



Burp Suite

from First Run to Website Hack in 60 min



About

- Application Security Engineer
- Bug Bounty Hunter
- Web, Mobile, Network pentests
- eWPT, eCPPT, CEH, CCNA, OSCP(in progress)
- Cyberpolice Teacher



What you need

- I. Laptop (Any OS)
- II. Burp Suite: <https://portswigger.net/burp>
- III. Larry_Lau :) <https://t.me/burpsuite>
- IV. Lab: <http://173.212.213.238:8{1-9}>
- V. Challenge <http://173.212.213.238:89/> HackIT tickets
- VI. GitHub <https://github.com/0Ntg0/0wasp-Kyiv>

**HACKEN
PROOF**

What can it do?

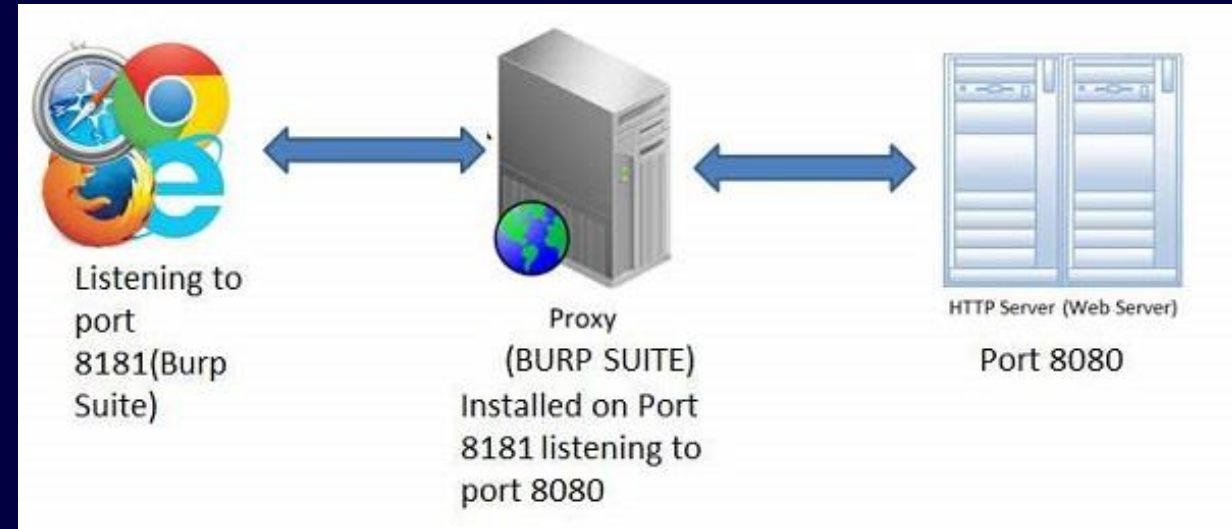


I. Everything

II. Modules

III. Public Extensions

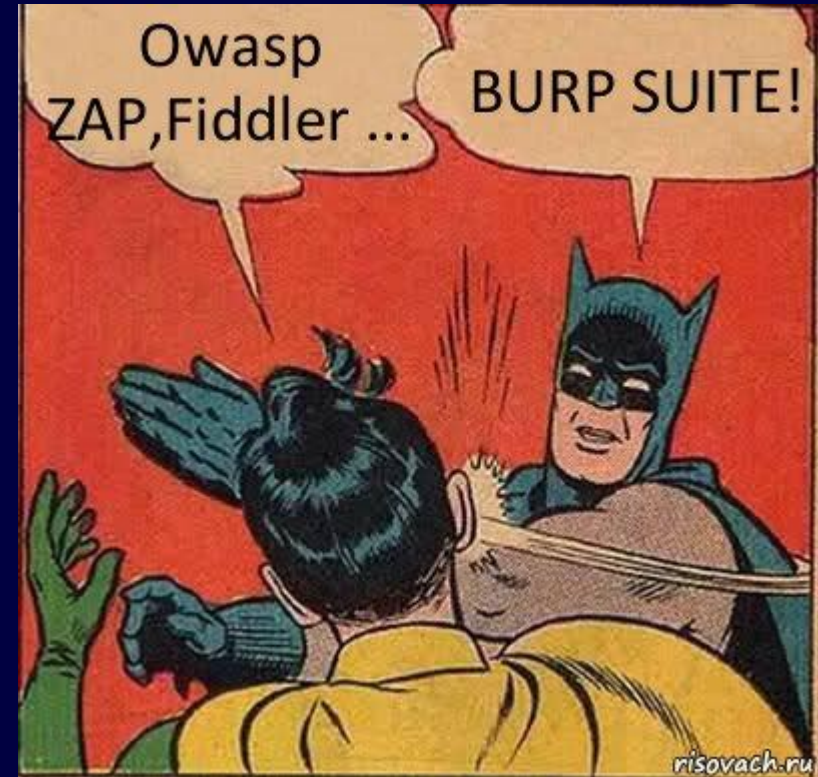
IV. Write your functionality!



HACKEN
PROOF

Why Burp Suite?

