COMPAGNIE TUNISIENNE DE FORAGE
19 RUE DE L'ARTISANAT – 2080 ARIANA - CHARGUIA II–TUNISIE
FAX N° (216-70) 836 568 – 837 041 PHONE N° (216-70)837 322

OBJET : CONSULTATION N° **PP26/616**

Mission d'audit de la sécurité du SITE WEB GESTION DES CONCOURS DE RECRUTEMENT

La Compagnie Tunisienne de Forage **(C.T.F.)** *souhaite mandater un bureau d'études pour réaliser une mission d'audit de sécurité du module de gestion des concours avant mise en exploitation conformément aux exigences précisées* ***ci-joint*** *dans le* ***cahier des charges en Annexe I.***

A cet effet, nous vous invitons à nous soumettre votre meilleure offre de prix en **TTC** *conformément à la procédure ci-dessous.*

PROCEDURE DE SOUMISSION *:*

Les offres doivent parvenir à la CTF :

Par plis fermés :

A l'adresse suivante 19 rue de l'Artisanat charguia 2 –2035 L'Aéroport Tunis-Tunisie, par voie postale sous plis scellés et recommandés ou par rapid poste, ou déposé au bureau d'ordre de CTF contre décharge.

L'enveloppe doit *:*

** être adressée au nom de :*
Monsieur le Président Directeur Général
** Porter uniquement :*
- *L'adresse de la CTF,*
- *Les références de la consultation* **(PP 26/616)**

- *La mention '' **NE PAS OUVRIR**''*

** contenir à l'exclusion de tout autre document :*
-Les documents demandés au niveau de cahier de charge

Le texte de la consultation & les annexes, dûment signés et portant obligatoirement le cachet du soumissionnaire.
- *Le bordereau de prix en* **ANNEXE 4** *dûment rempli, signé et portant obligatoirement le cachet du soumissionnaire.*

- *Les documents justificatifs demandés aux* **Annexes 2 et 3.**

-Les offres doivent parvenir dans les meilleurs délais mais pas plus tard que le **24/11/2026 à 17H**
Toute offre parvenue après les délais sera rejetée (le cachet du Bureau D'ordre de la CTF faisant foi).

Méthodologie d'évaluation

Les offres financières, après la correction des éventuelles fautes de calcul, seront classées du moins disant au plus disant sur la base du montant forfaitaire et sera retenue l'offre moins disant qui sera conforme techniquement aux prescriptions de la présente consultation.

Conditions particulières

- Les offres reçues dans les délais doivent rester valables au moins 90 jours et ce à compter du lendemain de la date limite de réception des offres.

- Le mode de paiement est de 45 jours, par virement bancaire, date réception de votre facture.

SALUTATIONS
C.T.F.
P/DIRECTION APPROVISIONNEMENT & MARKETING

C.T.F
TUNIS
COMPAGNIE TUNISIENNE DE FORAGE

ANNEXE I

Clauses Techniques

Audit de la sécurité du site web gestion des concours de recrutement

Compagnie Tunisienne de Forage (CTF)

Référence : PP26-616
Date : 17/11/2026

1. Contexte et objet de la consultation

Dans le cadre de la mise en exploitation du module web de gestion des concours de recrutement, et conformément à la réglementation nationale en matière de cybersécurité, la présente consultation a pour objet de sélectionner un cabinet d'audit accrédité par l'Agence Nationale de la Cybersécurité (ANCS) pour la réalisation d'un audit de sécurité applicative complet de cette plateforme avant sa mise à disposition du public.

2. Références réglementaires

- Décret-loi n° 2023-17 du 11 mars 2023, relatif à la cybersécurité, fixant les missions de l'ANCS et imposant l'évaluation complète de la sécurité des plateformes et sites web par un organisme accrédité, préalablement à leur mise à disposition du public ;
- Circulaire du Chef du Gouvernement n° 05 de l'année 2026 (2 septembre 2026), relative au renforcement de la sécurité des systèmes numériques nationaux, imposant notamment l'hébergement auprès d'entités agréées, le protocole HTTPS/SSL-TLS, l'authentification multifacteurs (MFA) pour les comptes administrateurs, un audit de sécurité périodique et une protection contre les attaques DDoS.

3. Périmètre de l'audit

L'audit couvre l'application web (interfaces candidat et administration) et ses API, les formulaires d'inscription et les dossiers de candidature, les mécanismes d'authentification et de gestion des privilèges, les journaux (logs), la base de données et les données à caractère personnel, ainsi que l'environnement d'hébergement et son exposition sur Internet (y compris la protection contre les attaques DDoS). Le détail du périmètre (accès, comptes de test) sera communiqué au prestataire retenu après signature d'une convention de confidentialité.

