Security Configuration Assistant for Apache, MySQL and PHP (SCAAMP) User Guide version 1.0

Birhanu Eshete
Adolfo Villafiorita
Komminist Weldemariam

Center for Information Technology
Fondazione Bruno Kessler (FBK)
Via Sommarive 18, Trento 38100, Italy

January 4, 2011

1 SCAAMP Overview

An absolutely secure software does not exist. In case it does, it is absolutely unusable. However, ensuring reasonable security of applications and environments on which applications are deployed is a necessity specially for web applications. To this end, it is fair to tackle security in a layered fashion. Among the different layers, addressing misconfiguration vulnerabilities of web applications is the subject of this user guide. SCAAMP is developed as a free and open source tool to allow web developers and administrators in pointing out and fixing security configuration vulnerabilities. You can use SCAAMP to audit security configuration details of Apache HTTP server, MyQL database server and PHP interpreter.

In addition to auditing, SCAAMP provides you with functionalities to fix security configuration settings to achieve better security configuration posture for web application development or for preparing a server environment to deploy a web application.

Since SCAAMP is developed using PHP, it is platform independent. Therefore, you can use it to audit and fix security configuration vulnerabilities of Apache, MySQL and PHP on Windows, Linux and MacOS.

2 SCAAMP Requirements

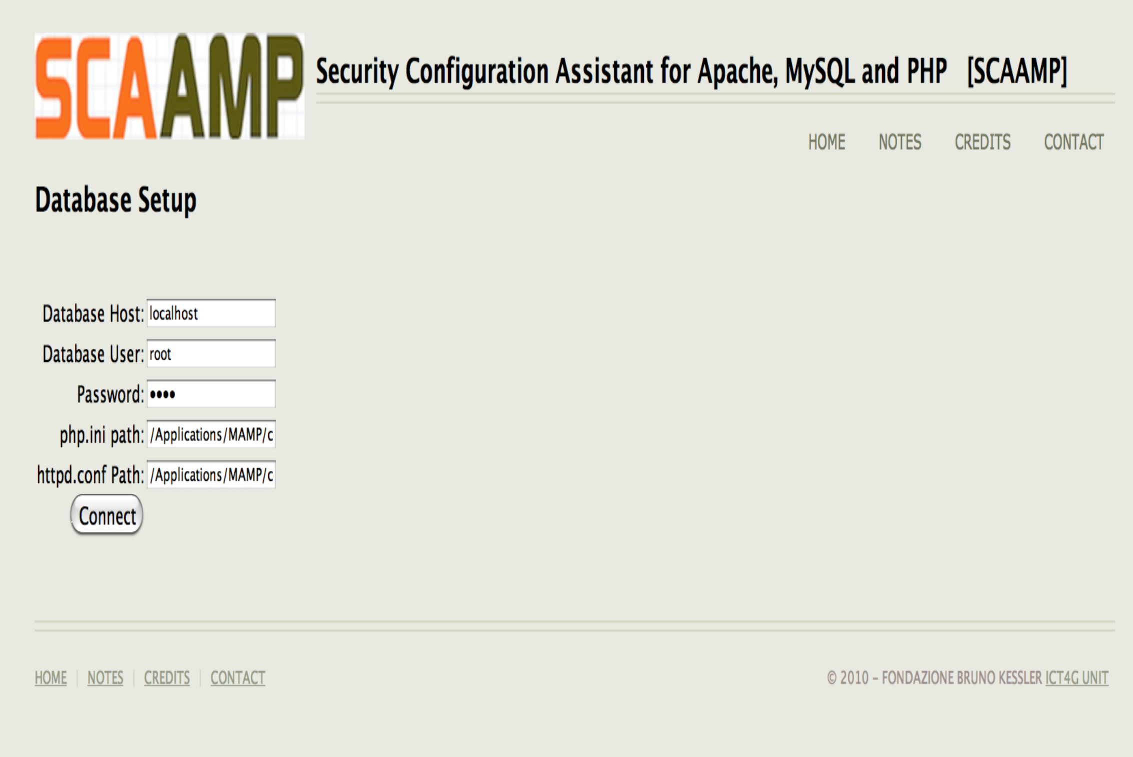
The following are all you need to proceed installation of SCAAMP:

- A user account with administrative(root) privileges so as to be able to install and configure web servers, database servers, server-side script interpreters.
- A system with Apache, MySQL and PHP installed either as server bundle (e.g. LAMP/WAMP/MAMP depending on your operating system) or separately installed and configured package of each.
- Verify that the local server environment is up and running by launching the localhost (e.g. http://localhost:8080).

