1. Set Burp Up To Work (one-time tasks)

- User Options ... Display ... Metal (must restart Burp)
- Project Options ... Misc ... Burp Collaborator Server (if you have one)
- Extender ... Python Environment ... Location of Jython standalone JAR
- http://burp ... download certificate ... install it ... trust it to "identify websites"
-- also available via Proxy >> Options >> Import/Export CA certificate
-- "import" to overcome certificate pinning, for example, where possible

2. Set up Burp To Work (every new test)

- Proxy ... Intercept ... "intercept is off"
- Dashboard ... "Task execution is paused" (click "resume")

2a. General Advice:

- Right Click on Everything
- https://bitbucket.org/mrbbking/quieter-firefox
- Use Browser Profiles for different privilege levels at the same time

3. Proxy

- Intercept is on vs off
-- Selective Interception by rules
- Comment and highlight on the fly
-- Extension:
- Multiple listners, multiple browser profiles, easier privesc testing
-- View filters
- SSL Stripping attack setup
- Proxy History is Where It's at
- WebSockets history and Repeater
- Match and Replace
- TLS passthrough
- Misc >> Don't sent items...

4. Target

- Use "Advanced Scope Control" because ... what's the other one for, again?
-- Do Not Accept the "don't send to proxy history" thing
-- Look at Flickr.com or wikipedia.org for some whys
-- Use Filters Instead
- Gray items: seen, not sent.
-- Burp and "seeing"
- Right click "Engagement Tools"
-- Search (to find rq/rs)
-- Find Comments
-- Find Scripts
-- Find References
-- Analyze Targetn
-- Schedule Task
-- Discover Content (but, and)
-- Compare Site Maps (at different priv levels)
--- Good Burp Training: https://www.lanmaster53.com/training/
-- Copy URLs / Copy Links

5. Repeater

- Send to Repeater, then send from Repeater, then modify
- Arrangement of panes for screenshots
- Rename tabs by clicking on them.
- fwd and back buttons
- Support for Web Sockets now

6. Intruder

- Clear selectively

- Scan Defined Insertion Points
- Payloads
-- Null Payloads (session keepalive)
- Payload Processing
-- prefix, suffix, encode, match/Replace. Hash
- Grep Match (retrospectively, even)
- Grep Extract
- Follow Redirections (pw sprays)

7. Decoder

- Base64 and binary output
- Use CyberChef

8. Comparer

- words is faster.
- number of differences in title bar

9. Project Options

- SOCKS Proxy
- "hosts" file!
- Drop out of scope requests

- Sessions
-- Cookies from the cookie jar and Repeater and Intruder
-- Macros (for another time ... this is "getting started")

10. Extender

- About Extender and the Java API
- "Install" Jython
- Finding Good Extensions:
-- There's like 250 of them in the BApp Store and no search
-- https://github.com/snoopysecurity/awesome-burp-extensions
-- Author   James 'albinowax' Kettle, PortSwigger Web Security
-- Sort by stars
-- Sort by popularity
-- Look for passive/active
-- Understand The World Has Limits And So Does Your JVM

- Some Good Ones from the BHIS Testers:

Retire.js
Turbo Intruder
Python Scripter
UploadScanner
Param Miner
Logger++

Passive
    Additional Scanner Checks
    Detect Dynamic JS
    Collaborator Everywhere
    CSP Auditor
    CSP-Bypass
    Error Message Checks (*)
    Headers Analyzer (*)
    Retire.js (*)
    Same Origin Method Execution

Active Integration (i.e. no extra effort beyond active scanning)
    Active Scan++
    Backslash Powered Scanner
    CSRF Scanner

```
    Conditional extensions based on technologies in use
    PHP Object Injection Check
    J2EEScan
    Java Deserialization Scanner

Other
    AuthMatrix - Great for testing permissions and privilege escalation.
    Autorize
    JSON Beautifier (*)
    Request Minifier - Reduces required parameters by repeatedly trying requests.
    Session Timeout Test - Finds the amount of time it takes for a session to timeout by
… using incremental backoff.
```