

Prérequis

(+) Avoir python ou python3 installé

(+) Avoir Git installé

Installation

1 - Télécharger le projet sur git en tapant dans votre invite de commande :

```
git clone https://github.com/alexispondo/ScanPlus.git
```

2 - Installer les modules nécessaires

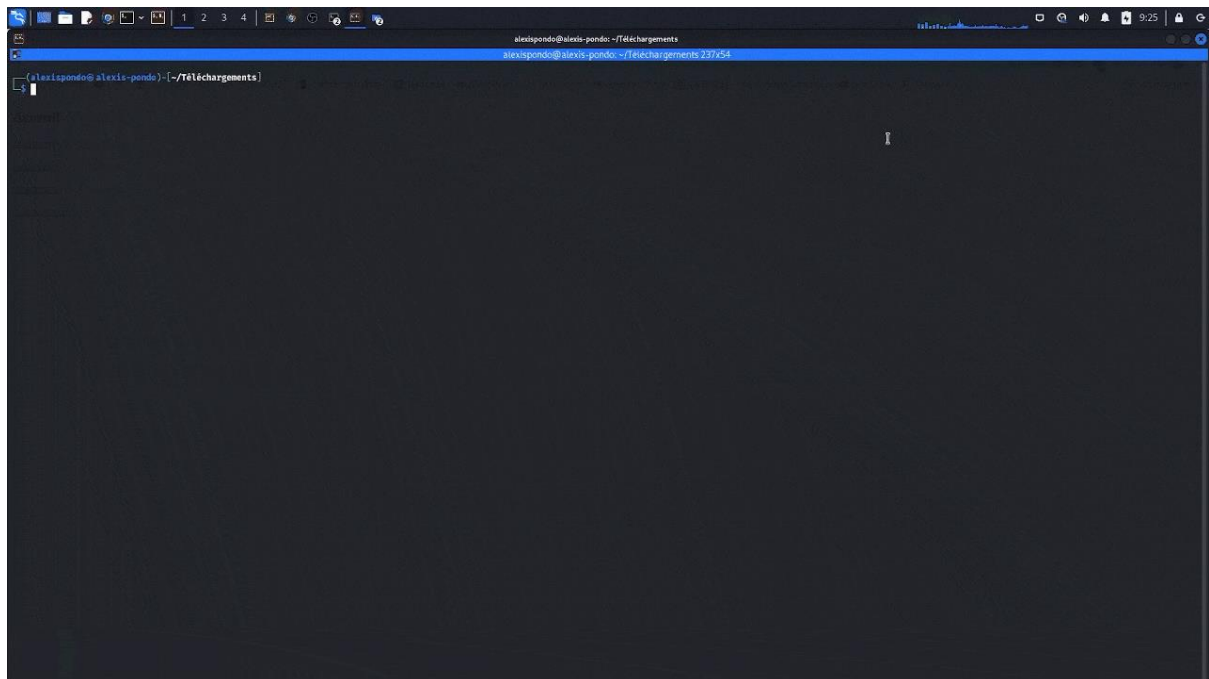
cd ScanPlus

cd ScanPlus

python3 installer.py ou python installer.py

3 – Démarrer le programme

python3 index.py ou python index.py



Caractéristiques du programme

Nom de programme : ScanPlus

Description : ScanPLus est un programme de scan de vulnérabilités permettant de détecter les failles de sécurité d'une application web.

Atouts : Ce programme apporte un plus de par sa conception qui lui permet d'effectuer plusieurs types de scans différents dans une même application web. Aussi il est important de préciser que l'outil est portable donc peut s'exécuter sur tous les OS.

Les scans effectués

1) Scan Global

Scan Global est le type de scan qui permet de détecter les vulnérabilités liées à la présentation de l'application web qui peuvent être exploitées par un attaquant. Ce type de scan permet entre autres de :