3 SCAAMP Installation and Setup

Installing SCAAMP is as simple as uncompressing the scaamp1x.zip (x refers to the release number)to the web root directory of your system. The web root directory could be the $HOME../www/ directory under Windows or $HOME/.../htdocs/ directory under most of the Linux distributions and MacOS. In general, whichever operating system you are using, uncompress the SCAAMP package under the directory in your server where web applications are hosted.

The next thing to do is to setup SCAAMP so that it will be ready for use. You launch SCAAMP as (e.g. http://localhost:8080/scaamp1x/setup.php). The



SCAAMP
Security Configuration Assistant for Apache, MySQL and PHP [SCAAMP]
HOME NOTES CREDITS CONTACT

Database Setup

Database Host: localhost

Database User: root

Password: ••••

php.ini path: /Applications/MAMP/c

httpd.conf Path: /Applications/MAMP/c

Connect
HOME | NOTES | CREDITS | CONTACT
© 2010 – FONDAZIONE BRUNO KESSLER ICT4G UNIT

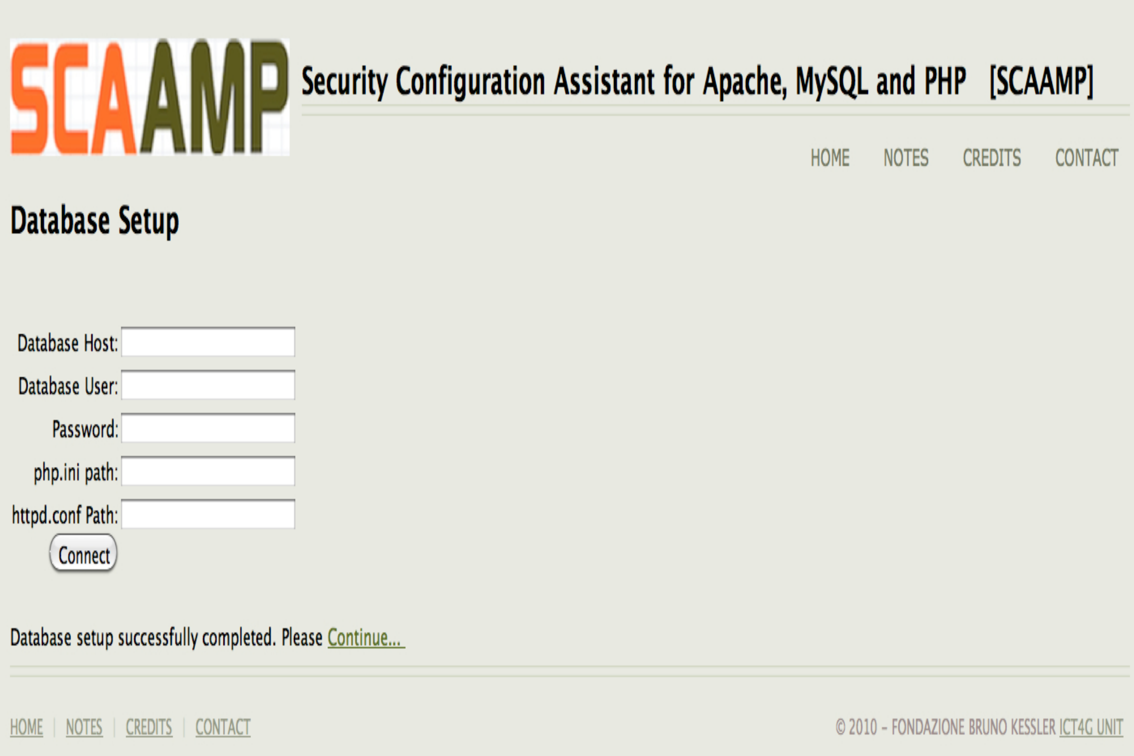
Figure 1: SCAAMP Setup

setup.php script is used to initialize the SCAAMP engine(see Figure 1) and requires you to provide:

