Aufspüren von Versteckten Verzeichnissen

Gobuster ist ein Tool, das du nutzen kannst, um nach versteckten Verzeichnissen auf einem Webserver zu suchen. Die Idee ist einfach: Finde heraus, welche Verzeichnisse öffentlich zugänglich sind, um potenzielle Schwachstellen zu identifizieren. Gobuster ist besonders praktisch, da es weniger Interaktion erfordert und alles über die Konsole gesteuert werden kann.

Beispielbefehl für Gobuster

```
gobuster dir -u http://10.0.2.17:80/ -w /usr/share/dirbuster/common.txt
```

Wichtig zu wissen ist, dass dieser Befehl keinen rekursiven Scan durchführt; es werden also nur Verzeichnisse auf der höchsten Ebene gesucht.

Dirbuster: Verzeichnissuche mit GUI

Dirbuster ist ähnlich wie Gobuster, bietet jedoch eine grafische Benutzeroberfläche. Du kannst eine vorgefertigte Wordlist wählen, um die Suche zu starten. Dirbuster bringt bereits mehrere Wordlists mit, wie zum Beispiel **common.txt**, die allgemein zu empfehlen ist.

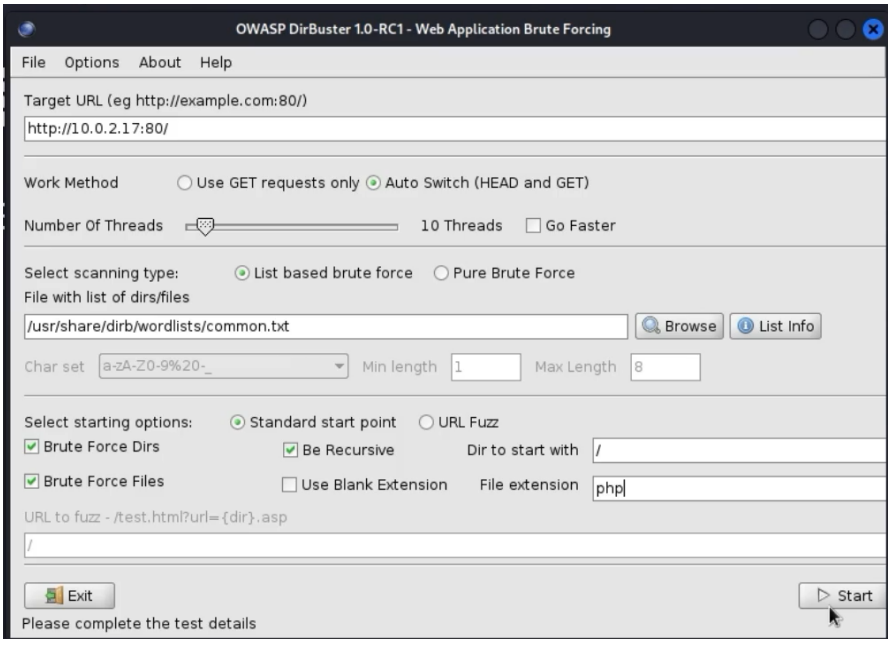

Abbildung 1: Mögliche Konfiguration für Dirbuster

Vorteile von Gobuster gegenüber Dirbuster

Bei Gobuster ist der große Vorteil die Konfigurierbarkeit direkt über den Konsolenbefehl. Du musst also nicht viel klicken, um etwa das Scannen einzelner Unterverzeichnisse zu stoppen.

Entdecken von phpinfo.php Dateien

Wenn du während des Scans eine **phpinfo.php** Datei findest, ist das oft ein Indikator für eine potenzielle Sicherheitslücke. Diese Datei kann verschiedene Informationen preisgeben, wie zum Beispiel die PHP-Version des Servers. Mit dieser Information kannst du dann weiter nach Sicherheitslücken suchen, zum Beispiel mit Frameworks wie **Metasploit**.