- Détecter les fichiers robots.txt
- Détecter les fichiers sitemap.xml
- Voir si le protocole de transfert de HyperText (http/https) est sécurisé ou non
- Détecter le langage de programmation de l'application
- Détecter le nom et la version du serveur web

```
alexispondo@alexis-pondo: ~/Téléchargements/ScanPlus/ScanPlus  
$ ./scanplus.py --help  
  
Demarrage ScanPlus...  
  
$$$$$$\n    $$$$ $\n$ $ _-$\n/$$_\\_||_$$$$$$$$ $$$ $$$$ $$$ |$\n\\$$$$$$$ $$_|_$$$ _$$$ \\$$$$$$$ $$$ $$$ |$ $$$ |\n   _$$$ $$$ /_$$$$$$$ $$$ | $$$ $$$ $$$ ||_|$$$$$$$$|\n$$_ $$_ $$$ _$ _$ $$$ | $$$ $$$ | $$$ | $$$ |\n\\$$$$$$$ \\$$$$$$$\\\\$$$$$$$ $$$ | $$$ | $$$ \\$$$$$$$ \\\\$$$$$$$)\n\nName: ScanPlus  
Version: v2.0  
Author : {  
    Developpeur : {  
        Nom: PONDIO Alexis  
        LinkedIn: https://www.linkedin.com/in/alexis-pondo/  
    },  
    Developpeur : {  
        Nom: DIDIA Suzanne  
        LinkedIn: https://www.linkedin.com/in/suzanne-didia-pa6384c7fa/  
    },  
    Developpeur : {  
        Nom: KONE Souman  
        LinkedIn: https://www.linkedin.com/in/souman-franck-aristide-konCSYAO9-BB7I7417A/  
    }  
}  
Github: https://github.com/alexispondo/ScanPlus
```

ScanPlus est un programme de scan de vulnérabilité développé par les étudiants de l'ESATIC.
Ce programme permet de scanner plusieurs vulnérabilités communes des sites web.
Sa différence vient du fait qu'il peut effectuer plusieurs types de scans distinct et indépendamment de la plateforme.

Quel scan voulez-vous exécuter ?

- 1) Scan Global
- 2) Scan Is_BruteForce
- 3) Scan CommonUserPass
- 4) Scan Injection SQL
- 5) Scan Injection XSS
- 6) Scan Injection de commande
- q) Quitter

```
$ ./scanplus.py
```

2) Scan Is_BruteForce

Le scan is_BruteForce est un scan qui permet de détecter si un formulaire de connexion est BruteForçable. En effet le programme test 10 connexions erronées consécutives et observe la réaction du serveur. Le formulaire de connexion est sécurisé si à partir d'un certain nombre d'essais z(03 ou 04), le serveur refuse les demandes de connexions à cause du nombre de tentatives de connexion, dans le cas contraire il est BruteForçable.

```
alexispondo@alexis-pondo:~/Téléchargements/ScanPlus/ScanPlus$ ./scanplus.py
démarrage ScanPlus...

$$$$$$\ $$(
$$ _$$$ \ $$$
$$ / \_ | $$$$$$\\ $$$$$$\\ $$$ | $$$ $$$ \\ $$$ | $$$ $$$$$$\\
\\$$$$$\\ $$$ / \_ | $$$ $$$ \\ $$$ | $$$ $$$ \\ $$$ | $$$ $$$ \\
$$$ \\ $$$ \\ $$$ _$$$ $$$ | $$$ $$$ \\ $$$ $$$ | $$$ \\ $$$ \\
\\$$$$$\\ \\$$$$$\\ \\$$$$$\\ $$$ | $$$ $$$ \\ $$$ \\$$$$$\\ \\$$$$$\\ \\

Name: ScanPlus
Version: v2.0
Author: {
    Developpeur: {
        Nom: PONGO Alexis
        LinkedIn: https://www.linkedin.com/in/alexis-pondo/
    },
    Developpeur: {
        Nom: DIDIA Suzanne
        LinkedIn: https://www.linkedin.com/in/suzanne-didia-9a63047a/?
    },
    Developpeur: {
        Nom: KONE Souman
        LinkedIn: https://www.linkedin.com/in/souman-franck-aristide-konsC3A9-ab717417a/?
    }
}
GitHub: https://github.com/alexispondo/ScanPlus

scanPlus est un programme de scan de vulnérabilité développé par les étudiants de l'ESATIC.
Ce programme permet de scanner plusieurs vulnérabilités communes des sites web.
Sa différence vient du fait qu'il peut effectuer plusieurs types de scans distinct et indépendamment de la plateforme.

quel scan voulez-vous exécuter ?
1) Scan Global
2) Scan Is_BruteForce
3) Scan CommonUserPass
4) Scan Injection SQL
5) Scan Injection XSS
6) Scan Injection de commande
q) Quitter
scanPlus> 
```

