Burp Suite Quick Start Guide

Getting Started

Initial Setup

```bash
# Launch Burp Suite (usually pre-installed on Kali)
burpsuite

# Or install if needed:
sudo apt update && sudo apt install burpsuite
```

Project Setup

1. Choose **Temporary project** (Community Edition)
2. Click **Next**
3. Select **Use Burp defaults**
4. Click **Start Burp**

Launch Built-in Browser

1. Go to **Proxy > Intercept**
2. Click **Open Browser**
3. Use this browser for all testing (avoids proxy setup issues)

Core Interface Overview

Essential Tabs You'll Use Most

- **Proxy > Intercept** - Turn traffic capture on/off
- **Proxy > HTTP History** - See all captured requests/responses
- **Repeater** - Modify and resend individual requests
- **Decoder** - Encode/decode data (Base64, URL, etc.)
- **Extensions** - Install additional tools

Traffic Flow Control

Intercept ON: Traffic stops at Burp, must click "Forward" **Intercept OFF:** Traffic flows normally, gets logged in HTTP History

Tip: Keep Intercept OFF most of the time, only turn ON when you need to modify requests live

Using Core Tools

Proxy - Capturing Traffic

1. Ensure Intercept is OFF for normal browsing
2. Navigate to target application in Burp browser
3. All traffic appears in **Proxy > HTTP History**
4. Right-click any request → **Send to Repeater** for modification

Repeater - Modifying Requests

1. Select request in HTTP History
2. Right-click → **Send to Repeater**
3. In Repeater tab: modify parameters, headers, or body
4. Click **Send** to see modified response
5. Compare original vs modified in side-by-side view

Decoder - Handling Encoded Data

Decoding:

1. Paste encoded string in top box
2. Click appropriate decode button (Base64, URL, etc.)
3. Decoded result appears below

Encoding:

1. Enter plain text
2. Click encode button for desired format
3. Use encoded result in requests

Common Request Analysis

Reading HTTP Requests

```
POST /login.php HTTP/1.1        ← Method and endpoint
Host: target.com                ← Target server
Content-Type: application/x-www-form-urlencoded

username=admin&password=test123  ← POST body data
```

Reading HTTP Responses

```
HTTP/1.1 200 OK                 ← Status code
Server: Apache/2.4.41           ← Server info
Content-Type: text/html

<html>...</html>                ← Response body
```

Key Things to Look For

- **POST data** - Form submissions, login attempts
- **GET parameters** - URL-based data (?id=123&user=admin)
- **Cookies** - Session tokens, authentication data
- **Status codes** - 200 (OK), 403 (Forbidden), 500 (Error)

Essential Extensions

Installing Extensions

1. Go to **Extensions** tab
2. Click **BApp Store**
3. Search and install:

Must-Have Extensions:

- **Logger++** - Enhanced traffic logging
- **Autorize** - Authorization testing
- **ActiveScan++** - Enhanced vulnerability scanning

Quick Troubleshooting

Browser Won't Load Pages

- Check if **Intercept is ON** → Turn it OFF
- Ensure you're using the **built-in Burp browser**
- Verify Burp Suite is still running

No Traffic Appearing in History

- Make sure you're using **Burp's built-in browser**
- Check that you navigated to HTTP sites (not just HTTPS with cert issues)
- Try refreshing the target page

Session Expired / Logged Out

- Simply log back into the application
- Capture a fresh authenticated request
- Continue testing with new session

Testing Workflow

Basic Vulnerability Testing Process

1. **Browse normally** with Intercept OFF
2. **Find interesting requests** in HTTP History
3. **Send to Repeater** for modification
4. **Modify parameters** (IDs, prices, user data)
5. **Analyze responses** for unexpected behavior
6. **Document findings** when something breaks

What to Test First

- **Change ID numbers** in URLs (?id=1 → ?id=2)
- **Modify hidden form fields** (prices, user levels)
- **Test different user contexts** (admin vs regular user)
- **Try extreme values** (negative numbers, very large values)

Pro Tips

- **Always test systematically** - don't just try random things
- **Save interesting requests** by starring them in HTTP History
- **Use search/filter** in HTTP History to find specific requests
- **Compare responses** side-by-side in Repeater
- **Document everything** - what you tested and what happened

---

This guide covers Burp Suite Community Edition basics. Keep this handy during all web application testing sessions.