dishonoring 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.

5. The audit report provided by the auditor shall have details of corrective action to be taken and steps to remove the identified vulnerabilities.

6. 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.

7. The vendor shall adhere to all terms and conditions as per agreement with CERT-India.

8. The vendor shall not sub contract any part of work assigned to another vendor or engage non-employees to perform the work.

9. 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-In and any other authorized Government entity. Any audit data should be wiped out from the vendor's domain after any engagement.

10. 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

11. The vendor shall provide any audit report or data as required by KSITM with respect to audits performed for the KIED.

12. To ensure that web based applications is free from the vulnerabilities of any nature. The audit exercise will need to undertake the following activities:

i) Identify the security vulnerabilities, which may be discovered during website security audit including cross-site scripting, Broken links/Weak session management, Buffer Overflows, Forceful browsing, Form/ hidden field manipulation, Command injection, Insecure use of cryptography, Cookie posing, SQL injection, Server miss- configuration, Well known platform vulnerabilities, Errors triggering sensitive information, leak etc.

ii) Identification and prioritization of various risks to the KIED online web applications

iii) Identify remedial solutions and recommendations for making the web applications secure.

iv) Undertake user profiling and suggest specific access methodologies and privileges for each category of the users identified.

v) The auditors will have to carry out an assessment of the vulnerabilities, threats and risks that exist in web application through Internet Vulnerability Assessment and Penetration Testing. This will include identifying remedial solutions and recommendations for implementations of the same to mitigate all identified risks, with the objective of enhancing the security of the system.

vi) Applications should be audited as per the CERT-in Standards. The auditor is expected to submit the final audit report after the remedies/recommendations are implemented and confirmed with retest.

vii) The Audit Firm/company has to submit a summary compliance report at the end of the assessment phase and the final Report will certify that EDC-KIED web applications are incompliance with the standards.

Deliverables and Audit Reports

I/513857/2024

The successful bidder will be required to submit the following documents in printed format (2 copies each) after the audit of above mentioned web application:

i. A detailed report with security status and discovered vulnerabilities weakness and mis-configurations with associated risk levels and recommended actions for risk mitigations especially with respect to payment gateway.
ii. Summary and detailed reports on security risk, vulnerabilities and audit with the necessary counter measures and recommended corrective actions to be undertaken by KIED.
iii. The vendor will be required to submit the deliverables as per terms and conditions of this document.

ANNEXURE-III

	Name of Organisation	**Kerala Institute for Entrepreneurship Development**
	Address	**HMT Colony, Rockwell Road, Kalamassery, Kochi**
	Billing Address	**CEO & Executive Director - KIED**
	Contact Person	9633050143
	Contact Number	9633050143
	E-mail	ceo.kied@gmail.com
	GSTN	**32AAATK4049H1ZV**
Web Application Scoping Sheet for Security Assessment		
Sl.No.	**Web Application Assessment Details**	**Description**
1	Web Application Name & Description	**EDC website and cms** : Experience seamless engagement with our integrated platform. Users effortlessly log in, register for exclusive events and programs, and stay informed with curated news and articles from KIED. Admins wield control through a dedicated portal, managing content updates, event registrations, and user approvals with precision and efficiency. Elevate your interaction experience with us.
2	Type of application Web/Application/ Mob/Rest / Thick / Thin instance to assesses & number of Application (s)	Web Application
3	How many login systems to assesses?	9 users, 5 admin

I/513857/2024

4	How many static pages to assesses? (Approximate)	20 + user side , 10 admin
5	How many dynamic pages to assesses? (Approximate)	35 + User Side, 40 + admin
6	Do you need want role-based testing performed against this application?	yes
7	Do you need want credentialed scans of web applications performed?	yes
8	Back-end Database (MS-SQL Server, PostgreSQL, Oracle, etc.)	Maria db
9	Authorization No. of roles & types of privileges for the different roles	9 users + 5 admin roles roles :
10	Whether the application contains any content management module (CMS) (If yes then which?) If its is Portal do mention please	yes, portal
11	Is it a hybrid application?	no
12	Whether the application was security audited earlier? If so, please mention details.	no
13	Front-end Tool [Server side Scripts] (i.e. c++, J2eee, ASP, Asp.NET, JSP, PHP, etc.) – PHP	php
14	Operating System Details (i.e.Windows-2003, Linux, AIX, Solaris, etc.)	linux
15	Application Server with Version (i.e. IIS 5.0.Apache, Tomcat, etc.)	Apache – 2.4.58
16	Total No. (Approximate) of Input Forms	More than 10
17	Total No. of input field	More than 100
18	Total No. of login modules	9 +5
19	Number of Web Services, if any	More than 100
20	Number of methods in all web services ?	4
21	Number of URL's require to assesses ?	1 for user side, 1 for admin panel
22	Is this REST /SOAP based Application	REST
23	Is it Thick or Thin Client Application	Thin
24	Is this Applications is ERP/ Enterprised based App	No
25	Does the application has or proposed to have payment gateway integration? Please specify	yes, HDFC (cc avenue)
26	Is Application hosted in Cloud ? If yes which under cloud provider private & others (Govt SDC)	Govt SDC

