# Reconnaissance and Fuzzing with FFUF

Jordan Davis  
Cybersecurity Portfolio Project

## Executive Summary

This document outlines the methodology, tools, and results of a practical reconnaissance and fuzzing assessment conducted using FFUF (Fuzz Faster U Fool). The exercise demonstrates a systematic approach to identifying subdomains, accepted file extensions, accessible pages, and parameter fuzzing, culminating in retrieval of a sensitive flag. The methodology follows real-world practices for offensive web application testing and is representative of industry-grade reconnaissance workflows.

## Objective

To identify subdomains, accepted file extensions, and discover hidden pages and parameters using FFUF. The goal is to demonstrate advanced fuzzing techniques, apply filtering logic, and extract valuable information from web services using open-source tools and publicly available wordlists.

## Tools and Environment

- Tool: FFUF (Fuzz Faster U Fool)  
- Wordlists: SecLists (DNS, extensions, directory names, parameter names, usernames)  
- Platform: Hack The Box Academy (Web Application FFUF Skill Assessment)  
- Environment: Pwnbox (Parrot Linux)

## Methodology and Results

### 1. Subdomain Discovery

Command:  
ffuf -w /opt/useful/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://academy.htb:39069 -H 'Host: FUZZ.academy.htb' -v -c -fs 985

Identified Subdomains:  
- test  
- archive  
- faculty

### 2. Extension Fuzzing

Command:  
ffuf -w /opt/useful/seclists/Discovery/Web-Content/web-extensions.txt:FUZZ -u http://academy.htb:39069/index.FUZZ -v -c

Identified Extensions:  
- academy.htb: .php, .phps  
- test.academy & archive.academy: .php  
- faculty.academy: .php7

### 3. Hidden Page Discovery

Command:  
ffuf -w /opt/useful/seclists/Discovery/Web-Content/directory-list-2.3-small.txt:FUZZ -u http://faculty.academy.htb:39069/courses/FUZZ -v -c -e .php,.php7,.phps -fs 287

Result: http://faculty.academy.htb:39069/courses/linux-security.php7

### 4. Parameter Discovery

Command:  
ffuf -w /opt/useful/seclists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u http://faculty.academy.htb:39069/courses/linux-security.php7?FUZZ=test -X POST -d 'FUZZ=key' -H 'Content-type: application/x-www-form-urlencoded' -fs 774

Discovered Parameters:  
- GET: user  
- POST: username

### 5. Parameter Value Fuzzing

Command:  
ffuf -w /opt/useful/seclists/Usernames/xato-net-10-million-usernames.txt:FUZZ -u http://faculty.academy.htb:48440/courses/linux-security.php7 -X POST -d 'username=FUZZ' -H 'Content-Type: application/x-www-form-urlencoded' -v -c -fs 781

Flag Retrieved With:  
curl http://faculty.academy.htb:48440/courses/linux-security.php7 -X POST -d 'username=harry'

## Conclusion

This assessment reinforced critical skills in subdomain enumeration, extension discovery, page fuzzing, parameter fuzzing, and value testing using FFUF. These skills are foundational in both bug bounty hunting and professional penetration testing workflows. The results show a complete and effective application of automation and filtering in recon tasks, making this a valuable and practical entry in any cybersecurity portfolio.