Cheatography

Fuzzing and Directory Browsing Cheat Sheet

by binca via cheatography.com/44948/cs/13323/

Fuzzing Defined

Sending random or pseudorandom strings via various inputs.

Use attack strings or wodlists.

Critical technique for directory browsing and username harvesting.

Fuzzing Results

Tools can help but you must look for deviations from the norm.

Work from known good based on spidering and forced browsing.

Look for errors and status codes, response size is also helpful.

SecLists

Collection of high quality web app pen test fuzzing sources.

Lists include usernames, passwords, URLs, sensitive data grep strings, fuzzing payloads and more.

ZAP's Fuzzer

Often overlooked in favor of Burp Intruder

ZAP 2.4+ improved with Advanced Fuzzer that is commercial quality.

Information Leakage

This is additional recon data that is not a direct exploit but useful as input in attacks later.
Types:
Valid users
Type of SQL Database
Underlying Directory structure
OS and service version

Directory Browsing

Enables an attacker to "break out" of the web server and surf the underlying file system.

Easy Apache/nginx test is to surf the site's /images directory

Google Searching for Directory Browsing

Google hacks available for discovering information leakage:
site: gov intitle: "index of" "last modified"

Be careful of Google shunning

Note: Search mitre.org for CVEs containing "leakage".

Tools for Directory Browsing

Tools	Wordlists
Nikto	SecLists
W3af	JBroFuzz
ZAP's Forced Browse	DIRB
Metasploit's WMAP and msfcrawler auxiliary module	FuzzDB

Note: WMAP has a wordlist as well, and DirBuster is a wordlist but has been deprecated and incorporated into ZAP.

UserDir Directive

Used by some servers for user-controlled content mapping.

Most common username form is firstinitial lastname.

Disabled by default in Apache, but can be enabled by un-commenting `#include conf/extra/httpd-userdir.conf` or by including the proper directives in a directory block within the main configuration file.

By **binca**
cheatography.com/binca/

Not published yet.
Last updated 9th November, 2017.