# BurpSuite Cheat Sheet

Introduction to the Cheat Sheet

&

Burp feature overview

# Cheat Sheet Developed By

Chris Dale @chrisadale

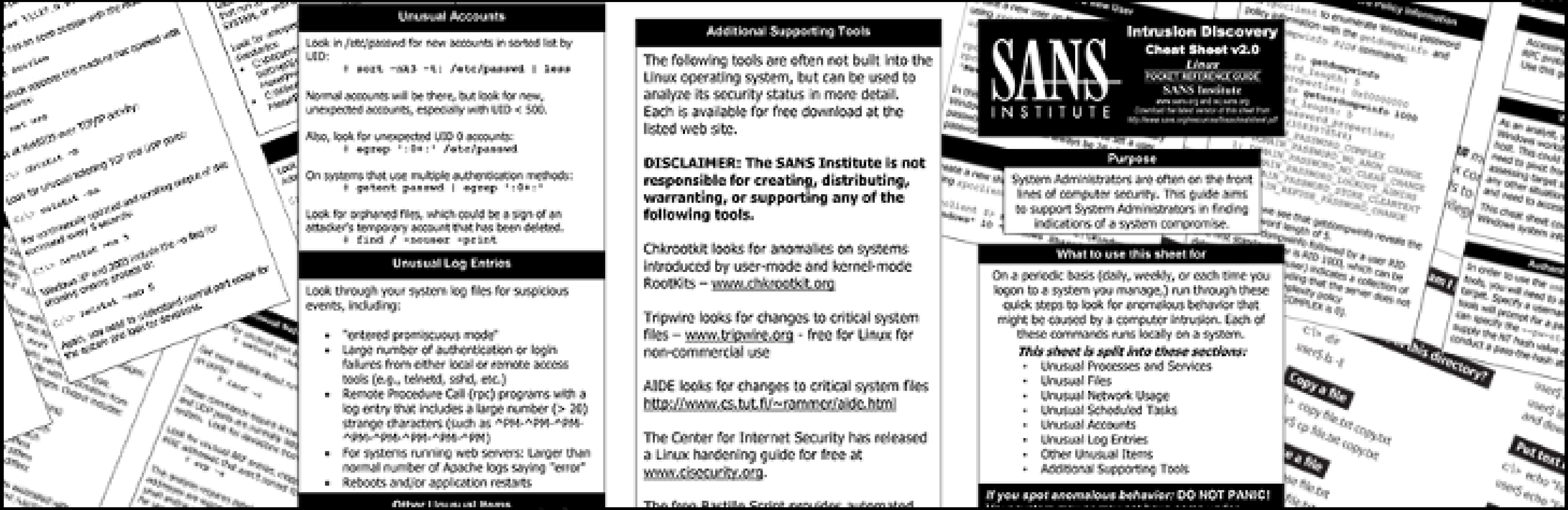
Principal Consultant River Security

Certified SANS Instructor

- Thanks to reviewers:
  - Moses Frost - @mosesrenegade
  - Bojan Zdrnja - @bojanz
  - Hassan El Hadary - @hassan_hadary
  - Randall Jones for making this happen!

# BurpSuite Free vs Pro

- Paid version has more features, primarily aimed towards penetration testers.
- Vulnerability Scanner which benefits from extensions
- Non-throttled Intruder for fuzzing scripts
- Project and session support
- Handy features such as:
  - Finding script references, scripts and comments
  - Content discovery
  - Reports on attack surface



## Unusual Accounts

Look in /etc/passwd for new accounts in sorted list by UID:

```
        # sort –nk3 –t: /etc/passwd | less
```

Normal accounts will be there, but look for new, unexpected accounts, especially with UID < 500.

Also, look for unexpected UID 0 accounts:

```
        # egrep ':0+:' /etc/passwd
```

On systems that use multiple authentication methods:

```
        # getent passwd | egrep ':0+:'
```

Look for orphaned files, which could be a sign of an attacker's temporary account that has been deleted.

```
        # find / -nouser -print
```

## Unusual Log Entries

Look through your system log files for suspicious events, including:

- "entered promiscuous mode"
- Large number of authentication or login failures from either local or remote access tools (e.g., telnetd, sshd, etc.)
- Remote Procedure Call (rpc) programs with a log entry that includes a large number (> 20) strange characters (such as ^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM)
- For systems running web servers: Larger than normal number of Apache logs saying "error"
- Reboots and/or application restarts

## Other Unusual Items

## Additional Supporting Tools

The following tools are often not built into the Linux operating system, but can be used to analyze its security status in more detail. Each is available for free download at the listed web site.