- Host name where your server environment is setup. This is usually localhost.
- Username for the MySQL database server (e,g. root or any other database user with create, select, delete, update privileges).
- Password corresponding to the user provided. Passwords are obviously case sensitive.
- Absolute path for the **php.ini** configuration file for the PHP interpreter in use. Make sure that you give the correct path or SCAAMP will encounter problems specially when updating configuration settings for PHP interpreter. The file is usually found under the conf/ directory of the server.
- Absolute path for the **httpd.conf** configuration file of the Apache server in use. Make sure that you give the correct path or SCAAMP will

encounter problems specially when updating configuration settings for Apache server. The file is usually found under the conf/ directory of the server.

Once you provide all the above credentials, click on the **Connect** button. If everything goes well, you will get a success message and a **Continue** button (see Figure 2)will lead you to the SCAAMP index page. Now you are ready to conduct security configuration audit of your server environment.



Security Configuration Assistant for Apache, MySQL and PHP [SCAAMP]

Database Setup

Database Host:

Database User:

Password:

php.ini path:

httpd.conf Path:

Database setup successfully completed. Please Continue...

© 2010 - FONDAZIONE BRUNO KESSLER ICT4G UNIT

Figure 2: SCAAMP Successful Setup

4 Important Points

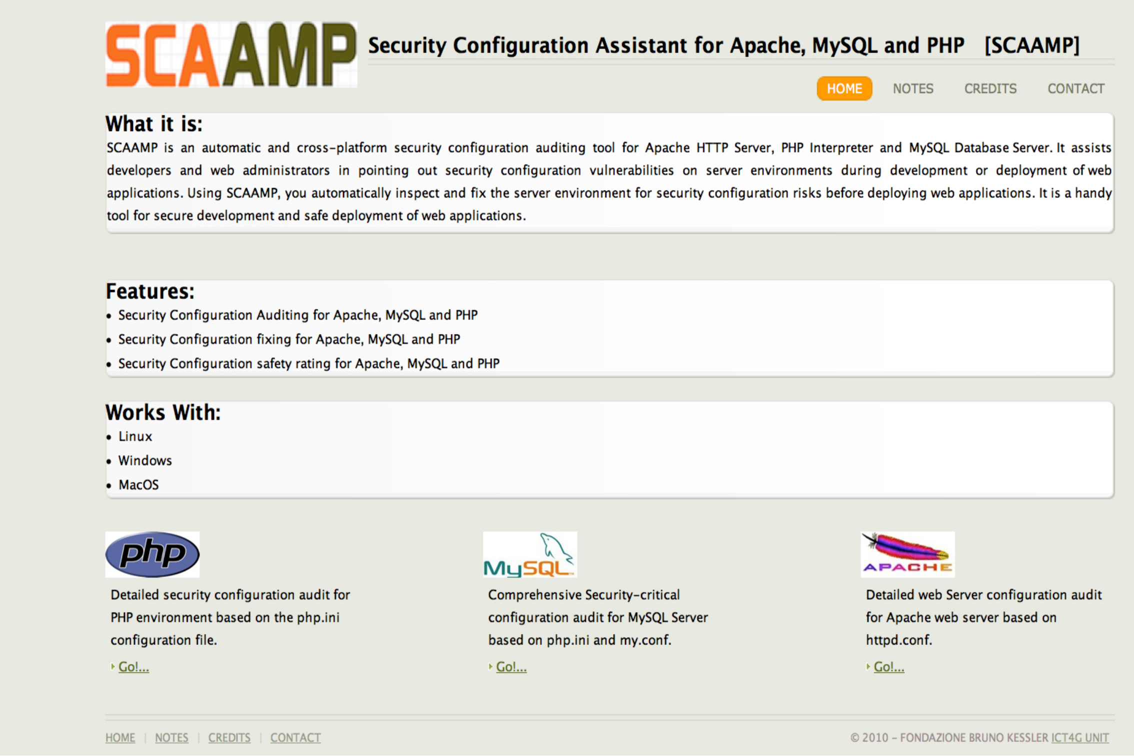
It is worth noting the following while using SCAAMP:

- Before you start fixing security configuration settings, make sure that you backup original configurations for PHP, Apache and MySQL for easy recovery.
- In all the cases, PHP is assumed to be installed as Apache module.