4. Objectifs de l'audit

- Identifier les vulnérabilités techniques et organisationnelles de la plateforme ;
- Évaluer l'authentification (notamment le MFA), les contrôles d'accès et les risques d'élévation de privilèges ou d'accès non autorisés ;
- Évaluer la protection des dossiers de candidature et des données personnelles, ainsi que les risques de contournement des règles métier du concours ;
- Évaluer la résistance aux attaques courantes (OWASP Top 10) et la robustesse du code source ;
- Évaluer les mécanismes de journalisation et de traçabilité (cf. art. 7) ;
- Formuler des recommandations correctives priorisées, préalables à la mise en exploitation.

5. Méthodologie et déroulement de la mission

Le prestataire devra mettre en œuvre une méthodologie reconnue, combinant les approches suivantes :

- Tests d'intrusion en boîte noire (sans information préalable, simulant un attaquant externe), en boîte grise (avec un accès authentifié, simulant un utilisateur malveillant) et, si le périmètre le permet, en boîte blanche (avec accès au code et à l'architecture) ;
- Analyse statique du code source (SAST) : détection des injections, dépendances vulnérables, secrets exposés, conformité OWASP ASVS ;
- Analyse dynamique (DAST) : tests d'intrusion applicatifs et sur les API, couverture de l'OWASP Top 10 (injection, XSS, authentification brisée, IDOR, exposition de données sensibles, etc.) ;
- Revue de la configuration serveur, réseau et des composants tiers, et vérification du chiffrement des échanges et du stockage.

La mission se déroule selon les phases indicatives suivantes :

Phase	Contenu	Durée
1	Cadrage : périmètre, enjeux, modalités de communication et de planification	A préciser
2	Audit technique : tests d'intrusion, analyse du code (SAST/DAST), recherche et exploitation de vulnérabilités	A préciser
3	Analyse des risques : classification des failles, catalogue de recommandations priorisées	A préciser
4	Synthèse et restitution : rapport final, présentation aux responsables	A préciser
5	Contre-audit (post-correction) : vérification des correctifs et validation finale	A préciser

Toutes les phases de la mission ne doivent pas dépasser 10 jours.

6. Authentification multifacteurs (MFA)

Conformément à la Circulaire n° 05/2026, le prestataire devra vérifier la présence et la robustesse du MFA, en particulier pour les comptes administrateurs et les comptes à privilèges élevés, et signaler toute absence ou défaillance comme non-conformité prioritaire.

7. Journalisation et traçabilité

Le prestataire devra évaluer les mécanismes de journalisation, de traçabilité et de conservation des événements de sécurité et des opérations sensibles, notamment par les comptes administrateurs, couvrant au minimum : les connexions et échecs d'authentification, la création/modification/suppression de comptes, les actions administratives, la modification des dossiers candidats, le téléchargement de documents, les changements de statut, les événements de sécurité, ainsi que la durée de conservation des journaux et leur protection contre toute modification non autorisée.

8. Classification des risques et obligation de correction

Chaque vulnérabilité identifiée sera classée selon le niveau de risque suivant :

Niveau	Description	Effet sur la mise en production
Acceptable	Aucun risque pour la confidentialité, l'intégrité ou la disponibilité	Aucune action requise
Faible	Pas de compromission directe, mais informations utiles à un attaquant	Correction recommandée
Moyen	Compromission partielle des données ou de l'infrastructure possible	Correction requise avant mise en production
Fort / Critique	Compromission significative des données, de l'infrastructure ou du processus de concours possible	Mise en production bloquée jusqu'à correction

- En cas de vulnérabilité critique nécessitant une action immédiate, une alerte sera transmise sans délai à la CTF, sans attendre le rapport final ;
- Le prestataire devra fournir, pour chaque vulnérabilité corrigée, des preuves de correction (captures, extraits de configuration, résultats de tests de validation) ;
- La mise en production définitive ne pourra être validée qu'après un rapport de contre-audit confirmant l'absence de vulnérabilité de niveau Moyen, Fort ou Critique non corrigée.

9. Exigences relatives au prestataire

- Accréditation ANCS en cours de validité (**condition éliminatoire**), attestation à joindre à l'offre ;
- Équipe d'auditeurs qualifiés (certifications type OSCP, CEH, CISSP, ISO 27001 Lead Auditor ou équivalent) ;
- Engagement contractuel de confidentialité sur les résultats de l'audit.

