

Ala Bouali

Tunisie Chaffar, Sfax 3044

admin@alabouali.com

+21658857249

<https://github.com/AlaBouali/>



Développeur web full-stack & Hacker éthique

COMPÉTENCES DIFFICILES

- Tests d'intrusion : Nmap, BurpSuite et tests manuels .
- Frameworks : Flask (3 ans d' expérience) , Odoo (2 ans d' expérience) , Django / FastAPI / Symfony (moins d' 1 an d' expérience chacun) , ReactJS / NextJS (suivi de tutoriels simples mais pas encore de gros projets) .
- Langages de programmation : Python / PHP (5 ans d' expérience) , JS / Java (2 ans d' expérience) , C / C # (1 an d' exp. au collège) .
- Outils de contrôle de version DevOps : Git, Github.
- Patrons architecturaux logiciels : MVC .
- Serveurs Web : Apache.
- Plates-formes cloud : Google Cloud Platform (GCP).
- Déploiement d'applications web sur : Heroku , Namecheap .
- Systèmes de gestion de contenu (CMS) : WordPress (<https://alabouali.com>).

SOMMAIRE

Je suis un programmeur autodidacte (depuis 2017) / pentester (depuis 2018) / freelancer (depuis 2019) qui adore le pentesting, le codage, le débogage et la résolution de problèmes ! Je trouve ça amusant et j'essaie d'en vivre. Je travaille généralement sur des projets seul et m'occupe de tout, mais aussi, je peux travailler avec une équipe où j'ai assigné des tâches spécifiques à faire par moi-même. Je suis une personne communicative et je fais de mon mieux pour livrer la meilleure version optimisée de mon travail dans les délais.

ÉDUCATION

- Informatique à l'ISIM Sfax : 2018 - 2022 .
- Licence Sciences Expérimentales (2018) : Lycée Ali Bourguiba .

CERTIFICATES

- [Learning Python](#)
- [Learning PHP](#)
- [Learning Java](#)
- [React.js Essential Training](#)
- [Flask Essential Training](#)
- [Building RESTful APIs with Flask](#)
- [Full Stack Web Development with Flask](#)
- [Django Essential Training](#)
- [Ethical Hacking: Hacking Web Servers and Web Applications](#)
- [Python for Security](#)
- [Secure Coding in Python](#)
- [Cybersecurity for IT Professionals](#)

EXPERIENCE

DES STAGES

- [ISIM Sfax](#): Réalisation d'un test d'intrusion sur le site Web de l'université et découverte de multiples vulnérabilités dans le cadre d'un stage .

TRAVAIL (EN TANT QU'INDEPENDANT) : 2019 – 2022

- [NMTC - Camp national des technologies Microsoft](#): A effectué un test d'intrusion sur son site Web après avoir obtenu l'autorisation du président du Microsoft Club ISIMS et signalé de multiples vulnérabilités.
- [Area-01](#): Le site subissait une attaque DDoS et j'avais été contacté pour apporter une solution et protéger le site. L'attaque a été mitigée avec succès.
- Techcom Chaffar : Installer Odoo sur Ubuntu 20.04 LTS VPS, gérer le serveur, le sécuriser, configurer l'application Odoo et installer des modules supplémentaires.
- Piedra : Installer Odoo sur un serveur Windows, gérer le serveur, le sécuriser, configurer l'application Odoo et installer des modules supplémentaires.

- Applications de bureau : Tkinter.
- Systèmes d'exploitation : Linux et Windows.
- Gestion de bases de données : SQLAlchemy (SQLite , MySQL , MariaDB , Oracle , PostgreSQL & MS SQL) , PyMongo (MongoDB) , Firebase (configurations et : gestion des utilisateurs, du stockage et des bases de données en temps réel) .
- Développement et intégration d'API : RESTAPI et JWT Authentication .
- WebSockets (intégré à FastAPI dans 1 projet).
- Réseaux : Scapy (capture, analyse et modification des paquets réseau et réalisation d'attaques).
- Réseau de distribution de contenu (CDN) et services de protection DDoS : CloudFlare .
- Comprendre les bases : Docker, python virtuel environnement & kubernetes .
- Autres compétences : sélénium, web scrapping & automatisation .

COMPÉTENCES COMMUNES

- Résolution de problèmes.
- La pensée créative .
- Personne flexible, adaptative et communicative.
- Éthique de travail élevée.

LANGUES

- arabe
- Anglais
- Français

BADGES LINKEDIN : [Ala Bouali](#)

- API Python / PHP / REST : dans le top 5% des personnes ayant passé l'évaluation .
- MySQL / Django : dans le top 30% des personnes ayant passé l'évaluation .

- Fournir des services aux personnes pour créer de petites applications Web avec Flask, corriger leurs scripts (python principalement), corriger les bogues, réviser le code et sécuriser leurs applications Web.