**DISCLAIMER: The SANS Institute is not responsible for creating, distributing, warranting, or supporting any of the following tools.**

Chkrootkit looks for anomalies on systems introduced by user-mode and kernel-mode RootKits – www.chkrootkit.org

Tripwire looks for changes to critical system files – www.tripwire.org - free for Linux for non-commercial use

AIDE looks for changes to critical system files http://www.cs.tut.fi/~rammer/aide.html

The Center for Internet Security has released a Linux hardening guide for free at www.cisecurity.org.

The free Bastille Script provides automated

SANS INSTITUTE

**Intrusion Discovery**

**Cheat Sheet v2.0**

*Linux*

POCKET REFERENCE GUIDE

SANS Institute

www.sans.org and isc.sans.org

Download the latest version of this sheet from

http://www.sans.org/resources/linsacheatsheet.pdf

## Purpose

System Administrators are often on the front lines of computer security. This guide aims to support System Administrators in finding indications of a system compromise.

## What to use this sheet for

On a periodic basis (daily, weekly, or each time you logon to a system you manage,) run through these quick steps to look for anomalous behavior that might be caused by a computer intrusion. Each of these commands runs locally on a system.

***This sheet is split into these sections:***

- Unusual Processes and Services
- Unusual Files
- Unusual Network Usage
- Unusual Scheduled Tasks
- Unusual Accounts
- Unusual Log Entries
- Other Unusual Items
- Additional Supporting Tools

***If you spot anomalous behavior:* DO NOT PANIC!**

# Cheat Sheet in Two Pages

## Navigational Hotkeys

```
Ctrl-Shift-T - Target Tab
Ctrl-Shift-P - Proxy Tab
Ctrl-Shift-R - Repeater Tab
Ctrl-Shift-I - Intruder Tab
Ctrl-Shift-O - Project Options Tab
Ctrl-Shift-D - Dashboard Tab
Ctrl-Equal - next tab
Ctrl-Minus - previous tab
```

## Editor Encoding / Decoding Hotkeys

```
Ctrl-B - Base64 selection
Ctrl-Shift-B - Base64 decode selection
Ctrl-H - Replace with HTML Entities
(key characters only)

Ctrl-Shift-H - Replace HTML entities
with characters

Ctrl-U - URL encode selection (key
characters only)
Ctrl-Shift-U - URL decode selection
```

## Burp Collaborator

The collaborator enables the penetration tester to listen for call-backs from vulnerable scripts and services via auto-generation of unique DNS names and works on the following protocols:

- DNS
- HTTP & HTTPS
- SMTP & SMTPS

Use the Burp extension Taborator to make Burp Collaborator easier to use on-the-fly.

## Global Hotkeys

```
Ctrl-I - Send to Intruder
Ctrl-R - Send to Repeater

Ctrl-S - Search (places cursor in
search field)
Ctrl-. - Go to next selection
Ctrl-m - Go to previous selection

Ctrl-A - Select all
Ctrl-Z - Undo
Ctrl-Y - Redo
```

## Editors Hotkeys

```
Ctrl-Delete - Delete Word
Ctrl-D - Delete Line
Ctrl-Backspace - Delete Word Backwards

Ctrl-Home - Go to beginning of document
Ctrl-Shift-Home - Go to beginning of
document and select data on its way
Ctrl-End - Go to end of document
Ctrl-Shift-End - Go to end of document
and select data on its way
Ctrl-Left - Go to Previous Word
Ctrl-Shift-Left - Go to Previous Word
and select data on its way
Ctrl-Right - Go to Next Word
Ctrl-Shift-Right - Go to Next Word and
select data on its way
```

## Tool Specific Hotkeys

```
Ctrl-F - Forward Request (Proxy)
Ctrl-T - Toggle Proxy Intercept On and
Off
Ctrl-Space - Send Request (Repeater)

Double-click <TAB> - Rename a tab
```

OFFENSIVE OPERATIONS

# Burp Suite Cheat Sheet v1.0

**By Chris Dale @chrisadale**

SANS

sans.org/offensive-operations

## Purpose

This cheat sheet enables users of Burp Suite with quicker operations and more ease of use. Burp Suite is the de-facto penetration testing tool for assessing web applications. It enables penetration testers to rapidly test applications via signature features like repeater, intruder, sequencer, and extender.