10. Équipe intervenante

Le prestataire devra affecter à la mission une équipe comprenant au minimum deux profils vérifiant les critères mentionnés à l'ANNEXE N°2.

11. Livrables attendus

Livrable	Contenu
Plan et démarche d'audit	Planning détaillé et méthodologie retenue
Rapport d'audit détaillé	Vulnérabilités, preuves, niveau de criticité (type CVSS), recommandations
Synthèse exécutive	Destinée à la Direction Générale
Preuves de correction	Pour chaque vulnérabilité de niveau Moyen, Fort ou Critique traitée
Rapport de contre-audit	Validation des correctifs et clôture de la mission

12. Composition de l'offre

Les soumissionnaires devront présenter une offre technique (présentation du cabinet, attestation ANCS, CV de l'équipe, références des trois dernières années de l'équipe intervenante (2024, 2025 & 2026), méthodologie et planning) et une offre financière (devis détaillé HT/TTC, modalités de paiement, validité de l'offre de 90 jours minimum), sous plis séparés.

13. Confidentialité

Les résultats de l'audit demeurent la propriété exclusive de la CTF et ne pourront être communiqués à des tiers sans autorisation écrite préalable.

.

Annexes

ANNEXE N°1 : Structure du capital de la société soumissionnaire

Raison sociale : .....

N° de Matricule Fiscal : .....

Inscrit au registre de commerce sous le numéro : .....

Adhérant à la CNSS sous le n° .....

Adresse :
.....
.....
Téléphone : .....**Fax :** .....

Statut de la société : Sarl : ..... S.A. : .....
Capital : ..... DT

Activités de la société :
.....
.....
.....

Personnel de la société :
- Nombre de(s) ingénieur(s) .....
- Nombre d'auditeurs en Informatique (Sécurité, Système d'information, tc.) .....
- Nombre des techniciens.....
- Total du personnel.....

Nom de la Personne bénéficiant de la procuration et signant les documents relatifs à l'offre
.....

Qualité de cette personne (fonction) .....

Tunis le, ...

Lu et approuvé
Signature et cachet du soumissionnaire



ANNEXE N°2 : Qualification de l'équipe intervenante

Chef de Projet		
Critères	**Minimum exigé**	**Réponse du soumissionnaire**
Diplôme universitaire	Diplôme d'ingénieur ou titulaire d'un master en sécurité des systèmes d'information	
Certification	- Certifié par **l'ANCS** (certification en cours de validité) - ISO 27001 Lead Auditor - ISO 27005 Risk Manager - ISO 27032 Cybersecurity manager	
Expérience professionnelle en matière sécurité informatique	10 ans	
Nombre de projets similaires (site web, application web, plateforme web.) en tant que chef de projet effectuées durant les trois dernières années (2024, 2025 et 2026).	5 projets	

Consultant/Auditeur		
Critères	**Minimum exigé**	**Réponse du soumissionnaire**
Diplôme universitaire	Master en sécurité des systèmes d'information	
Certification	- Certifié par **l'ANCS** (certification en cours de validité) - ISO 27005 Risk Manager	
Expérience professionnelle en matière sécurité informatique	3 ans	
Nombre de projets similaires (site web, application web, plateforme web.) effectuées durant les trois dernières années (2024, 2025 et 2026).	3 projets	

Les critères mentionnés dans les deux tableaux ci-dessus doivent être obligatoirement justifiés par les pièces (diplômes, certifications, Lien ANCS, attestations du client, PV de réception, Attestation de bonne exécution, Contrats).
Les certifications demandées doivent être valides au moment de dépôt des offres.

ANNEXE N°3 : Fiche des références de l'équipe du projet pour des missions de même nature (site web, application web ou plateforme web)

Organisme	Intervenant	Objet de la mission	Déroulement de la mission		Responsable du client à contacter	
			DU	AU	Nom	Téléphone

Les missions mentionnées dans le tableau ci-dessus doivent être obligatoirement justifiées par des pièces certifiées conformes (PV de réception ou attestation du client).

Fait à.....le .....

Signature et Cachet du soumissionnaire

ANNEXE N°4 : Bordereau des prix :

(A remplir et à insérer obligatoirement dans l'enveloppe de l'offre financière)

Soumissionnaire : .....

Code d'identifiant fiscal : .....

Désignation	Prix Forfaitaire HT En Chiffres	% TVA	Prix TTC En Chiffres
Mission d'Audit de sécurité du module de gestion des concours de recrutement			
TOTAL			

Total en toutes lettres (TTC) :
:.....
.....

Fait à ....., le.....
Cachet & Signature du Soumissionnaire