PROJETS

DES APPLICATIONS WEB

- Une plateforme pour un centre de formation permettant de gérer ses utilisateurs (formateurs et participants) ont chacun leurs permissions et actions, avec un panneau d'administration pour gérer en plus des utilisateurs : cours, sessions de formation, posts, événements... Elle a été créée à l'aide de Flask, SQLAlchemy , HTML & Tailwind (CSS) . Compte administrateur par défaut : admin / admin . Lien: <https://coursescenter.herokuapp.com/> Une application web d'analyse de données qui permet de :
 - 1- Télécharger les fichiers Excel et les enregistrer en historique et les analyser pour les présenter sous forme d'histogramme des différents TOP n défauts selon CreateTime.
 - * ERROR_Log (TOP n de ScriptNameUser selon CreateTime (le choix de l'intervalle de date et n saisi par l'utilisateur depuis un formulaire))
 - * REW_Log ((TOP n de KSK selon CreateTime) (TOP n de OperatorComment selon CreateTime))
 - * ERROR_Log et REW_Log affichent des erreurs dans le système de production de l'entreprise. Ces analyses facilitent la prise de décision.
 - 2- Gérer les commentaires (OperatorComment) qui présentent le problème identifié par les employés et l'afficher sous forme d'histogrammes des différents TOP n défauts : o Purifier les commentaires. o Préparation des commentaires types. o Remplacez les anciens commentaires par des commentaires préparés. o Afficher les commentaires sous forme d'histogramme.
 - 3- Autoriser l'administrateur à ajouter de nouveaux utilisateurs (employés) et accordez-leur chacun leurs droits d'accès.
 - 4- Autoriser les utilisateurs à gérer leur compte. Utilisé : Flask , SQLAlchemy , Matplotlib , HTML , Tailwind (CSS) .
- **Stajili**: un moteur de recherche pour gratter et présenter des offres de stages aux collégiens pour faciliter leur recherche et gagner du temps. Créé avec « Flask-man » : Flask, HTML, CSS, Javascript et firebase pour les utilisateurs et la gestion de base de données en temps réel. Lien : <https://stajili.herokuapp.com/> Enregistrement d'écran : <https://vimeo.com/689000991/b50640aca1>
- **Scanner Web en ligne de Bane**: un scanner de vulnérabilité en ligne basé sur mon précédent projet "bane". Il prend votre page cible et effectue l'analyse préférée puis représente le résultat de l'analyse sur un tableau HTML. Lien : <http://bane-demo.herokuapp.com/> Filtrer enregistrement: <https://vimeo.com/689015484/cd688fb0f9>
- **Application de gestion des bureaux pour la poste tunisie**: J'ai utilisé Flask sur le back-end, HTML et CSS pour le front-end et SQLite comme base de données. Il s'agit d'un compte de test sur la version de test en direct de l'application. Matricule : 111111 Mot de passe : test Région : Nabeul Lien : <https://gestion-bureaux-poste.herokuapp.com/connexion.html> Enregistrement d'écran: <https://vimeo.com/688959163/dd967f3b92>

MENTIONS HONORABLES POUR MES PROJETS

- [Meilleurs scanners CSRF \(bane\).](#)
- [Cadre de piratage tout-en-un pour l'équipe rouge Pentesting.](#)
- [Les 4 meilleurs dépôts Python IoT Hacking \(bane\).](#)
- [Meilleurs scanners XSS \(bane\).](#)
- [Meilleurs projets open source d'exécution de code à distance \(bane\).](#)
- [Meilleurs projets open source d'attaques Bruteforce \(bane\).](#)
- [Meilleurs projets open source de détournement de clic \(bane\).](#)
- [Mentionné dans les formulaires de Huawei comme alternative à telnetlib pour contrôler à distance les routeurs via le protocole telnet \(xtelnet\).](#)

DÉVELOPPEMENT WEB

- **School uploads:** un partage et stockage de fichiers (sur firebase) pendant une durée définie. Vous téléchargez des fichiers jusqu'à 300 Mo et l'application les conservera avec votre nom jusqu'à une date de votre choix.
Lien : <https://school-uploads.herokuapp.com/>
Enregistrement d'écran : <https://vimeo.com/689020710/3cc3331e27>

PROJETS PERSONNELS

SÉCURITÉ

- **Bane :** (135 STARS / 39 FORKS) un module pur python que j'ai créé pour automatiser et faciliter le processus de recherche de vulnérabilités web et réseaux avec aucun outil de pentest externe n'est nécessaire.
<https://github.com/AlaBouali/bane>
- **Sanitizy :** un autre module python pour fournir une couche de sécurité supplémentaire à vos projets python en fournissant des classes avec des fonctions statiques pour assainir, filtrer et bloquer les entrées malveillantes.
<https://github.com/AlaBouali/sanitizy>
- **Flask-man :** module python pour créer et gérer vos projets Flask plus facilement en créant les fichiers et bases de données nécessaires, les tables, les codes et en installant les exigences pour eux. Cela fait gagner du temps et facilite le développement du projet grâce aux fichiers python contenant chacun des fonctions utiles, des classes et des variables prédéfinies, bien organisées et nommées ! Il a tout le nécessaire pour créer de grands projets.
https://github.com/AlaBouali/flask_man

RÉSEAU / IoT

- **Xtelnet :** un module python pour authentifier, exécuter des commandes et recevoir une sortie de manière plus simple via le protocole telnet avec 1 ou plusieurs machines à distance en parallèle (un meilleur remplacement pour "telnetlib") .
Idéal pour les IoT pour un contrôle meilleur et plus fluide. Cela fonctionne parfaitement avec presque n'importe quel serveur telnet!
<https://github.com/AlaBouali/xtelnet>

PRIX

- Remercié par l'administration de [Sup'Com](#) pour avoir trouvé plusieurs vulnérabilités sur leur site Web (2022).
- Remercié par l'administration de [ISIM Sfax](#) pour avoir trouvé plusieurs vulnérabilités sur leur site Web (2021).
- Trouvé 2 bogues de type de risque d'abus valides sur Google (2020).
- Récompenses sur Hackerone : [Ala Bouali](#).