I/513857/2024

1	What services do you expose to the internet? (Examples: Web, database, FTP, SSH, etc.)	Web
2	What type of authentication do you use for your web services? (Examples: PubCookie, Windows Integrated, htaccess, etc.)	ht access
3	What languages do you use for your web services? (Examples: PHP, Perl, Ruby, ASP, etc.)	php
4	What antivirus application (s) do you use?	nil
5	Is your antivirus application implemented using a “managed” client/server architecture, or in a stand-alone configuration?	no
6	What Enterprise Resource Planning (ERP/MIS) application (s) does your organization use? (Examples – SAP, Peoplesoft, Oracle, JD Edwards), Any Other Vender Applications.	NA
7	Please include a brief description of each.	
8	What E-commerce application (s) does your organization use? Please include a brief description of each.	
9	What database technologies does your organization use? (Examples – Oracle, Microsoft SQL, IBM DB2, MySQL) . Please include a brief description of the purpose for each.	MY SQL
10	What services do you expose to the end users in internet?	

1	Application Name and Description detailed	Edc website and cms : Experience seamless engagement with our integrated platform. Users effortlessly log in, register for exclusive events and programs, and stay informed with curated news and articles from KIED. Admins wield control through a dedicated portal, managing content updates, event registrations, and user approvals with precision and efficiency. Elevate your interaction experience with us.
2	Primary programming language used to develop the application	PHP, React js
	Additional components, used in the application,	

I/513857/2024

3	which are developed in the programming languages other than the primary language.	
4	Is the architecture document of the application available? (Yes/No)	No
5	Does the application process any data which falls under the PCI-DSS, HIPPA, etc. international standards/regulations? If yes, then Please specify.	No
6	Is security incorporated in the SDLC of the application? (Yes/No)	Yes
7	Backend database used in the application.	Maria db
8	Type of the application.	
	●CMS based application	**yes**
	●Custom developed application	Yes
9	Any third party library used in the application? (Yes/No)	Yes
10	How is access control enforced in the application e.g. database role mapping, per page access checks?	database role mapping, per page access checks
11	How data access layer is implemented?	
	●Dynamic SQL strings	yes
	●Stored Procedures	
	●Prepared Statements	
12	What authentication mode is implemented?	
	●SSO	
	●Form based login	yes
	●LDAP authentication	
	●Other	
13	No of user roles in the application	9 users + 5 admin roles roles :
14	No of application users	200
15	Any protocols other than HTTP or HTTPS used in the application.	no
16	Is the application accessible over the internet? (Yes/No)	yes
17	Total number of web servers and their details.	Apache , Nginx
18	Total number of application servers and their hardware details.	

I/513857/2024

19	Total number of database servers and their hardware details	Maria db
20	No of total code files in the application	More than 200
21	At what instance of the application this security assessment will be conducted?	
	●Production	
	●UAT	Yes
22	Is web application firewall used to protect the application? (Yes/No)	No
23	Is load balancer/ Application firewall used to analyze and balance the traffic? (Yes/No)	no
24	Details About Current Application layout and Architecture	
	●Diagram	
	●Work Flow	Yes
	●Any issues you faced in past, current on security aspect in your applications.	

For each Application whether its web or mobile please fill in different sheet

If mobile applications requirement is there then kindly fill it up

S. No.	Mobile Applications - Android Parameters	Details
1	Number of Screens in Mob app	
2	Total No. of Input Forms	
3	Total No. Parameters in API	
4	Total No of Input fields	
4	Total No of User Roles such as admin, manager, user	
5	Type of App such as Native apps or Mobile web Apps, or Hybrid Apps	
6	Technologies such as HTML, CSS, asp.net, Java, PHP or any details	
7	Backend web Services & Database	

I/513857/2024

S. No.	Mobile Applications - iOS Parameters	Details
1	Number of Screens in Mob app	
2	Total No. of Input Forms	
3	Total No. Parameters in API	
4	Total No of Input fields	
4	Total No of User Roles such as admin, manager, user	
5	Type of App such as Native apps or Mobile web Apps, or Hybrid Apps	
6	Technologies such as HTML, CSS, asp.net, Java, PHP or any details	
7	Backend web Services & Database	

-
-

ANNEXURE-IV

QUOTATION FOR CONDUCTING THE SECUIRTY AUDIT OF WEB APPLICATION OF EDC-KIED

QUOTATION / BID (On Company Letter Head)

1. Name of the Bidder :

2. Address for Correspondence :

3. Contact number :

4. e-mail :

I/we hereby submit the quote for conducting Security Audit of web application of EDC-KIED as per the Scope of work given and within the time specified and in accordance with the terms and conditions of Quotation Notice.- **KIED/SQN/2024/004** Dated:23-05-2024.

Description	Price Quoted (in Rs)	Tax (if any)	Total Cost (Rs.)
(i)	(ii)	(iii)	(iv)
Security Auditing of website www.edckerala.org			

Thus the total amount quoted including GST and applicable all other charges is

I/513857/2024

Rs……./-

(Rupees……
…… ……...)

The rate quoted rate must be valid for the period of contract from the date of opening of financial bid.

Place- Signature-

Date- Name of the authorized Signatory.

(Seal of the Company /Firm)