3) Scan CommonUserPass

Le Scan CommonUserPass est un Scan qui vérifie si un formulaire de connexion est vulnérable aux noms d'utilisateur et mots de passe communs. Le programme prend en paramètre l'URL de la page de connexion, les inputs tels que username, password, submit et le message d'erreur qui est retourné lorsque les identifiants sont incorrects.

```
alexispondo@alexis-pondo: ~/projet_pi/ScanPlus
alexispondo@alexis-pondo: ~/projet_pi/ScanPlus 237x54

1) Scan Global
2) Scan IsBruteForce
3) Scan CommonUserPass
4) Scan Injection SQL
5) Scan Injection XSS
6) Scan Injection de commande
q) Quitter

scanplus> 3

=====
Vous avez choisi le scan des informations d'identification commune

Entrez l'URL de la page de connexion ex: https://example.com/login
scanplus> url >> http://127.0.0.1/Web/con.php

Entrez le nom de l'input username, ex: user
scanplus> username >> username

Entrez le nom de l'input password, ex: pass
scanplus> password >> pass

Entrez le message d'erreur, ex: Identifiants invalides.
scanplus> error >> Désol

Entrez le nom du bouton d'envoi, ex: submit
scanplus> submit >> submit

login-1 : username = admin || password = admin ===== Username or Password Incorrect
login-2 : username = admin || password = pass ===== Username or Password Incorrect
login-3 : username = admin || password = password ===== Username or Password Incorrect
login-4 : username = user || password = 1234 ===== Username or Password Incorrect
login-5 : username = 17-CM7ICM77M2 || password = p0ss3ssw0rd ===== Username or Password Incorrect
login-6 : username = user || password = user ===== Username or Password Incorrect
login-7 : username = user || password = pass ===== Username or Password Incorrect
login-8 : username = admin || password = pass1234 ===== Username or Password Incorrect
login-9 : username = admin || password = 1234 ===== Username or Password Incorrect
login-10 : username = root || password = root ===== Username or Password Incorrect
login-11 : username = username || password = password ===== Username or Password Incorrect
login-12 : username = pondo || password = pondo ===== Correct Username and Password

=====
Vous avez choisi le scan des informations d'identification commune

Entrez l'URL de la page de connexion ex: https://example.com/login
scanplus> url >> [ ]
```

