burp suite community edition
Go straight to download
x64 - download

FoxyProxy chrome extension
Add extension.

next → ... → finish
license key

Extension → options → proxies → add
Add proxy Add

Title proxy Hostname 127.0.0.1
Port 8083

→ Save

check if added

---

testphp.vulnweb.com

Burp

Proxy - Proxy Settings
Add bind to port : 8083
All interface
Ok

---

testphp.vulnweb.com
guestbook

test

Burp proxy → on
Intercept → on.
→ Add message

Burp
≡
↳ send to repeater.

Repeater
↳ Request
anonymous: replace → test
2nd replace → <script>alert(1)</script>

Send.

Response
right click
→ show response in browser

copy url
browser → paste url
→ alert message ↳ XSS

Turn off proxy

Signup
- username
- password

Proxy on.
intercept on
Login

Request ≡
send to intruder

Intruder

user select → add §

pass select → add §

? [sniper] attack → change cluster bomb attack

Payloads

[1]

→ add 4 data

one real and 3 dummy

[2]

→ add 4 data

one real and 3 dummy

Start attack

correct → status code 200.

others → 302