Web Tools For CTF (Capture The Flag)

BURPSUITE

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.

RACCOON

Raccoon is a tool made for reconnaissance and information gathering with an emphasis on simplicity. It will do everything from fetching DNS records, retrieving WHOIS information, obtaining TLS data, detecting WAF presence and up to threaded dir busting and subdomain enumeration.

POSTMAN

Postman is a software development tool. It enables people to test calls to APIs. Postman users enter data. The data is sent to a special web server address. Typically, information is returned, which Postman presents to the user.

SQLMAP

SQL Injection is a code injection technique where an attacker executes malicious SQL queries that control a web application's database.

W3AF

w3af (Web Application Attack and Audit Framework) is an open-source web application security scanner. The project provides a vulnerability scanner and exploitation tool for Web applications. It provides information about security vulnerabilities for use in penetration testing engagements.

Ciphey

Automatically decrypt encryptions without knowing the key or cipher, decode encodings, and crack hashes

Stego Toolkit

This project is a Docker image useful for solving Steganography challenges as those you can find at CTF platforms like hackthebox.eu.

Ismail Ahmed