It is split into two pages, one page containing common shortcuts to use within the application, the second page containing useful extensions and tips-and-tricks. It is recommended to manually check and test the different extensions available in the product; many which may be very useful to your testing, but outside of what this cheat sheet can cover.

Burp Suite comes in a free community edition and a commercial professional edition. It has a built in Chromium browser for easy set-up of HTTP and SSL/TLS interception.

***POCKET REFERENCE GUIDE***

## Hunting for Vulnerabilities 1/2

Users can contribute with extensions to aid in the discovery of vulnerabilities. Be aware of false-positives and use your pentesting capabilities to ensure you fully explore the findings.

**Param Miner**
Allows high-performance identifying of unlinked parameters. Check for unlinked GET and Headers, and unlinked POST when applicable.

**Backslash Powered Scanner**
Will give alerts on interesting transformations of data or other interesting things. Often, it will be false-positives, but it allows the penetration tester to focus on potential vulnerabilities.

**Software Vulnerability scanner**
Checks software version numbers against vulnhub.com for vulnerabilities.

## Authorization and Authentication

**SAML-Raider**
Useful to inspect SAML messages, edit and re-sign them.

**JSON Web Tokens**
Lets you decode and manipulate JSON web tokens on the fly, check their validity and automate common attacks.

**Autorize**
Detect if scripts are accessible via different roles or unauthenticated in the web-application.

## Hunting for Vulnerabilities 2/2

**HTTP Request Smuggler**
This is an extension for Burp Suite designed to help you launch HTTP Request Smuggling attacks.

**Active scan++**
Allows us to find more vulnerabilities in terms of suspicious input transformation, XML input handling, host header attacks and more.

**Retire.js**
Finds outdated JavaScript and links to the relevant CVE's for your investigations.

## Utilities

These extensions are helpful utilities to a variety of different situations and help bring the penetration tester to their full potential.

**Logger++**
Use this plugin to log and monitor your attacks from e.g., scanner and more. Sort by status-code and do an extra inspection on server 500 errors. When you have done inspections, clear the logs.

**Turbo Intruder**
Python scriptable interface where one can achieve custom functionality and very high speeds of HTTP requests through http pipelining.

**Taborator**
Quickly add and monitor Burp collaborator interactions.

## Rest API

The REST API can be enabled in user options. It will by default be enabled on http://127.0.0.1:1337/. It supports interaction via web-application too, not just CLI. Below is a list of endpoints via their URL and the respective cURL command to use them.

The API can be especially useful when you need to send a consolidated list of URLs from a different tool to the scan engine, or perhaps use Burp Suite in headless mode.

To open Burp Suite in headless mode run it with the following arguments:

```
java -jar -Xmx4g -Djava.awt.headless=true /path/to/burp.jar
```

Get a list of defined issues:

