Scanner de vulnérabilités avec Wapiti

DOCUMENT CREATED
BY ERICSSON

CYBERSÉCURITÉ

Étape 1 : Lancer Wapiti

```
WAPITI(1)                                                    WAPITI(1)

NAME
       wapiti - A web application vulnerability scanner in Python

SYNOPSIS
       wapiti -u BASE_URL [options]

DESCRIPTION
       Wapiti  allows  you  to  audit the security of your web applica-
       tions.
```

Sur Kali Linux, ouvre un terminal.

Commandes à exécuter :

- Scanne l'application web avec Wapiti :

wapiti -u http://172.16.10.2/mutillidae -o /root/wapiti-report

Options :

- -u : URL cible.
- -o : Nom du fichier pour sauvegarder le rapport (ici rapport.html).

Étape 2 : Analyser le rapport

```
[*] Launching module sql
---
MySQL Injection in http://172.16.10.5/mutillidae/index.php via injection in the parameter username
Evil request:
    GET /mutillidae/index.php?page=user-info.php&username=%C2%BF%27%22%28&password=Letm3in_&user-info-php-submit-button
=View+Account+Details HTTP/1.1
    Host: 172.16.10.5
    Referer: http://172.16.10.5/mutillidae/index.php?page=user-info.php
```

Ouvrir le rapport :

- Une fois le scan terminé, ouvrez le fichier généré :

xdg-open rapport.html

Analysez les vulnérabilités listées, comme :

- Failles XSS.
- Vulnérabilités SQL Injection.
- Directories accessibles.