4) Scan d'injection SQL

Ce Scan permet de détecter si un formulaire de connexion est vulnérable aux injections SQL. Le programme prend en paramètre l'URL de la page de connexion les names des input username, password, submit et le message d'erreur qui est retourné lorsque les identifiants sont incorrects. Le programme teste ensuite une liste de commandes d'injection SQL pour détecter celle qui arrive à bypasser le formulaire.

```
alexispondo@alexis-pondo: ~/projet_pi/ScanPlus
alexispondo@alexis-pondo: ~/projet_pi/ScanPlus 237x54

Quel scan voulez-vous exécuter ?

1) Scan Global
2) Scan IsBruteForce
3) Scan CommonUserPass
4) Scan Injection SQL
5) Scan Injection XSS
6) Scan Injection de commande
q) Quitter

scanplus> 4

=====
Vous avez choisi un scan d'injection sql

Entrez l'URL de la page de connexion ex: https://example.com/login
scanplus> url >> http://127.0.0.1/Web/con.php

Entrez le nom de l'input username, ex: user
scanplus> username >> username

Entrez le nom de l'input password, ex: pass
scanplus> password >> pass

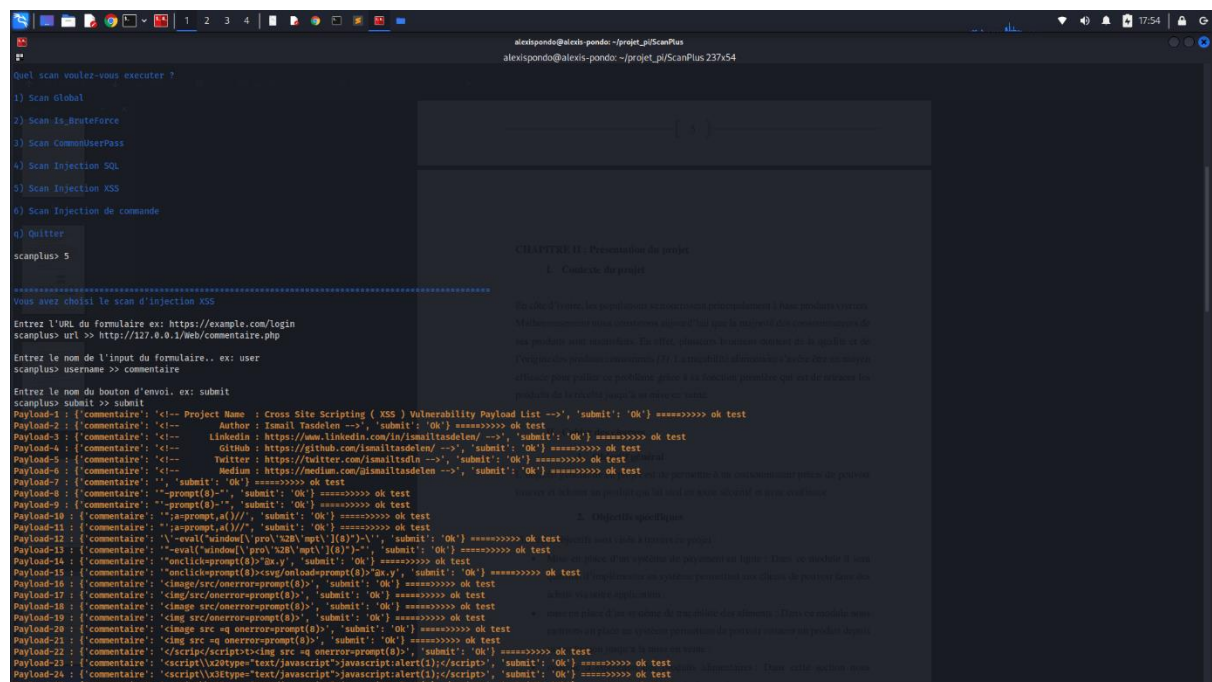
Entrez le message d'erreur, ex: Identifiants invalides.
scanplus> error >> Désolé

Entrez le nom du bouton d'envoi, ex: submit
scanplus> submit >> submit

login-1 : username = ' || password = ' || ===== Bad Login
login-2 : username = ' || password = ' || ===== Bad Login
login-3 : username = ' || password = ' || ===== Bad Login
login-4 : username = ' || password = ' || ===== Bad Login
login-5 : username = ' || password = ' || ===== Bad Login
login-6 : username = ' or ' || password = ' or ' || ===== Bad Login
login-7 : username = ' or ' || password = ' or ' || ===== Bad Login
login-8 : username = ' or ' || password = ' or ' || ===== Bad Login
login-9 : username = ' or ' || password = ' or ' || ===== Bad Login
login-10 : username = ' or ' || password = ' or ' || ===== Bad Login
login-11 : username = ' || password = ' || ===== Bad Login
login-12 : username = ' || password = ' || ===== Bad Login
login-13 : username = ' || password = ' || ===== Bad Login
login-14 : username = ' || password = ' || ===== Bad Login
login-15 : username = ' || password = ' || ===== Bad Login
login-16 : username = ' or ' || password = ' or ' || ===== Bad Login
login-17 : username = ' or ' || password = ' or ' || ===== Bad Login
login-18 : username = ' or ' || password = ' or ' || ===== Bad Login
```

