Dirb / Gobuster

Se tratando de web hacking algo muito útil é identificar os diretórios existentes no serviço web a fim de encontrar alguma vulnerabilidade ou um ponto de entrada, para realizar esse processo nós podemos por exemplo explorar o código fonte da página para tentar achar algo, ou usar a ferramenta de network do google para analisar a comunicação entre cliente e servidor, podemos até mesmo fazer esse mesmo processo usando uma proxy como o burp, mas esses não são os únicos método que podemos usar para achar diretórios em um site, os métodos citados anteriormente tem a vantagem de dificilmente serem detectados, porém também possuem a desvantagem de levar muito tempo para se ter resultados, pensando na otimização de tempo e eficiência nós vamos aprender a usar duas ferramentas que automatizam esse processo de procura de diretórios.

Dirb

O dirb é uma ferramenta para detecção de Web content, como já foi abordado anteriormente, essa ferramenta é muito simples de usar, veja só:

```
dirb https://siteteste.com
```

Para usar o dirb nós apenas precisamos escrever seu nome no terminal e então definir o site alvo, com esse comando será feito um scan básico trazendo todos os diretórios encontrados. Caso queira ver outras funcionalidades digite dirb e dê enter para exibir as opções do dirb.

Gobuster

O gobuster também é uma ferramenta simples de ser usada, mesmo precisando de mais alguns caprichos para ser executada, veja o exemplo de um scan simples com o gobuster:

```
gobuster -e -u https://siteteste.com -w /usr/share/wordlists/dirb/common.txt
```

Agora vamos entender:

- A flag -u serve para definir o scan de websites.
- A flag -e serve para mostrar o resultado do scan na tela.
- A flag -w serve para definir uma wordlist.

A diferença básica do gobuster para o dirb é que com o dirb você não possui a necessidade de indicar um wordlist, já com o gobuster isso é necessário, porém o gobuster trás os resultados de uma forma mais dinâmica o que deixa mais fácil de ler.

jcesar_n

JulioCesarNSM

Obrigado!