Web Pentest Cheat Sheet

by luvbutrfly via cheatography.com/122732/cs/22928/

Parameter Tampering

Hack The Form - Firefox Addon

Reconnaissance

COMMAND	ACTION
recon-ng	recon scan
nmap -sT <IP>	network TCP scan
nmap -sV <IP>	network service/version scan
zenmap	GUI scan
Wafw00f	scan for wafs
OSINT	research online
WHOIS	DNS info
Google Dorking	Google OSINT
Shodan	search engine scans web
NSE	Nmap scripting engine
Nessus	Vulnerability scanner

BeEF (Browser Exploitation Framework)

Decode Cookies

Cyberchef	https://gchq.github.io/CyberChef/

Path/Directory Traversal

URL Manipulation	insert after page= portion of URL
URL addition	../../../../../../../../-etc/passwd

Exploits

Metasploit

netcat

Enumeration

sqlmap

Metasploitable Framework

XSS Stored

Enter to message field	<script>alert(document.cookie);</script>

*vuln from unsanitized input

SQL Injection

sqlmap	command line autodetect sql inj. vulns

Broken Authentication

Validation Bypass

By **luvbutrfly**
cheatography.com/luvbutrfly/

Not published yet.
Last updated 16th October, 2020.

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com