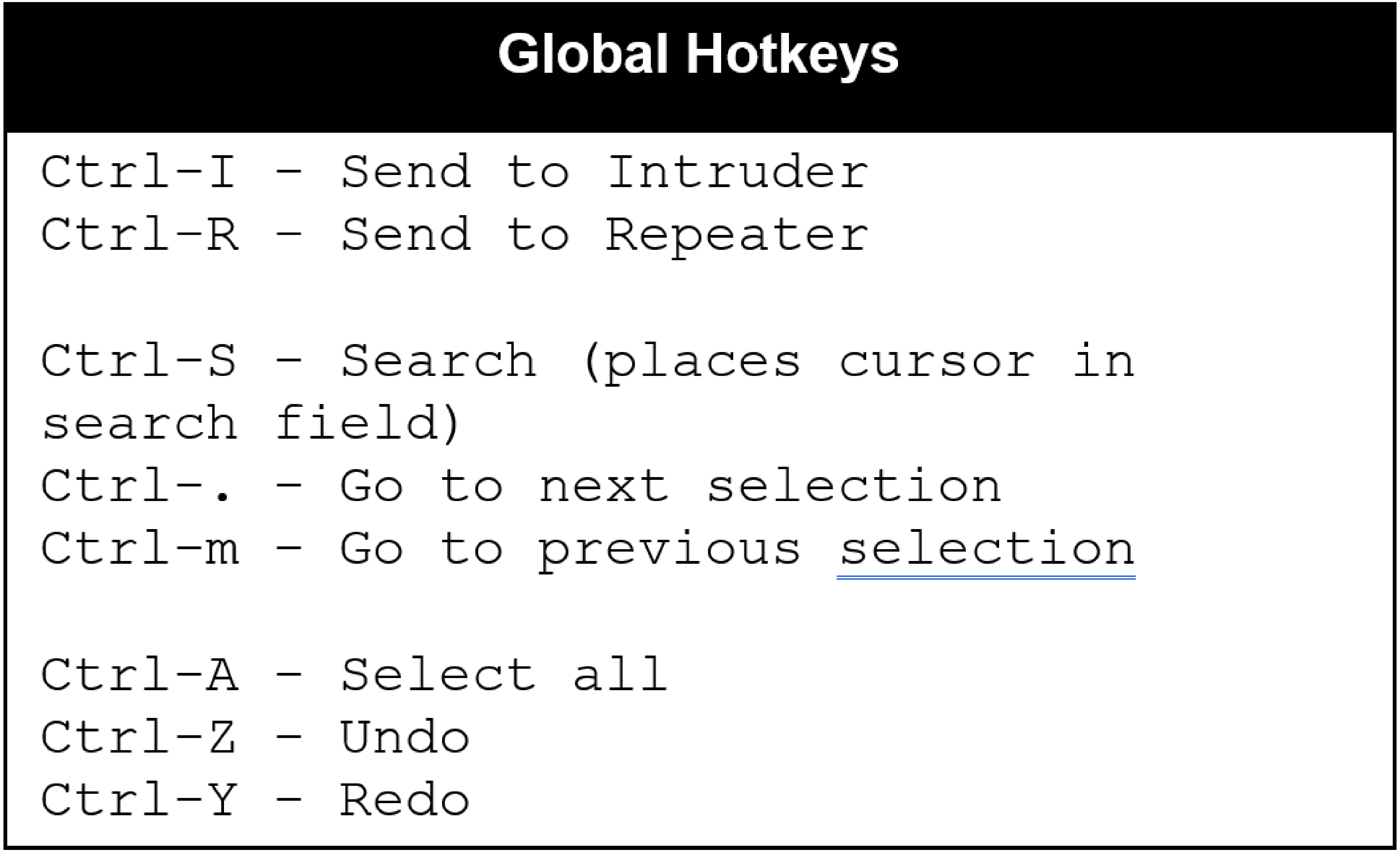
```
http://localhost:1337/knowledge_base/issue_definitions
curl -vgw "\n" -X GET 'http://127.0.0.1:1337/v0.1/knowledge_base/issue_definitions'
```

Scan a URL with the Active Scanner (vulnerability scanner):

```
http://localhost:1337/scan
curl -vgw "\n" -X POST 'http://127.0.0.1:1337/v0.1/scan' -d '{"urls":["http://target.tgt/scanTarget1","http://target.tgt/scanTarget2"]}'
```

Check the status and progress of a given scan:

```
http://localhost:1337/scan/task_id
curl -vgw "\n" -X GET 'http://127.0.0.1:1337/v0.1/scan/mytask_identifier'
```



## Global Hotkeys

Ctrl-I - Send to Intruder
Ctrl-R - Send to Repeater

Ctrl-S - Search (places cursor in search field)
Ctrl-. - Go to next selection
Ctrl-m - Go to previous selection

Ctrl-A - Select all
Ctrl-Z - Undo
Ctrl-Y - Redo

# Navigational Hotkeys

Ctrl-Shift-T - Target Tab

Ctrl-Shift-P - Proxy Tab

Ctrl-Shift-R - Repeater Tab

Ctrl-Shift-I - Intruder Tab

Ctrl-Shift-O - Project Options Tab

Ctrl-Shift-D - Dashboard Tab

Ctrl-Equal - next tab

Ctrl-Minus - previous tab

# Editor Encoding / Decoding Hotkeys

Ctrl-B - Base64 selection
Ctrl-Shift-B - Base64 decode selection
Ctrl-H - Replace with HTML Entities (key characters only)

