Version : 20/08/2021

API Security CTF

Organisateurs : F5 Labs, bjCSIRT et AfricaCERT

bjCSIRT ÉQUIPE NATIONALE DE RÉPONSE AUX INCIDENTS DE SÉCURITÉ INFORMATIQUE

PRÉSIDENCE DE LA RÉPUBLIQUE DU BÉNIN

AfricaCERT

United Teams promoting Cybersecurity in Africa

I. CONTEXTE ET JUSTIFICATION

La numérisation des services et la sécurisation des actifs numériques constituent aujourd'hui un pilier de développement essentiels du continent africain. Afin d'atteindre cet objectif une montée en compétence des apprenants en informatique est vitale afin de mieux préparer la jeunesse aux défis sécuritaires de l'informatique. Pour une jeunesse africaine compétitive dans le secteur de la sécurité des systèmes d'information, les étudiants doivent maîtriser les systèmes d'exploitation, les services d'application, l'ingénierie logicielle, l'administration système, la programmation de scripts et la mise en réseau. L'apprentissage à travers les CTFs (Capture the Flag) a prouvé être efficace et permet d'exposer les apprenants aux problèmes qui permettent de mettre en pratique les notions apprises ou de les approfondir par la recherche.

Dans le domaine de la sécurité informatique, les plateformes web sont les plus fréquemment affectées par des failles. C'est dans cette optique que, l'organisateur **F5 Labs** en collaboration avec **bjCSIRT** et **AfricaCERT**, organisent un événement de type « Capture the Flag » basé sur le thème de la sécurité des API pour in fine éduquer et former les participants sur un des aspects importants de la sécurité des applications web.

II. API SECURITY CTF

II.1. Qu'est ce qu'un CTF ?

Dans le monde de la cybersécurité, le CTF « capture the flag » (capture du drapeau en français) est un jeu dans lequel les concurrents (individuels ou en équipe) tentent de capturer les drapeaux à travers la résolution d'exercices pratiques afin de marquer le plus de points pour gagner la partie. Les exercices présentent des systèmes intentionnellement vulnérables que les concurrents doivent réussir à compromettre. Chaque "drapeau" qu'ils réussissent à capturer (par exemple en découvrant un fichier contenant une chaine de caractères) leur rapportera des points et les fera monter dans un classement. Les CTF ne sont pas seulement un excellent moyen de prouver les compétences, mais aussi une méthode pour les débutants d'apprendre à penser comme des hackers. L'évènement « CTF API Security » en lui-même dure environ 1 heure et maintient un affichage des scores en direct de tous les concurrents.

Une fois la compétition terminée, l'équipe F5 Labs attribuera des prix aux gagnants et guidera chacun à travers les défis pour montrer comment ils auraient pu être relevés. Même en tant que débutant en cybersécurité, API Security CTF permettra d'instruire les participants aux méthodes qu'utilisent les attaquants lors de la recherche des vulnérabilités dans les applications web et spécifiquement comment ils ciblent les API.

API Security CTF est conçu à des fins éducatives et, en tant que tel, de nombreux défis devraient être relativement faciles pour les expérimentés.

II.2. Exigences

Tous les défis peuvent être relevés en utilisant uniquement des outils du navigateur web et des scripts. Cependant, quelques outils offrent également un moyen de compléter les challenges tels que :

- Postman : https://www.postman.com/downloads/
- THC-Hydra : https://securitytutorials.co.uk/brute-forcing-passwords-with-thc-hydra/

(Facultatif)

- Un navigateur Web à jour et une connaissance des outils de développement
- Une certaine connaissance de JSON, des requêtes HTTP, des en-têtes et des mécanismes d'authentification.

III. ORGANISATEURS :

- Les équipes F5 Labs, bjCSIRT et AfricaCERT

IV. OBJECTIF

- Éduquer les participants aux vulnérabilités des API.

V. RESULTAT

Les participants sont capables de détecter les vulnérabilités liées aux API, savoir comment y remédier et savoir les sécuriser.