- Make sure that other web servers (e.g. IIS) are not listening on the same port number as Apache to avoid conflicts.
- All configuration directives viewed after audit are security critical ones.

5 SCAAMP Security Configuration Auditing

To conduct security configuration audit you just launch SCAAMP (see Figure 3) index page (e.g. http://localhost/scaamp1x) and you click on the **Go!** button of Apache, MySQL or PHP. Then after, you click on the **Run Configuration Audit** button to scan current configuration.



Security Configuration Assistant for Apache, MySQL and PHP [SCAAMP]

What it is:

SCAAMP is an automatic and cross-platform security configuration auditing tool for Apache HTTP Server, PHP Interpreter and MySQL Database Server. It assists developers and web administrators in pointing out security configuration vulnerabilities on server environments during development or deployment of web applications. Using SCAAMP, you automatically inspect and fix the server environment for security configuration risks before deploying web applications. It is a handy tool for secure development and safe deployment of web applications.

Features:

- Security Configuration Auditing for Apache, MySQL and PHP
- Security Configuration fixing for Apache, MySQL and PHP
- Security Configuration safety rating for Apache, MySQL and PHP

Works With:

- Linux
- Windows
- MacOS

Detailed security configuration audit for PHP environment based on the php.ini configuration file.

Go!...

Comprehensive Security-critical configuration audit for MySQL Server based on php.ini and my.conf.

Go!...

Detailed web Server configuration audit for Apache web server based on httpd.conf.

Go!...