Ctrl-Shift-H - Replace HTML entities with characters

Ctrl-U - URL encode selection (key characters only)
Ctrl-Shift-U - URL decode selection

## Tool Specific Hotkeys

Ctrl-F - Forward Request (Proxy)
Ctrl-T - Toggle Proxy Intercept On and Off
Ctrl-Space - Send Request (Repeater)

Double-click <TAB> - Rename a tab

# Burp Collaborator

The collaborator enables the penetration tester to listen for call-backs from vulnerable scripts and services via auto-generation of unique DNS names and works on the following protocols:

- DNS
- HTTP & HTTPS
- SMTP & SMTPS

Use the Burp extension Taborator to make Burp Collaborator easier to use on-the-fly.

# Hunting for Vulnerabilities 1/2

Users can contribute with extensions which aids in the discovery of vulnerabilities. Be aware of false-positives and use your pentesting capabilities to ensure you fully explore the findings.

**Param Miner**
Allows high-performance identifying of unlinked parameters. Check for unlinked GET and Headers, and unlinked POST when applicable.

**Backslash Powered Scanner**
Will give alerts on interesting transformations of data or other interesting things. Often, it will be false-positives, but it allows the penetration tester to focus on potential vulnerabilities.

**Software Vulnerability scanner**
Checks software version numbers against vulners.com for vulnerabilities.

## Hunting for Vulnerabilities 2/2

**HTTP Request Smuggler**
This is an extension for Burp Suite designed to help you launch HTTP Request Smuggling attacks.

**Active scan++**
Allows us to find more vulnerabilities in terms of suspicious input transformation, XML input handling, host header attacks and more.

**Retire.js**
Finds outdated JavaScript and links to the relevant CVE's for your investigations.

## Authorization and Authentication

**SAML-Raider**
Useful to inspect SAML messages, edit and re-sign them.

**JSON Web Tokens**
Lets you decode and manipulate JSON web tokens on the fly, check their validity and automate common attacks.

**Autorize**
Detect if scripts are accessible via different roles or unauthenticated in the web-application.

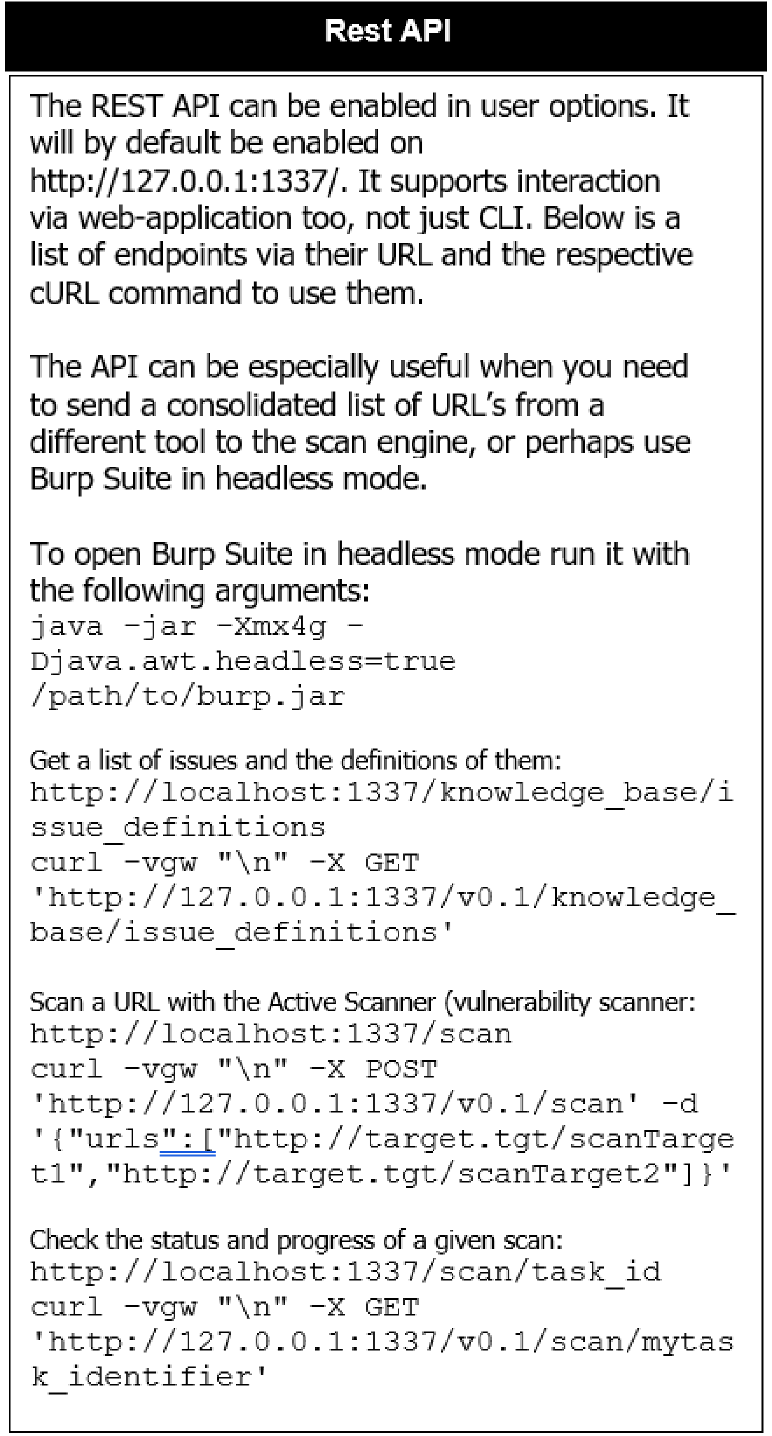
# Utilities

These extensions are helpful utilities to a variety of different situations and help bring the penetration tester to their full potential.

**Logger++**
Use this plugin to log and monitor your attacks from e.g., scanner and more. Sort by status-code and do an extra inspection on server 500 errors. When you have done inspections, clear the logs.

**Turbo Intruder**
Python scriptable interface where one can achieve custom functionality and very high speeds of HTTP requests through http pipelining.

**Taborator**
Quickly add and monitor Burp collaborator interactions.



## Rest API

The REST API can be enabled in user options. It will by default be enabled on http://127.0.0.1:1337/. It supports interaction via web-application too, not just CLI. Below is a list of endpoints via their URL and the respective cURL command to use them.

The API can be especially useful when you need to send a consolidated list of URL's from a different tool to the scan engine, or perhaps use Burp Suite in headless mode.

To open Burp Suite in headless mode run it with the following arguments:

```
java -jar -Xmx4g -
Djava.awt.headless=true
/path/to/burp.jar
```

Get a list of issues and the definitions of them:

```
http://localhost:1337/knowledge_base/i
ssue_definitions
curl -vgw "\n" -X GET
'http://127.0.0.1:1337/v0.1/knowledge_
base/issue_definitions'
```

