REQUEST FOR INFORMATION N°90007426
WEB VULNERABILITY SCANNING SYSTEM

I. Introduction

The Bank has a few public websites including its institutional website, statistical database, digital repositories, and others. Given the importance of the information, it is crucial to assure the integrity and security of these websites.

About that, the Bank requires conducting market research to identify and evaluate potential platforms to support web vulnerability scanning on the Bank's public sites, that allows to carry out in those sites an exhaustive and automated analysis.

II. Objective

The Bank is looking for technological solutions that facilitate the detection, analysis, and reporting of web vulnerabilities. The desired platform must be capable of executing regular and consistent scans without manual intervention, providing detailed and understandable reports that can be used to improve security measures.

To assure the effectiveness and security of the web vulnerability scanning platform that is sought to be implemented, the following functionalities are considered important:

1. The platform must be accessible and usable exclusively through a web browser from the Bank's internal network.

2. Allow for automatic execution of vulnerability scans at regular intervals or as configured by the user, assuring continuous evaluations.

3. It must allow selecting the type or intensity level of the scan to be performed.

4. It is essential that the platform includes mechanisms to prevent blocks or assure continue service in case of blocks caused by cybersecurity controls implemented by the Bank.

5. The tool must provide real-time security notifications and alerts.

6. It must have analytics and reporting capabilities, allowing to generate detailed and customized reports about vulnerabilities obtained from the last scan as well as the previous ones.

7. The platform must be able to detect a wide variety of vulnerabilities, including updates on known vulnerabilities and a high-precision analyzer that minimizes false positives and false negatives.

III. Request for information Process

The current request for information will be adjusted to the following Activity Calendar:

ACTIVITIES	DATE
Publication of the request for information	Thursday, September 05, 2024
Communication by Providers of its Interest to Participate in this Process	Friday, September 13, 2024
Reception of Questions and Clarifications by Providers	Tuesday, September 24, 2024
Response to Questions by the Bank	Friday, September 27, 2024
Submission of Questionnaire Response by Providers	Friday, October 11, 2024
Individual Meetings with Providers	Tuesday, October 15, and Wednesday, October 16, 2024
Closing of request for information Consultation	Wednesday, October 23, 2024

The providers interested in participate in this Request for Information Process must communicate their interest to the RFI Process Responsible, Ms. Cecilia Krebs, to the email address ckrebs@bcentral.cl with a copy to the Technical counterpart, Mr. Fabián Estefanía, to the email address festefania@bcentral.cl, indicating in the subject line **INTERÉS EN PARTICIPAR: 90007426 Web Vulnerability Scanning System** until the deadline established in the Calendar of Activities.

In case the Provider have queries or observations regarding this process and its Questionnaire, they must formulate them on the established date in the Activities Calendar attached, to the email address ckrebs@bcentral.cl with a copy to festefania@bcentral.cl, indicating in the subject line **PREGUNTAS: 90007426 Web Vulnerability Scanning System**. These will be responded to all providers who have manifested their interest in participating, without indicate the author of the questions or observations formulated.

Afterwards, the Provider must send their responses to the detailed questionnaire in section V of this document on the date established in the Activities Calendar, to the following email addresses: ckrebs@bcentral.cl with a copy to festefania@bcentral.cl, indicating in the subject line **RESPUESTA: 90007426 Web Vulnerability Scanning System**.

Once the responses to the Questionnaire are received, the Bank may request additional information or clarification from all or some of the providers, on an individual basis.

After evaluating the responses to the questionnaire, the Bank may require individually to the participant providers, to hold a meeting to complement or clarify specific aspects of their products and/or services informed in their responses. This meeting will be scheduled at the dates indicated in the Activities Calendar and coordinated in a timely manner.

IV. Additional Considerations

- It is hereby stated that this request for information process does not constitute a tender or quotation, and therefore providers should refrain from sending formal economic proposals, since no award is considered.

- This request is solely for informational purposes and does not obligate in any case to the Central Bank of Chile to acquire or contract the Products and/or Services consulted.

- In case that the Central Bank of Chile requires the acquisition or contracting of these Products and/or Services, a Tender or Quotation process will be initiated through its Purchasing Department, establishing the technical, administrative, legal, and economic conditions under which the provision of Products and/or Services would be contracted by the Bank.

V. Questionnaire

1. In the following section (VI.) we request general information about your company regarding the applications offered and its background, including contact details.

2. Platform Functionalities:
   a) What are the main functional features of your platform?
   b) Does it allow adjusting the level of network traffic or requests that will be generated by the vulnerability scanning execution on selected assets?
   c) Does it permit automatic execution of vulnerability scanning at regular intervals?
   d) Does the solution allow rotating a stock of sites at determined periods?
   e) Is there any technical requirement that the Bank needs to comply with before scanning a website?
   f) Are there mechanisms to avoid blocks or provide continuity of service in the face of cybersecurity controls implemented by the Bank that may block traffic? Please comment on this.
   g) How are the scan results displayed? Does it include details about the presentation of detected vulnerabilities, their severity, and specific recommendations for its mitigation?
   h) Does the solution implement security notifications and alerts?
   i) Does the solution have updates to its vulnerability database? At what regularity?
   j) Does the solution have profiling and access controls by role?

k) Does the solution have mechanisms for integration with other tools? For example: Single Sign-On.
l) What kind of technical support does the company offer?
m) From where (geographical location) are the analysis performed?
n) Does the solution have the capability to interrupt the analysis immediately?
o) Does the solution have assistance in evaluating reports and analysis assisted by AI?
p) Does the the solution´s coverage allow, among others, to cover the main OWASP security risks?
q) Does the solution provide a summary of vulnerabilities with their levels of severity (CVSS score), along with recommendations for mitigation?
r) Does the solution allow to integrate two-factor´s authentication?

VI. Experience and Background of the Company

1) Company Experience

Years in the market	
Years of experience in similar services/products – Web vulnerability scanning	
Total number of employees	
Total number of consultants	(number - specialty)
Total number of certified consultants	(number - specialty)
Company certifications, if any	
Indicate representations or "partnerships", if any	
Indicate alliances for providing the consulted services (if not able to provide the totality of modules or services autonomously)	

2) Clients of the Company in Chile with the Application Modules

Active clients – Web vulnerability scanner	(Indicate number and list the top three, specifying SaaS or On-Premise mode)

3) Company Background

Business Name:	
ID:	
Address:	

Commercial Contact

Name:	
Email address:	
Mobile phone:	

Santiago, September 5th, 2024

Purchasing Department
Accounting Management and Planning Division