

# Introduction

Welcome to the **Attacking Web Applications with Ffuf** module!

There are many tools and methods to utilize for directory and parameter fuzzing/brute-forcing. In this module we will mainly focus on the **ffuf** tool for web fuzzing, as it is one of the most common and reliable tools available for web fuzzing.

The following topics will be discussed:

- Fuzzing for directories
- Fuzzing for files and extensions
- Identifying hidden vhosts
- Fuzzing for PHP parameters
- Fuzzing for parameter values

Tools such as **ffuf** provide us with a handy automated way to fuzz the web application's individual components or a web page. This means, for example, that we use a list that is used to send requests to the webserver if the page with the name from our list exists on the webserver. If we get a response code 200, then we know that this page exists on the webserver, and we can look at it manually.

Next ➔

✔ Mark Complete & Next

 Cheat Sheet


## Table of Contents

### Introduction

Introduction

Web Fuzzing

### Basic Fuzzing

 Directory Fuzzing

 Page Fuzzing

 Recursive Fuzzing

### Domain Fuzzing

DNS Records

 Sub-domain Fuzzing

Vhost Fuzzing

 Filtering Results

### Parameter Fuzzing

 Parameter Fuzzing - GET

Parameter Fuzzing - POST

 Value Fuzzing

### Skills Assessment



My Workstation

OFFLINE

Start Instance

1 / 1 spawns left