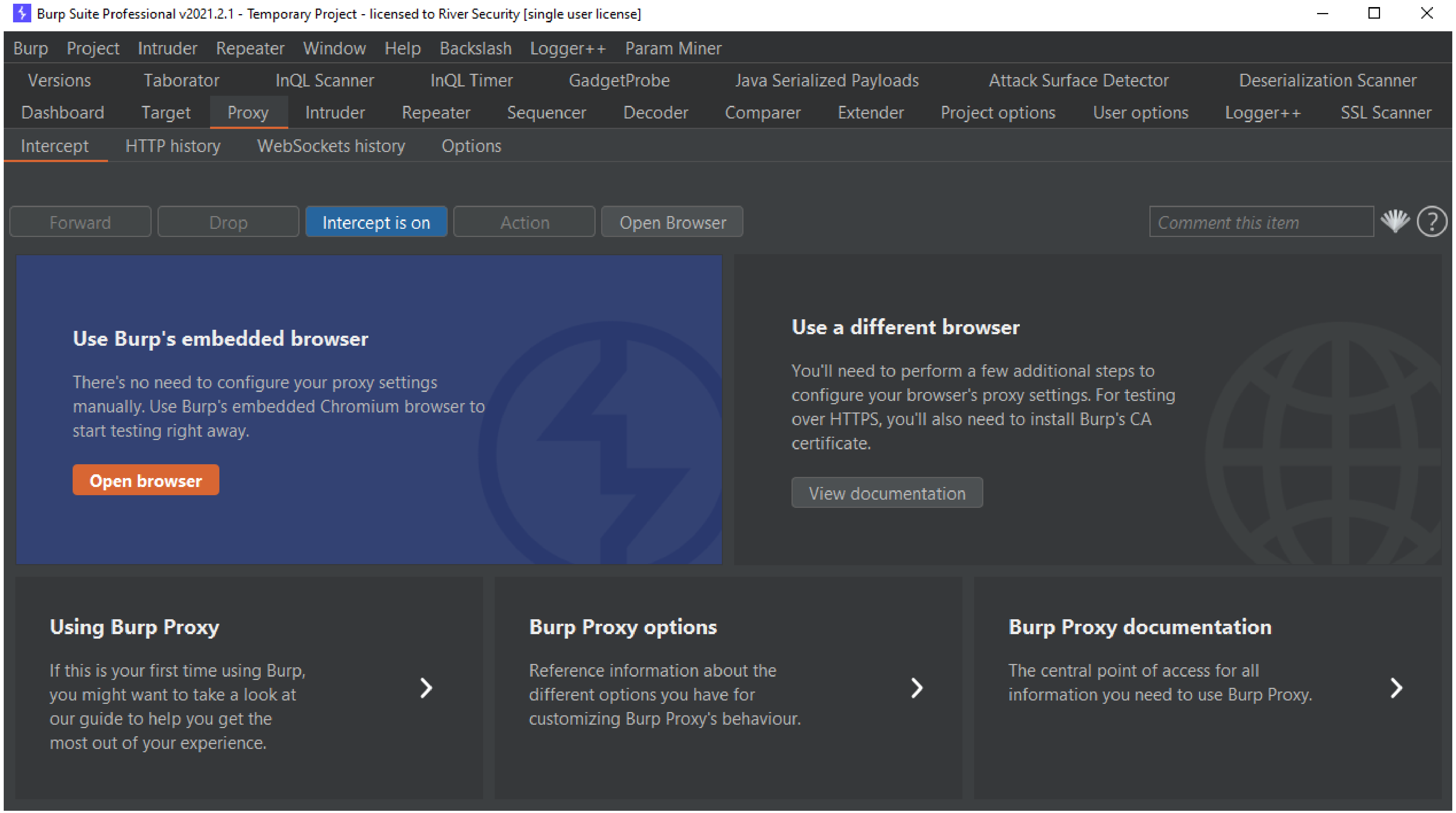
Scan a URL with the Active Scanner (vulnerability scanner:

```
http://localhost:1337/scan
curl -vgw "\n" -X POST
'http://127.0.0.1:1337/v0.1/scan' -d
'{"urls":["http://target.tgt/scanTarge
t1","http://target.tgt/scanTarget2"]}'
```

Check the status and progress of a given scan:

```
http://localhost:1337/scan/task_id
curl -vgw "\n" -X GET
'http://127.0.0.1:1337/v0.1/scan/mytas
k_identifier'
```

# Built-in Browser



Burp Suite Professional v2021.2.1 - Temporary Project - licensed to River Security [single user license]
Burp Project Intruder Repeater Window Help Backslash Logger++ Param Miner
Versions Taborator InQL Scanner InQL Timer GadgetProbe Java Serialized Payloads Attack Surface Detector Deserialization Scanner
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Logger++ SSL Scanner
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
?

### Use Burp's embedded browser

There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.

### Use a different browser

You'll need to perform a few additional steps to configure your browser's proxy settings. For testing over HTTPS, you'll also need to install Burp's CA certificate.

### Using Burp Proxy

If this is your first time using Burp, you might want to take a look at our guide to help you get the most out of your experience.

### Burp Proxy options

Reference information about the different options you have for customizing Burp Proxy's behaviour.

