Sensitive Data Exposure

Lab 2: Fuzzing using Feroxbuster | Sensitive Data Exposure

When website does not have robots.txt or it could not contain such information as we saw in previous lab. This is the case which means we don't know the sensitive file on server which are publicly available. So, we need to find URI instead robots.txt as URI.

One way: Type every URI manually one by one.

https://github.com/danielmiessler/SecLists/blob/master/Discovery/Web-Content/common.txt

Second way: Hacker take a word list, where different possible path/URI available and that can be used one by one or go with any tool.

Go and read this HTTP response status code:

https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Status

follow these steps:

Step 1: Save Word list as file (In our case in Desktop).

Step 2: Open **https://portswigger.net/**

Step 3: Go to "information disclosure on debug page" under information disclosure section.

Step 4: We can use different tools to prevent with manual typing each URI and so for this:

Gobuster: https://github.com/OJ/gobuster

ffuf: https://github.com/ffuf/ffuf

Dirbuster: https://github.com/kajanM/DirBuster

feroxbuster: https://github.com/epi052/feroxbuster

Step 5: Here we are selecting feroxbuster as a tool so open kali and install it by:

Sudo apt update && sudo apt install -y fereoxbuster

Step 6: Follow the instruction from given GitHub page or if using Linux and located in same directory where Word list file located then type command:

curl -sL https://raw.githubusercontent.com/epi052/feroxbuster/main/install-nix.sh | bash

Step 7: Step 6: Read the Desktop (Since Word List file is in Desktop: common.txt) from terminal. Now execute:

$ ./feroxbuster –help

$ ./feroxbuster -u URL_Of_WebSecurity_Academy.net/ -w common.txt

This will do brute force with all word list one by one in this target URL.

Step 8: Click on .php file> find secret key. Go to discloser under environment and submit the secret key.

Note: This fuzzing is the part of recon and came into the under the category of Active reconnaissance.