https://owasp.org/www-chapter-tunisia/

الوكالة الوطنيّة للسّلامة المعلوماتيّة

Agence Nationale de la Sécurité Informatique

https://www.ansi.tn/

OTIP- OWASP Tunisia Infographic Project

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Présentation du projet OTIP

- **OWASP (Open Web Application Project) Tunisia Chapter** et **ANSI (Agence Nationale de la sécurité Informatique) co-organisent OTIP(OWASP Tunisia Infographic Project)**, un projet de création de *contenu infographique* qui vise à promouvoir la ***sensibilisation autour de la sécurité applicative auprès des développeurs logiciel en Tunisie***.
- Il s'agit d'un **projet communautaire** (en équipe) qui permet de vulgariser les différentes vulnérabilités applicatives citées par OWASP, montrer la possibilité de leurs exploitations et proposer des recommandations favorisant la sécurité par la conception (Secure By Design) et aiguiller vers les références, guides et outils open-source proposés par OWASP (www.owasp.org)
- Les équipes s'engageant à participer à ce projet peuvent être constituées de profils différents (étudiants, ingénieurs, infographistes, professionnels, enseignants…) ayant des connaissances techniques de base sur les langages de programmation tels que : PHP, JAVA, JAVASCRIPT , PYTHON.., sur les concepts de base de la sécurité informatique et sur infographie animée/design graphique
- **Le projet sera mené sur plusieurs étapes (appels à candidature)** durant chacune d'elle le contenu d'une ou plusieurs équipes participantes **sera reconnu, sélectionné, validé et diffusé** sur les canaux de l'ANSI et OWASP Tunisia Chapter après révision potentielle (Sites WEB, Chaines Youtube, Facebook, Linkedin..).

Cahier de charge (Premier Appel P1)

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

- ***Demandé:*** **une vidéo animée (capsule) de maximum 3 minutes traitant une vulnérabilité parmi les TOP 3 OWASP Web Application Security Risks** (SQL injection, Broken Authentication, Sensitive Data Exposure) . Se référencer à www.owasp.org
- **Public Cible: Les programmeurs Tunisiens**
- ***But:*** Sensibiliser à la sécurité du code dès la conception (**Secure Coding By design**).
- ***Requis:*** **La vidéo devrait être « éducative », « ludique »** et **« professionnelle ».** La vidéo devrait **être sous titrée en français** et animée en utilisant **le dialect tunisien (ou arabe) et le français**. Les dessins utilisés devraient se rapprocher **des personnages tunisiens.** Les logos de OWASP Tunisia Chapter et ANSI devraient figurer en bas de la vidéo

- **Chaque vidéo doit comporter les phases suivantes:**

1. Définition simple de la vulnérabilité, exemple: SQL injection

2. Causes de cette vulnérabilité

3. Scénario normal puis scénario d'attaque: *Par exemple, montrer le process normal d'authentification d'un utilisateur (login/password) du moment de la saisie au niveau du formulaire jusqu'au serveur d'application puis la base de données. Ensuite, le scénario d'attaque par le personnage pirate en injectant du code au niveau des champs et montrer par animation comment l'authentification est bypassée et qu'une session est allouée sans mot de passe fourni (Les candidats sont libres d'utiliser ce scénario ou un autre exemple de leur choix)*

4. Impacts de l'exploitation de la vulnérabilité

5. Montrer code vulnérable par l'exemple *(choisir deux langages différents : JAVA,PHP, PYTHON..)*

6. Comment prévenir l'attaque par l'exemple (secure code). *Par exemple, montrer un code en utilisant Prepared Statement*

7. Recommandations en donnant les liens et des références adaptées exclusivement OWASP (projets, guidelines, outils…). *Par exemple, lien vers OWASP TOP 10, OWASP Secure Code review, OWASP Secure testing guide , OWASP ZAP (scanner de vulnérabilités DAST), OWASP Sonarqube (Scanner de vulénrabilités SAST), OWASP WEBGOAT (plateforme d'apprentissage pour le pentest des applications WEB JAVA)….*

8. Placer à la fin le logo de OWASP Tunisia Chapter et ANSI avec les liens vers les sites WEB (https://owasp.org/www-chapter-tunisia/ et https://www.ansi.tn/)

Il s'agit d'un projet communautaire, les vidéos ne doivent référencier aucune société ou produits commerciaux

Appel à Candidature

- L’équipe candidate doit être formée d’au moins deux membres.
- Les connaissances requises sont principalement: les langages développement (PHP, JAVA,PYTHON ou autres), les concepts de base de la sécurité informatique et infographie animée/design graphique
- Un jury traitera les projets soumis, les critères de sélection sont principalement: Un contenu pertinent, clair, professionnel et cohérent, l’innovation de la présentation, l’originalité et qualité du texte de l’animation et de l’image,
- l’équipe gagnante bénéficiera de
  - Attestation de reconnaissance de la part de OWASP Tunisia Chapter et ANSI
  - Publication du contenu multimédia gagnant sur les pages officielles des organisateurs (site, réseaux sociaux, Youtube…) après révision et validation finale.
- L’équipe non sélectionnée est vivement appelée à participer dans les appels à candidature ultérieurs.
- Il s’agit d’un projet communautaire national à valeur ajoutée, n’hésitez pas à participer!
- Formulaire d’inscription: https://forms.gle/gidgdLZk8p9wQHTw8

OTIP- OWASP Tunisia Infographic Project

Contacts

Sites web:

https://owasp.org/www-chapter-tunisia/

https://www.ansi.tn/

Youtube:

https://www.youtube.com/channel/UC1M1Ppxbbi3HoYBpqYKjlgA

https://www.youtube.com/channel/UCvDg94OdVjjEVPEcdaKdlLw

Facebook:

https://www.facebook.com/OWASP.Tunisia.Chapter.Official

https://www.facebook.com/ansitn

Nihel Ben Youssef- OWASP Tunisia Chapter Leader
Nihel.benyoussef@owasp.org

Wafa Dahmani- Chef Unité prospection et Veille chez ANSI
wafa.dahmani@ansi.tn

Mohamed Ali Bensouilah-Analyste Principal chez ANSI
bensouilah.mohamedali@ansi.tn

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique