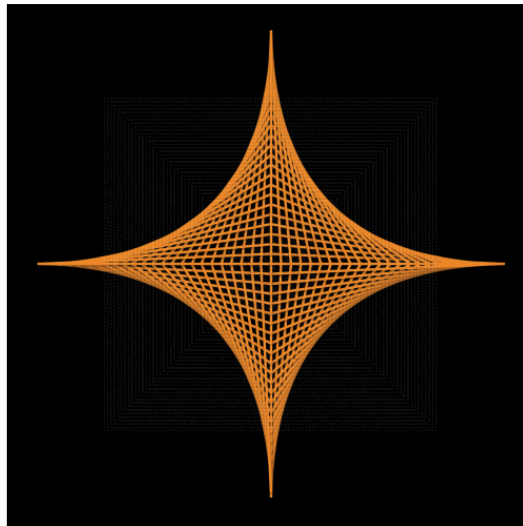


WEB-SPA
Single HTTP/S Request Authorisation Web Knocking
User Guide
_v0.5

Oliver Merki, Yiannis Pavlosoglou

September 15, 2013



seleucus.net

1 Welcome

Thank you for taking an interest in web-spa. As the user guide, this document aims to put you in control of "*speaking*" to your web server in a covert manner. After reading this, you should have a clear understanding of how to issue Operating System (O/S) commands via submitting a URL request to a web server.

This introductory section describes where this user guide fits in the wider remit of web-spa documentation. It gives a definition of what web-spa is and provides an outline on how the sections of this document are structured.

1.1 This Guide & Other Supporting Documentation

The discrepant event discussed herein is web knocking. This document is one of three, with the purpose of describing how web-spa can be used. The three documents are:

- **Web-spa Administration Guide** This document describes how to setup and use the web-spa server. It details how to create new users and add new action numbers with respective O/S commands assigned to them
- **Web-spa Specification Guide** This document describes the actual design detailing the use case, specification, requirements and actual attacks, which this tool has been engineered to withstand
- **Web-spa User Guide** This document describes how to use the web-spa client for issuing commands through a URL request to a web server.

This user guide aims to enable anyone who would be interested in using web-spa to do so. As soon as you install the server side component and decide what actions to allow, you'll be ready to use the corresponding client for issuing direct actions that work for you.

If this is your first time of using web-spa, please note that the client operations described in this document, will not work if a server web-spa instance has not been configured to receive them.

Thus, knowing a client implementation goes hand-in-hand with a server instance for it, please also have a look at the web-spa administration guide document to see how the two can be used in tandem.

1.2 What is Web-Spa?

Web-spa is a complete client/server tool that allows you to send premeditated commands to the system your web server is running on.

1.3 How To Read This User Guide

There is one main section to this user guide, entitled "*Running the Web-Spa Client*". This section has five sub-sections, taking the reader through the 3 necessary steps in order for a web-knock to be created.

This document concludes with the observation that a web-spa knock URL request is only valid for the current minute running and that a new web-knock would have to be created for every minute.

2 Obtaining Web-Spa

This section provides important installation information to help you quickly get started using web-spa on Windows, Mac OS and Unix operating systems.

2.1 System Requirements

You need a computer with the following:

- An Operating System (O/S) of your choice with Java Runtime Environment (JRE) 6 later installed
- 128 megabytes (MB), or greater, of RAM
- 10 MB of free hard-disk space

2.2 The Download

You can obtain the latest release of web-spa from:

- <http://code.google.com/p/web-spa/>

At the time of writing, the current version is webspa-05.zip (~5MB) The download contains the following files:

- web-spa-05.jar
- README
- doc\00-web-spa-administration-guide.pdf
- doc\00-web-spa-specification-guide.pdf
- doc\00-web-spa-user-guide.pdf

Both client and server are bundled into a single executable jar. With the exception of a small shell script, some notes and documentation, all you need is the jar file to run web-spa.

2.3 No Installer?

We have intentionally made web-spa lightweight. As a result, no further configuration or install is required. This is part of the design, in order to keep all that is required to run this tool in a single directory.

3 Running the Web-Spa Client

As this tool is a command-line tool, in this section we take you through the steps required to run web-spa in *client mode*.

3.1 Specifying the Client Parameter

To run web-spa in *client mode* at the command prompt type:

```
user@bath-spa:~# java -jar web-spa-0.5.jar -client
```

This will produce a welcome screen and ask the user to enter 3 necessary inputs, in order for the web-knock request to be created. These are:

1. The host name & protocol
2. Your unique pass-phrase
3. Your selected action number

We will go through each of these in detail now.

3.2 Specifying the Host Name & Protocol

This can be an IP Address or a DNS entry with a protocol specification of either that of the Hypertext Transfer Protocol (HTTP) or the Hypertext Transfer Protocol Secure (HTTPS).

What you will next see on screen is:

```
user@bath-spa:~# java -jar web-spa-0.5.jar -client
```

```
Web-Spa - Single HTTP/S Request Authorisation - version 0.5  
(web-spa@seleucus.net)
```

```
= [Required] Please enter the target host [e.g. http://localhost/]:
```

Assuming that the server running web-spa in *server mode* is

1. www.mywebknockjumphost.com
2. Using HTTPS

Simply type:

```
= [Required] Please enter the target host [e.g. http://localhost/]:  
https://www.mywebknockjumphost.com
```

And press enter.

3.3 Entering Your Unique Pass-Phrase

As a user of web-spa, your administrator would have given you through an *out-of-band* channel your unique pass-phrase. Enter this now:

```
=[Required] Please enter your pass-phrase for that host:
```

Please note that your pass-phrase will not appear on the screen. You will be asked to re-enter your pass-phrase in order to make certain you are generating a web-knock using the correct value.

```
=[Required] Please enter your pass-phrase for that host:
```

```
=[Required] Re-enter the above value:
```

If the values entered don't match, you will be asked to start again, as this is a required input, necessary to generate a web-knock request.

3.4 Selecting an Action Number

As a user of web-spa, your administrator would have given you a maximum of 10 O/S commands, mapped to a unique single digit from [0-9]. An example set view can be seen below:

#	O/S Command	Last Executed
0	sh -c "service apache2 star...	2013-08-10 21:06:42.255
1	sh -c "service apache2 stop...	has never been executed
2	sh -c "/etc/init.d/ssh star...	2013-08-22 11:04:17.133
3	sh -c "/etc/init.d/ssh stop...	has never been executed
4	sh -c "service mysql start;...	2013-08-10 21:07:21.300
5	sh -c "service mysql stop; ...	2013-08-10 21:07:11.600

Based on the above example set view, let's assume that you as a user want to start the Secure Shell (SSH). For this, select action number 2:

```
=[Required] Please enter the action you want to execute on
the host [0,9]: 2
```

And press enter.

3.5 Your Web-Spa Knock

The next screen will display your web-spa knock:

Your Web-Spa Knock is:

```
https://www.mywebknockjumpost.com/72z0WzeM_MmEzZXDrCTY1wd  
3d6-Ks4tRDeZw0PrRlNpraCCMHGmlEhumG14bP1V7s5wvuA5vIA9a_w1JW  
zB0fuQyVHBsF261veaJ/
```

-[Optional] Copy the above URL to the clipboard [Y/n]?

Goodbye!

user@bath-spa:~#

Please note, that this knock is only valid for the current minute running. If the current minute in time changes, you will need to execute the above process again, as your above displayed request will be invalid.

4 Abbreviations

HTTP/S	Hypertext Transfer Protocol / Secure
JRE	Java Runtime Environment
O/S	Operating System
SSH	Secure Shell