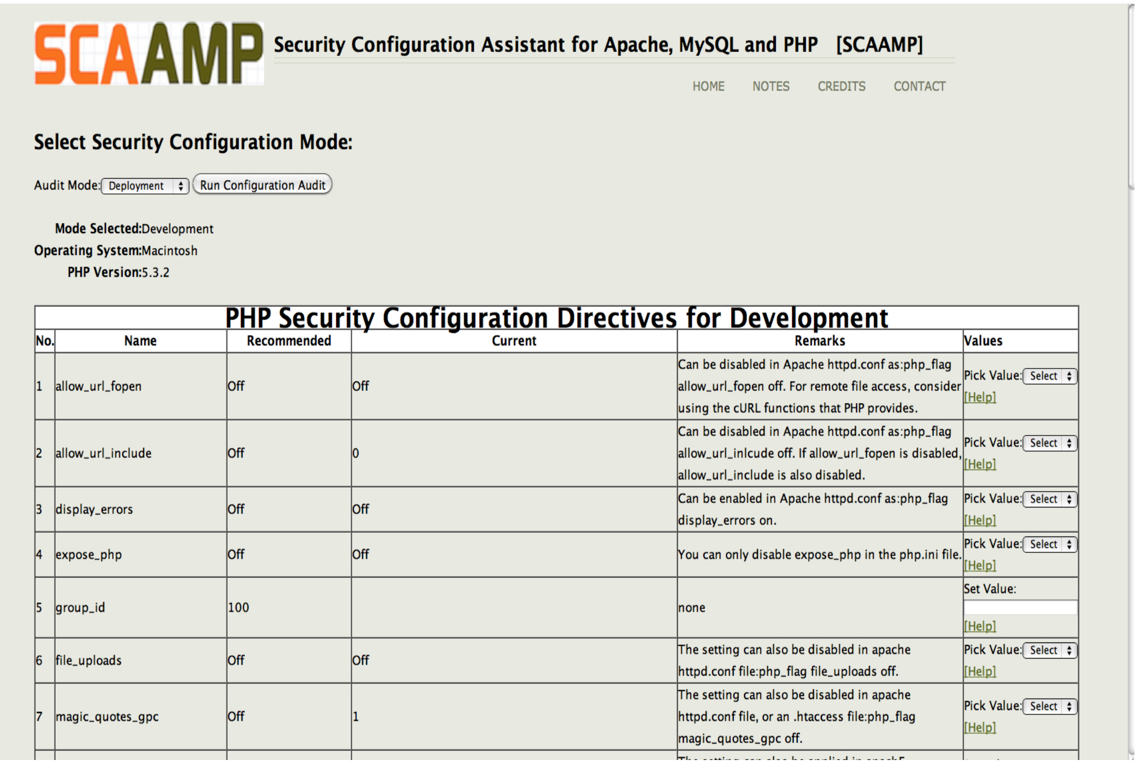
HOME | NOTES | CREDITS | CONTACT

© 2010 – FONDAZIONE BRUNO KESSLER ICT4G UNIT

Figure 3: SCAAMP Index Page

The snapshots in Figure 4 and Figure 5 show the audit outputs which typically show the directive name, current value, recommended value, remark,and options to change each value of the directive. To learn more about the specific characteristics of each configuration directive, you can click the **Help** link which opens a pop-up window that displays detailed description of the directive.

At the bottom of the audit output, you also get the safety rating summary which reports the percentage of correctly/incorrectly set configuration directives



SCAAMP
Security Configuration Assistant for Apache, MySQL and PHP [SCAAMP]
HOME
NOTES
CREDITS
CONTACT

Select Security Configuration Mode:

Audit Mode: Deployment ⬍ Run Configuration Audit

Mode Selected: Development
Operating System: Macintosh
PHP Version:5.3.2

PHP Security Configuration Directives for Development

No.	Name	Recommended	Current	Remarks	Values
1	allow_url_fopen	Off	Off	Can be disabled in Apache httpd.conf as:php_flag allow_url_fopen off. For remote file access, consider using the cURL functions that PHP provides.	Pick Value: Select ⬍ [Help]
2	allow_url_include	Off	0	Can be disabled in Apache httpd.conf as:php_flag allow_url_inlcude off. If allow_url_fopen is disabled, allow_url_include is also disabled.	Pick Value: Select ⬍ [Help]
3	display_errors	Off	Off	Can be enabled in Apache httpd.conf as:php_flag display_errors on.	Pick Value: Select ⬍ [Help]
4	expose_php	Off	Off	You can only disable expose_php in the php.ini file.	Pick Value: Select ⬍ [Help]
5	group_id	100		none	Set Value: [Help]
6	file_uploads	Off	Off	The setting can also be disabled in apache httpd.conf file:php_flag file_uploads off.	Pick Value: Select ⬍ [Help]
7	magic_quotes_gpc	Off	1	The setting can also be disabled in apache httpd.conf file, or an .htaccess file:php_flag magic_quotes_gpc off.	Pick Value: Select ⬍ [Help]

