TÉRMINOS DE REFERENCIA

"SERVICIO DE ETHICAL HACKING"

1. ANTECEDENTES

El 23 de julio del 2021 la República del Perú suscribió con el Banco Interamericano de Desarrollo – BID el Contrato de Préstamo N.º 5287/OC-PE para la ejecución del Programa de Innovación, Modernización Tecnológica y Emprendimiento. La Unidad Ejecutora es el Programa Nacional de Desarrollo Tecnológico e Innovación - PROINNOVATE.

El objetivo del Programa es incrementar la productividad de las empresas. Los objetivos específicos son: (i) aumentar la inversión privada en innovación empresarial; y (ii) fortalecer la capacidad del Gobierno de Perú para diseñar, orientar e implementar políticas de innovación empresarial a largo plazo.
La presente adquisición será financiada en el marco del Componente 4: Fortalecimiento de Capacidades Institucionales, subcomponente 4.1.4: Modernización de la Plataforma Tecnológica de ProInnóvate.

2. OBJETO DE LA CONTRATACIÓN.

Contratar un servicio de Ethical Hacking para la evaluación de vulnerabilidades a la que está expuesta la infraestructura tecnológica de ProInnóvate, mediante la metodología OWASP.

3. FINALIDAD DE LA CONTRATACIÓN.

Analizar la infraestructura tecnológica de TI, que da soporte a los sistemas de información y poder determinar el nivel de exposición y las vulnerabilidades potenciales que podrían ser explotadas por un intruso para acceder de manera NO autorizada y realizar modificaciones de información en los sistemas de la organización comprometiendo de esta forma la confidencialidad, integridad y disponibilidad de la información.

4. DESCRIPCIÓN DEL SERVICIO

ÍTEM	CANTIDAD	UNIDAD MEDIDA	DESCRIPCIÓN
1	01	Servicio	Servicio de Ethical Hacking

- El proveedor deberá de presentar un cronograma y planificación de actividades del proyecto. Se deberá crear un Acta de Inicio del Proyecto.

- El proveedor deberá de entregar un informe detallado que contemple una matriz con el resumen de las vulnerabilidades detectadas. El proveedor deberá incluir las recomendaciones para minimizar la ocurrencia de futuros ataques.

- El servicio no debe de afectar el funcionamiento de los sistemas o el desempeño de la red. Esta actividad será coordinada entre la UIT y el proveedor para buscar la mejor hora de ejecución en aras de minimizar riesgos.

- El postor deberá indicar en su informe el detalle de las herramientas y/o productos que utilizará durante la ejecución del servicio.

- El proveedor deberá contemplar el escaneo de puertos y servicios.
- El proveedor deberá identificar las vulnerabilidades en la infraestructura tecnológica de la organización. Este análisis comprende servidores y firewalls.
- Se deben identificar vulnerabilidades asociadas con malas prácticas de desarrollo de los sistemas de información basado en la metodología OWASP.
- Se debe realizar un análisis de direcciones IPs públicas para identificar vulnerabilidades.
- Verificación de fallas conocidas a nivel de protocolos (TLS, HTTPS, POP, SMTP, IMAP, MAPI, SMB, NFS, FTP) y TCP/IP en general.
- Detectar las vulnerabilidades en el servicio de base de datos y ataques de SQL Injection, XSS, XSRF, etc.
- Escaneo de las vulnerabilidades de los servidores en general (correo, base de datos, aplicaciones, archivos, etc).
- Descubrir los activos de información publicados en internet.
- Evaluar las vulnerabilidades de estos activos definiendo su criticidad e impacto usando el score base CVSS.
- Ejecutar las pruebas que sean necesarias realizar para descartar los falsos positivos (detección de amenazas que no son reales) en las vulnerabilidades detectadas.
- Hacer uso de las herramientas de Ethical Hacking para demostrar la veracidad de los resultados.
- El servicio se realizará bajo la modalidad de "caja negra"
- Presentar un informe detallado de las vulnerabilidades detectadas durante la ejecución del servicio adjuntando las conclusiones y recomendaciones para corregir las vulnerabilidades, mitigar los riesgos y mejorar la postura de seguridad de la organización.
- Realizar el retest (refrendo) de las vulnerabilidades una vez que la organización haya realizado la corrección respectiva. Este refrendo no debe exceder los 6 meses calendarios.
- Bajo ninguna circunstancia y en ningún momento se generará algún tipo de cambio sobre los sistemas y/o información a las que se logre acceso.

Para el presente servicio, la entidad no brindará ninguna información sobre los sistemas y servicios informáticos al proveedor. Esta información está compuesta por direcciones IP, usuarios, credenciales, URLs, nombres de dominio, diagramas de red, etc. El objetivo es que el escenario sea el más real posible frente la probabilidad de ocurrencia de un ataque que provenga desde internet. El proveedor deberá brindar una charla de concientización de por lo menos 2 horas dirigida al personal de UIT sobre los siguientes temas:

- Fuga de Información.
- Ciberseguridad.

5. REQUISITOS MÍNIMOS DE CALIFICACIÓN DEL POSTOR Y/O PERSONAL

Experiencia del postor

El postor debe ser una persona jurídica y debe de acreditar como mínimo dos (02) servicios relacionados con la ejecución de este tipo de proyectos de ciberseguridad (análisis de vulnerabilidades y Ethical Hacking) en empresas públicas y/o privadas, la cual será validado mediante cartas y/o constancias.

No encontrarse inhabilitado para contratar con el estado.