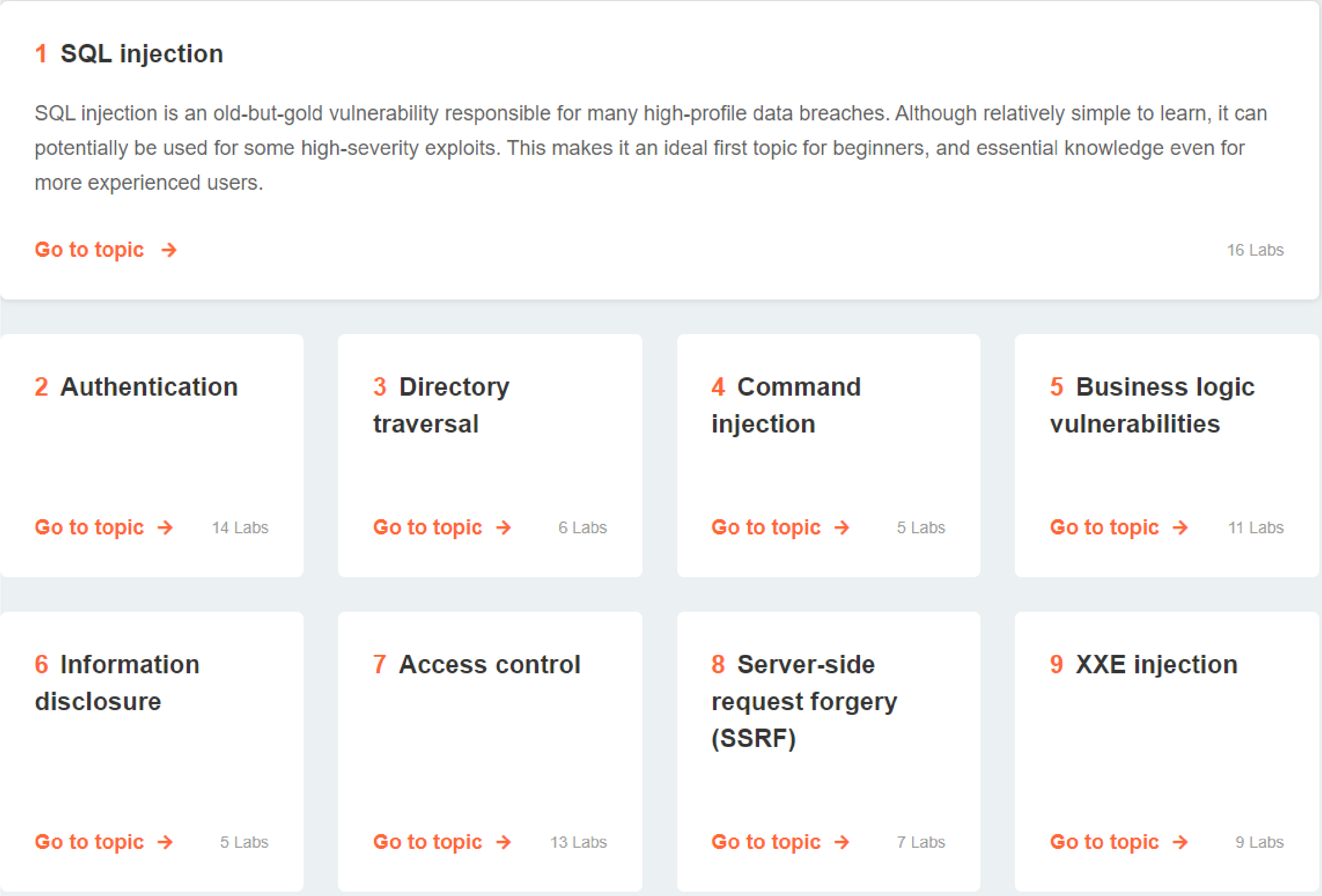
### Burp Proxy documentation

The central point of access for all information you need to use Burp Proxy.

# Other things I really wanted to share

- Goto Search Option
- Renaming Tabs
- Chaining proxies
- Sequencing values
- Configuring scans
- Discover content
- Find references and Comments

# PortSwigger Web-Academy



1 SQL injection

SQL injection is an old-but-gold vulnerability responsible for many high-profile data breaches. Although relatively simple to learn, it can potentially be used for some high-severity exploits. This makes it an ideal first topic for beginners, and essential knowledge even for more experienced users.

Go to topic → 16 Labs

2 Authentication

Go to topic → 14 Labs

3 Directory traversal

Go to topic → 6 Labs

4 Command injection

Go to topic → 5 Labs

5 Business logic vulnerabilities

Go to topic → 11 Labs

6 Information disclosure

Go to topic → 5 Labs

7 Access control

Go to topic → 13 Labs

8 Server-side request forgery (SSRF)

Go to topic → 7 Labs

9 XXE injection

Go to topic → 9 Labs

RIVER SECURITY

- chris@riversecurity.no
- https://riversecurity.eu
- https://www.linkedin.com/company/river-security