5) Scan d'injection XSS

Ce Scan permet de détecter si un formulaire de commentaire par exemple est vulnérable aux injections XSS. Le programme prend en paramètre l'URL de la page de commentaire, les noms des inputs : commentaire et du submit. Le programme teste ensuite une liste de commandes d'injection XSS pour détecter celles qui arrivent à affecter l'application. Il faudra ensuite vérifier les effets sur l'application pour voir leurs impacts.



```
alexispondo@alexis-pondo: ~/projet_pi/ScanPlus
alexispondo@alexis-pondo: ~/projet_pi/ScanPlus$
Quel scan voulez-vous exécuter ?
1) Scan Global
2) Scan IsBruteForce
3) Scan CommenterPass
4) Scan Injection SQL
5) Scan Injection XSS
6) Scan Injection de commande
a) Quitter
ScanPlus 5
Vous avez choisi le scan d'injection XSS
Entrez l'URL du formulaire ex: https://example.com/login
ScanPlus: url >> http://127.0.0.1/web/commentaire.php
Entrez le nom de l'input du formulaire.. ex: user
ScanPlus: username >> commentaire
Entrez le nom du bouton d'envoi. ex: submit
ScanPlus: submit >> submit
Payload-1: { 'commentaire': '<!-- Project Name : Cross Site Scripting ( XSS ) Vulnerability Payload List -->', 'submit': 'Ok' } ===== ok test
Payload-2: { 'commentaire': '<!-- Author : Ismail Tasdelen -->', 'submit': 'Ok' } ===== ok test
Payload-3: { 'commentaire': '<!-- LinkedIn : https://www.linkedin.com/in/ismailtasdelen/ -->', 'submit': 'Ok' } ===== ok test
Payload-4: { 'commentaire': '<!-- GitHub : https://github.com/ismailtasdelen/ -->', 'submit': 'Ok' } ===== ok test
Payload-5: { 'commentaire': '<!-- Twitter : https://twitter.com/ismailtasdelen -->', 'submit': 'Ok' } ===== ok test
Payload-6: { 'commentaire': '<!-- Medium : https://medium.com/ismailtasdelen -->', 'submit': 'Ok' } ===== ok test
Payload-7: { 'commentaire': '<!-- prompt(0)-->', 'submit': 'Ok' } ===== ok test
Payload-8: { 'commentaire': '<!-- prompt(0)-->', 'submit': 'Ok' } ===== ok test
Payload-9: { 'commentaire': '<!-- prompt(0)-->', 'submit': 'Ok' } ===== ok test
Payload-10: { 'commentaire': '<!-- prompt(0)-->', 'submit': 'Ok' } ===== ok test
Payload-11: { 'commentaire': '<!-- prompt(0)-->', 'submit': 'Ok' } ===== ok test
Payload-12: { 'commentaire': '<!-- eval(window.prompt(0))-->', 'submit': 'Ok' } ===== ok test
Payload-13: { 'commentaire': '<!-- eval(window.prompt(0))-->', 'submit': 'Ok' } ===== ok test
Payload-14: { 'commentaire': '<!-- eval(window.prompt(0))-->', 'submit': 'Ok' } ===== ok test
Payload-15: { 'commentaire': '<!-- eval(window.prompt(0))-->', 'submit': 'Ok' } ===== ok test
Payload-16: { 'commentaire': '<!-- eval(window.prompt(0))-->', 'submit': 'Ok' } ===== ok test
Payload-17: { 'commentaire': '<!-- eval(window.prompt(0))-->', 'submit': 'Ok' } ===== ok test
Payload-18: { 'commentaire': '<!-- eval(window.prompt(0))-->', 'submit': 'Ok' } ===== ok test
Payload-19: { 'commentaire': '<!-- eval(window.prompt(0))-->', 'submit': 'Ok' } ===== ok test
Payload-20: { 'commentaire': '<!-- eval(window.prompt(0))-->', 'submit': 'Ok' } ===== ok test
Payload-21: { 'commentaire': '<!-- eval(window.prompt(0))-->', 'submit': 'Ok' } ===== ok test
Payload-22: { 'commentaire': '<!-- eval(window.prompt(0))-->', 'submit': 'Ok' } ===== ok test
Payload-23: { 'commentaire': '<!-- eval(window.prompt(0))-->', 'submit': 'Ok' } ===== ok test
Payload-24: { 'commentaire': '<!-- eval(window.prompt(0))-->', 'submit': 'Ok' } ===== ok test
```

6) Scan d'injection de commande

Ce Scan permet de détecter si un formulaire de recherche par exemple est vulnérable aux injections de commandes. Le programme prend en paramètre l'URL de la page de recherche, les noms du formulaire de recherche et du submit. Le programme teste ensuite une liste de commandes d'injection de commandes pour détecter celles qui arrivent à exécuter des commandes sur le système. Il faudra ensuite vérifier les effets sur l'application pour voir leurs impacts.


```
alexispondo@alexis-pondo: ~/projet_pi5canPlus
alexispondo@alexis-pondo: ~/projet_pi5canPlus

<form method="POST" action="comande.php">
  <label>IP</label><br>
  <input type="text" name="ip"><br><br>
  <input type="submit" name="submit">
</form>
</div>

<pre></pre>
</div>
</body>
</html>
Payload-10 : {'ip': 'id', 'submit': 'Ok'} =====>>> ok test

<DOCTYPE html>
<html>
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>IP</title>
</head>
<body>
  <a href="index.php?Returnc/a">
    <h2>Entrez votre IP</h2>
    <form method="POST" action="comande.php">
      <label>IP</label><br>
      <input type="text" name="ip"><br><br>
      <input type="submit" name="submit">
    </form>
  </div>

<pre>uid=1(daemon) gid=1(daemon) groupes=1(daemon)
</pre>
</div>
</body>
</html>
Payload-11 : {'ip': 'id', 'submit': 'Ok'} =====>>> ok test

<DOCTYPE html>
<html>
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>IP</title>
```