Experiencia del personal técnico

- Profesional bachiller y/o titulado en Ingeniería de Sistemas o carreras similares.
- Experiencia profesional mínima de 5 años como especialista en seguridad de la información y/o ciberseguridad.
- Experiencia profesional mínima de 5 años desempeñándose en proyectos de evaluación de Ethical Hacking, análisis de vulnerabilidades y pruebas de penetración.
- Deberá acreditar los certificados correspondientes de haber participado en 5 proyectos de Ethical Hacking.
- Deberá contar como mínimo con 2 certificaciones vigentes de las siguientes entidades Mile2, EC Council, Open Sec, Certiprof, ISC2, que podrían ser las siguientes o similares:

  ✓ CPEH (Certified Professional Ethical Hacker) de Mile2.
  ✓ CEH (Certified Ethical Hacking) de EC Council.
  ✓ OSEH (Open Sec Ethical Hacker) de Open Sec.
  ✓ LCSPC (Lead Cyber Security Professional Certificate) de CertiProf.
  ✓ CISSP (Certified Information Systems Security Professional) de ISC2.
  ✓ CC (Certified in Cyber Security) de ISC2.

6. PRODUCTOS A OBTENER

- ✓ El proveedor deberá de presentar un cronograma y planificación de actividades del proyecto. Se deberá crear un Acta de Inicio del Proyecto.
- ✓ El proveedor deberá de entregar un informe detallado que contemple una matriz con el resumen de las vulnerabilidades detectadas. El proveedor deberá incluir las recomendaciones para minimizar la ocurrencia de futuros ataques.
- ✓ Presentar un informe detallado de las vulnerabilidades detectadas durante la ejecución del servicio adjuntando las conclusiones y recomendaciones para corregir las vulnerabilidades, mitigar los riesgos y mejorar la postura de seguridad de la organización.

7. LUGAR Y PLAZO DE ENTREGA

En la sede central de ProInnóvate, Jr. Juan Bielovucich N° 1325 – Lince, Lima. Para el presente servicio, la ejecución por parte del proveedor será en modalidad remota.
Sin embargo, queda a discreción de la Unidad de Tecnologías de la Información si el proveedor deberá sustentar con alguna prueba los hallazgos detectados de forma presencial en la sede central de ProInnóvate.

El plazo del servicio no deberá de exceder los sesenta (60) días calendario, después de notificada la orden de servicio, la Unidad de Tecnologías de la Información coordinará de forma directa con el proveedor la ejecución del servicio

8. FORMA DE PAGO

El pago se efectuará luego de emitida la conformidad por el área usuaria, el proveedor deberá considerar toda la documentación indicada en el presente documento.

9. PENALIDADES

En caso de retraso injustificado en la ejecución de las prestaciones objeto del presente contrato, se aplicará al consultor una penalidad por cada día calendario de atraso, deducible previa comunicación, del pago pendiente.

$$\text{Penalidad diaria} = \frac{0.10 \times \text{monto}}{F \times \text{plazo en días}}$$

Donde F tiene los siguientes valores:
• Para plazos menores o iguales a sesenta (60) días: F = 0.40.
• Para plazos mayores a sesenta (60) días: F=0.25

Tanto el monto como el plazo se refieren según corresponda, al contrato, o en caso éste involucre obligaciones de ejecución periódica, a la prestación parcial que fuera materia de retraso.

La penalidad será aplicada hasta por un monto máximo equivalente al diez por ciento (10%) del monto contractual. Cuando se alcance el monto máximo de penalidad, la entidad contratante podrá resolver el contrato por incumplimiento.

10. REPONSABLE DE DAR LA CONFORMIDAD

La conformidad será emitida por la Unidad de Tecnologías de la Información.

11. CONFIDENCIALIDAD DE LA INFORMACIÓN

El Contratista queda expresamente obligado a mantener absoluta confidencialidad y reserva sobre la información obtenida, obtenida al tener acceso durante la ejecución del servicio, así como los informes y documentos que produzca, relacionados con la ejecución del presente servicio, deberá ser considerada confidencial, no pudiendo copiar, utilizar o ser divulgada sin autorización expresa y por escrito de ProInnóvate.
Esta obligación de reserva o confidencialidad seguirá vigente aún después del vencimiento del plazo de la contratación. Los títulos de propiedad, derechos de autor y todo otro tipo de derechos de cualquier naturaleza sobre cualquier material producido bajo las estipulaciones de este Contrato son cedidos a ProInnóvate en forma exclusiva y sin costo adicional alguno.

12. RESPONSABILIDAD POR VICIOS OCULTOS:

a) La recepción conforme de ProInnóvate no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos.

b) El Contratista es responsable por la calidad ofrecida y por los vicios ocultos de los servicios ofertados por un plazo no menor de tres años contado a partir de la conformidad otorgada por la Oficina de Tecnologías de la Información y Comunicaciones).

La conformidad del servicio por parte del PROINNOVATE no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos. El plazo máximo de responsabilidad de la firma consultora es de un (01) año contado a partir de la conformidad otorgada por el PROINNOVATE.

13. SEGURIDAD Y SALUD EN EL TRABAJO

Indicaciones para realizar el trabajo en la Entidad:
Datos del personal que asistirá:
• Nombre y RUC de la empresa.
• Nombres completos.
• Número de DNI.
• El rango de horario que asistirán.

14. ANTISOBORNO

Los participantes se obligan a conducirse en todo momento, durante la postulación al concurso, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participantes, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas.

Además, los participantes se comprometen a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

15. VALOR REFERENCIAL

S/ 105,000.00 (CIENTO CINCO MIL SOLES CON 00/100)

Firma Digital
Firmado digitalmente por DIEHL ARELLANO Ludwig FAU 20565526694 hard
Motivo: Soy el autor del documento
Fecha: 06.09.2023 20:05:53 -05:00