# Burp Suite Quick Reference

## Basic Setup

```bash
# Start Burp Suite
burpsuite

# Project setup: Temporary project → Use Burp defaults → Start Burp
```

## Core Interface

- **Proxy > Intercept** - Traffic capture on/off
- **Proxy > HTTP History** - All captured requests
- **Repeater** - Modify and resend requests
- **Intruder** - Automated attacks
- **Decoder** - Encode/decode data

## Firefox & FoxyProxy Setup

```
1. Install FoxyProxy extension
2. Add proxy: HTTP, 127.0.0.1, Port 8080
3. about:config → network.proxy.allow_hijacking_localhost = true
4. Import Burp certificate: http://burp → Download CA cert → Firefox certificates
```

## Essential Workflows

### Capture & Modify

1. Browse with **Intercept OFF**
2. Find request in **HTTP History**
3. Right-click → **Send to Repeater**
4. Modify parameters → **Send**

### Intruder Brute Force

1. Send request to **Intruder**
2. **Positions:** Clear → Select field → Add
3. **Payloads:** Add wordlist
4. **Start Attack** → Look for different response lengths

### Compare Responses

1. Select two responses in **HTTP History**
2. Right-click → **Send to Comparer (responses)**
3. **Words/Bytes** comparison → Look for differences

## Quick Troubleshooting

- **Browser hangs:** Check if Intercept is ON
- **No traffic:** Use built-in browser or verify FoxyProxy settings
- **HTTPS errors:** Import Burp CA certificate
- **Session expired:** Re-login and capture fresh request