- OWASP ZAP
- Postman
- WebScarab
- Fiddler
- Poster
- Charles proxy



HACKEN
PROOF

Burp Suite Editions



Community – FREE	Professional – 400\$	Enterprise – 4,000\$
Web scanner	Web scanner	Web scanner
Scheduled and repeat scans	Scheduled and repeat scans	Scheduled and repeat scans
Unlimited scalability	Unlimited scalability	Unlimited scalability
CI integration	CI integration	CI integration
Advanced manual tools	Advanced manual tools	Advanced manual tools
Essential manual tools	Essential manual tools	Essential manual tools

HACKEN
PROOF

How to start



- I. Run FF
- II. Run Burp Suite: `java -jar burpsuite.jar`
- III. Set up proxy in FF
- IV. Set up CA Certificate

n00b: Intercept off -> Spider -> Scanner -> Analyze for FP -> Report

r00t: Scope, Spider, Proxy, Repeater, Intruder, Extensions, Macros



Burp Suite Modules



- Target

- Proxy



- Scanner

- Repeater



- Intruder



- Sequencer

- Decoder



- Extender

- Comparer



- Collaborator

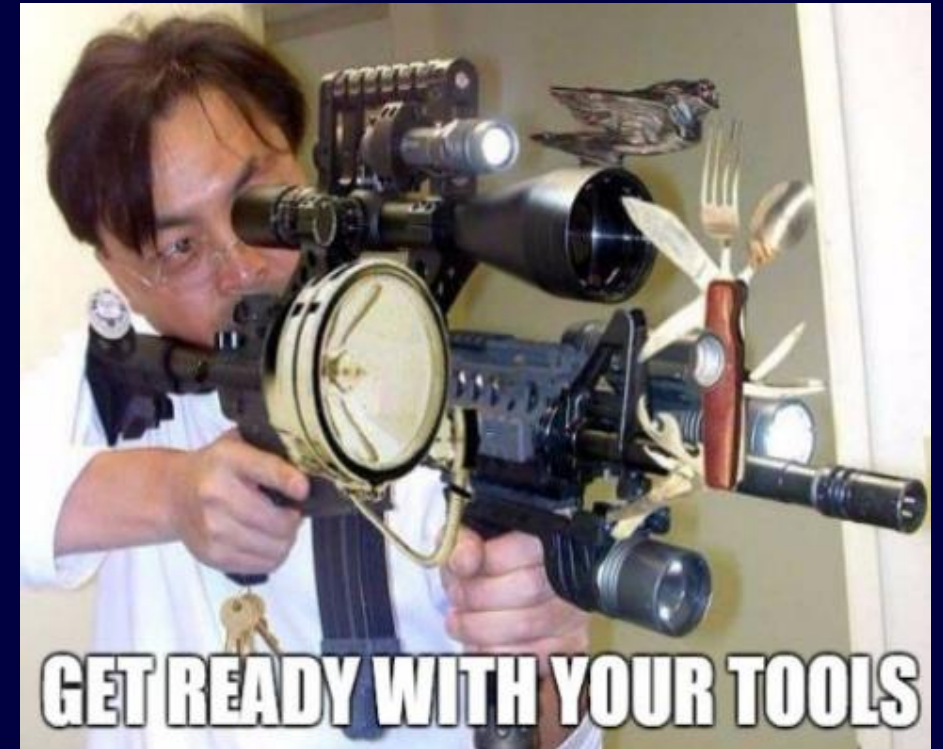
B⁶⁴

HACKEN
PROOF

Top Extensions

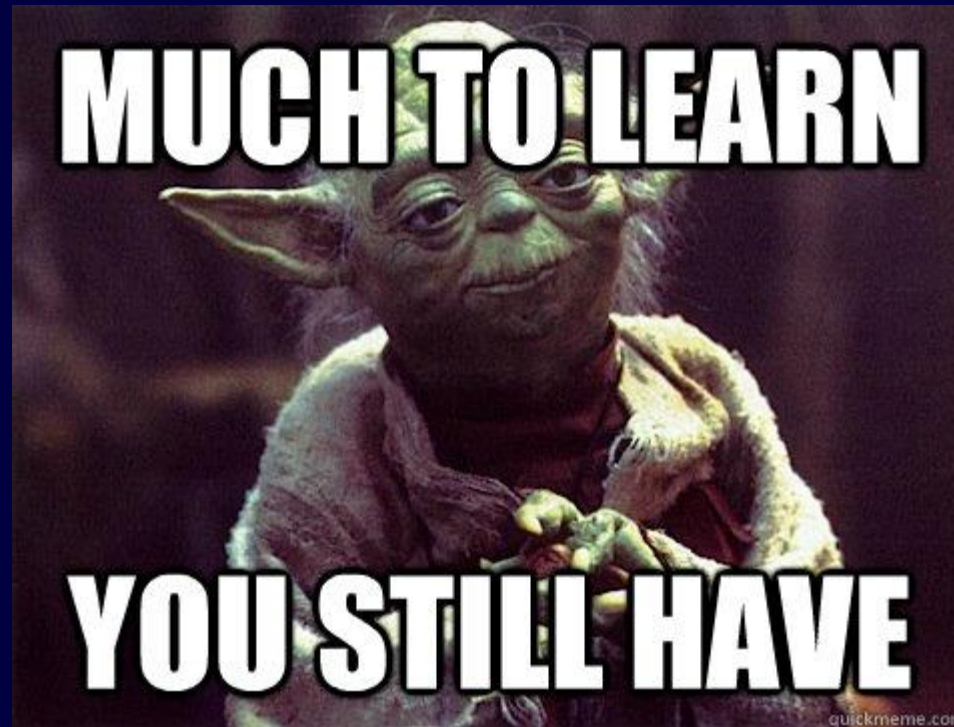


- Reflector
- C02
- Sentinel
- Random IP Address Header
- Json Beautifier
- XSS Validator
- Vulners Scanner
- ActiveScan++
- AuthMatrix



HACKEN
PROOF

Let's start practice!



HACKEN
PROOF

Contacts

Eduard Babych

- @j0ns1k
- [linkedin.com/in/eduard-babych/](https://www.linkedin.com/in/eduard-babych/)
- e.babych@hacken.io



HACKEN
PROOF