



[View Full Course Details including Latest Schedule Online](#)

**PHOENIX TS**

## Burp Suite Training

This Burp Suite Training course is designed to show students how to effectively leverage the Burp Suite tool in their cybersecurity efforts.

### Course Overview

Our 3-day, instructor-led Burp Suite Training course combines lecture and exercises to teach students the following:

- How to perform security tests on web applications using Burp
- How to use different components of Burp Suite including Proxy, Intruder, Scanner, and Repeater
- To customize Burp Extensions when using [Java](#), [Python](#), and [Ruby](#)

Before taking this course, students should have minimal to significant experience with web applications.

### Course Outline

#### Getting Started with Burp

- Starting Burp from the command line
- Specifying memory size for Burp
- Ensuring that IPv4 is allowed
- Working with other JVMs

#### Configuring Browsers to Proxy through Burp

- Configuring widely used browsers to proxy through Burp Suite



## Setting the Scope and Dealing with Upstream Proxies

- Multiple ways to add targets to the scope
- Scope and Burp Suite tools
- Scope inclusion versus exclusion
- Dropping out-of-scope requests
- Dealing with upstream proxies and SOCKS proxies

## SSL and Other Advanced Settings

- Importing the Burp certificate in Mozilla Firefox
- Importing the Burp certificate in Microsoft IE and Google Chrome
- Installing the Burp certificate in iOS or Android
- SSL pass-through
- Invisible Proxy

## Using Burp Tools as a Power User

- Target
- Proxy
- The Message Analysis tab
- Actions on the intercepted requests
- Intruder
- Scanner
- Repeater
- Spidering
- Sequencer
- Decoder
- Comparer
- Alerts

## Searching, Extracting, Pattern Matching

- Filtering
- Matching
- Grep - match and grep - extract



## Using Engagement Tools and Other Utilities

- Search
- Target analyzer
- Content discovery
- Task scheduler
- CSRF proof of concept generator

## Using Burp Extensions and Writing Your Own

- Setting up the Python runtime for Burp Extensions
- Setting up the Ruby environment for Burp Extensions
- Loading and installing a Burp Extension from the Burp App Store
- Loading and installing a Burp Extension manually
- Managing Burp Extensions
- Writing our own Burp Extensions
- Noteworthy Burp Extensions

## Saving Securely, Backing up, and other Maintenance Activities

- Saving and restoring a state
- Automatic backups
- Scheduled tasks
- Logging all activities

## Resources, References and Links

- Primary references
- Web application security testing with Burp
- Miscellaneous security testing tutorials with Burp Suite
- Pentesting thick clients
- Testing mobile applications for web security using Burp Suite
- Extensions references
- Books

## Burp Suite Training FAQs

### Who should take this class?



# PhoenixTS

301-258-8200 | [Sales@PhoenixTS.com](mailto:Sales@PhoenixTS.com) | [www.PhoenixTS.com](http://www.PhoenixTS.com)

This class is ideal for Security Analysts, SOC Analysts/Team Leads and Network and Information Security Managers.

## Starting at \$2,500

### ATTENTION

## Government Employees & Government Contractors call 240.667.7757 for GSA Pricing.



### Price Match Guarantee

We'll match any competitor's price quote. Call us at 240-667-7757.

### This **Burp Suite Training** course includes:

- 3 days of instructor-led training
- Burp Suite Training book
- Notepad, pen and highlighter
- Variety of bagels, fruits, doughnuts and cereal available at the start of class\*
- Tea, coffee and soda available throughout the day\*
- Freshly baked cookies every afternoon\*



**PhoenixTS**

301-258-8200 | [Sales@PhoenixTS.com](mailto:Sales@PhoenixTS.com) | [www.PhoenixTS.com](http://www.PhoenixTS.com)

*\*denotes this benefit is only available at participating locations*