VI. PARTICIPANTS

- Étudiants à l'université suivant des cours en informatique (de la 1ere à la 3e année) ;
- Tranche d'âge : 17 à 22 ans ;
- Une priorité sera accordée aux jeunes femmes étudiantes en informatique ;

VII. LIEU ET DATE (sous réserve de modifications)

- **10 Septembre 2021 à 15 heures (GMT)**
- En ligne (les organisateurs fourniront les liens d'enregistrement et de participation)

VIII. PROGRAMME PRELIMINAIRE (sous réserve de modifications)

Horaire	Activité	Durée
	Exposé de F5 Labs sur les incidents de sécurité des API (c'est-à-dire l'importance de la sécurité des API)	15 minutes
	Explication et présentation de l'événement	15 minutes
	Top départ du CTF	60 minutes
	Courtes pauses toutes les 15 minutes pour prodiguer des conseils et indices	5 minutes
	Fin de la partie: annonce du gagnant (prix compris, etc)	5 min
	Démonstrations et solutions : pour les participants qui voudraient connaître les solutions aux challenges, F5 Labs présentera quelques moyens de relever certains des défis.	30 minutes

Veuillez noter que l'événement se tiendra exclusivement en Anglais ;

IX. LOTS GAGNANTS

1ere place : une certification OSCP: Offensive Security Certified Professional

2e place: une certification CEH: Certified Ethical Hacker (CEH)

3e place : une certification Certified Network Defender (CND)

I. CONTEXT OF THE EVENT

Digital technology and the rise of cybersecurity today are both pillars of development on the African continent. To better prepare the young generation for the security challenges of the sector there is a necessity to increase the skills of learners in the field. Thus, to be more competitive, computer science students must be proficient in operating systems, application services, software engineering, system administration, scripting, and networking. Learning through CTFs has proven to be effective and allows apprentices to be exposed to problems that allow the concepts learned to be put into practice or to be deepened through research.

In the world of computer security, web platforms are the most frequently affected by flaws and vulnerabilities. It is with this in mind that the organizers F5 Labs in collaboration with bjCSIRT and AfricaCERT are organizing a “Capture the Flag” type event based on the theme of **API security**.

II. API SECURITY CTF

II.1. What is a CTF?

In cybersecurity, CTF "capture the flag" is a game in which the competitors (individual or in team) try to capture the flags through the resolution of practical exercises to score the most points and win the game. The exercises present intentionally vulnerable systems that competitors must succeed in compromising. Each "flag" they manage to capture (e.g.by learning a secret) will earn them points and move them up a leaderboard. CTFs are not only a great way to prove skills, but also a method for beginners to learn to think like hackers. The "CTF API Security" event itself runs for approximately one (01) hour and maintains a live score display of all competitors.

Once the competition is over, the F5 Labs team will award prizes to the winners and guide everyone through each of the challenges to show how they could have been completed. Even as a cybersecurity beginner, API Security CTF will allow them to learn how attackers plan to attack applications and, in this case, how they target APIs. API Security CTF is designed for educational purposes, and as such, many challenges should be relatively easy for experienced developers.

2.2 Requirements

All of the challenges can be completed using only browser tools and some simple scripting. However, security tools provide an alternative way to complete some of them.

Some tools that may be useful include:

- Postman https://www.postman.com/downloads/
- THC-Hydra https://securitytutorials.co.uk/brute-forcing-passwords-with-thc-hydra/

(Optional)

- An up-to-date web browser and familiarity with the developer tools it provides
- Some knowledge of JSON, HTTP transactions, headers and authentication schemes

III. ORGANIZERS:

- F5 Labs, bjCSIRT and AfricaCERT teams

IV. OBJECTIVES

- Educate participants about API vulnerabilities.

V. RESULT

- Participants are able to detect API vulnerabilities, how to remediate these vulnerabilities and know how to secure API.

VI. PARTICIPANTS

- University students taking computer courses or related (from 1st to 3rd year);
- Age group: 17 to 22 years old;
- Priority will be given to young female computer science students.

VII. PLACE AND DATE (subject to change)

- **September 10th 2021 at 3pm (UTC)**
- Online (the organizers will provide the registration and participation links)

VIII. PRELIMINARY SCHEDULE (subject to change)

Schedu-le	Activity	Duration
	F5 Labs overview of API security incidents (i.e. why should we care about API security)	15 min
	Explanation and run-through of the event	15 min
	The game begins: contestants attempt to complete the challenges	60 min
	Short breaks every 15 minutes to give tips and clues	5 min
	Game concludes: announcement of the winner (inc. prizes, etc)	5 min
	Show and tell: for those that want to stick around we take them through some ways to complete some of the challenges	30 min

Please note the event will be held exclusively in English.

IX. WINNERS PRIZES

1st place : Offensive Security Certified Professional certification (OSCP)

2nd place : Certified Ethical Hacker certification (CEH)

3rd place: Certified Network Defender Certification (CND)