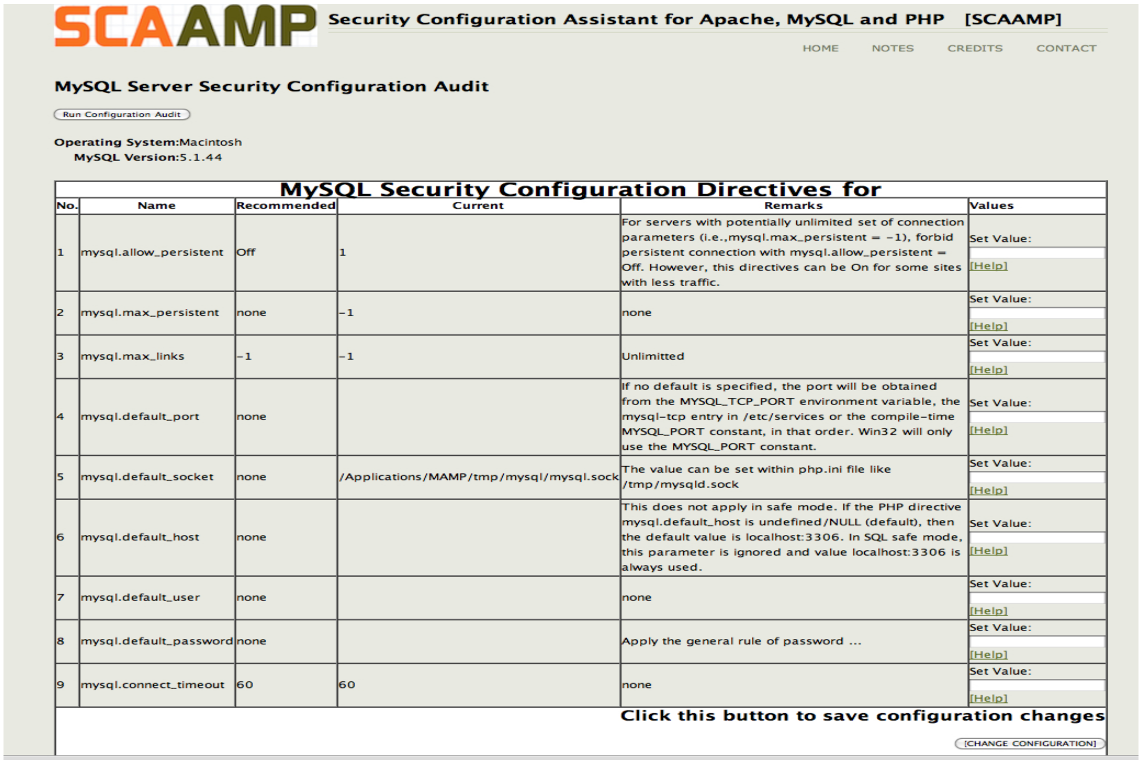
Figure 4: PHP Audit Output

with respect to recommended values. In the case where recommended and current value of a certain configuration directive are not the same, you have to change the current value to the recommended. In doing so, you have to take the appropriate cautions by reading the description and remark of the directive you are dealing with. This is because, some directives have specific mode of usage and may depend on or affect other directives.

6 SCAAMP Security Configuration Fixing

After you inspect the current security configuration of PHP, Apache or MySQL, to improve the security configuration, you just change the individual directive values from unsafe to safe values. By safe, we mean the recommended values based on the description and remarks attached to each directive. Once you change as many values of directives as you want, click on the **Change Configuration** button at the bottom of the audit output.

Once you make the configuration fixing, you have to reset the server environment since the security configuration directive values are read when the server starts. Reseting the server environment depends on the type of server pack-



SCAAMP
Security Configuration Assistant for Apache, MySQL and PHP [SCAAMP]
HOME
NOTES
CREDITS
CONTACT
Run Configuration Audit

MySQL Server Security Configuration Audit

Operating System:Macintosh
MySQL Version:5.1.44

MySQL Security Configuration Directives for

No.	Name	Recommended	Current	Remarks	Values
1	mysql.allow_persistent	Off	1	For servers with potentially unlimited set of connection parameters (i.e.,mysql.max_persistent = -1), forbid persistent connection with mysql.allow_persistent = Off. However, this directives can be On for some sites with less traffic.	Set Value: [Help]
2	mysql.max_persistent	none	-1	none	Set Value: [Help]
3	mysql.max_links	-1	-1	Unlimitted	Set Value: [Help]
4	mysql.default_port	none		If no default is specified, the port will be obtained from the MYSQL_TCP_PORT environment variable, the mysql-tcp entry in /etc/services or the compile-time MYSQL_PORT constant, in that order. Win32 will only use the MYSQL_PORT constant.	Set Value: [Help]
5	mysql.default_socket	none	/Applications/MAMP/tmp/mysql/mysql.sock	The value can be set within php.ini file like /tmp/mysqld.sock	Set Value: [Help]
6	mysql.default_host	none		This does not apply in safe mode. If the PHP directive mysql.default_host is undefined/NULL (default), then the default value is localhost:3306. In SQL safe mode, this parameter is ignored and value localhost:3306 is always used.	Set Value: [Help]
7	mysql.default_user	none		none	Set Value: [Help]
8	mysql.default_password	none		Apply the general rule of password ...	Set Value: [Help]
9	mysql.connect_timeout	60	60	none	Set Value: [Help]

Click this button to save configuration changes

Figure 5: MySQL Audit Output

age you are using and the operating system. Some of the server packages (e.g. MAMP, WAMP) come with control panels that are a click away from resetting the server. While for others (e.g. LAMP for linux), you have to execute scripts (e.g. lamp stop, lamp start). The bottom line is that you already have an idea on how to start and stop the server environment.

To check whether the changes have been reflected or not, you simply repeat the audit process and verify if there is a change on the percentage of correctly set directive values on the safety rating summary.

7 Your Feedbacks

This is just the first version of SCAAMP. There are a lot of issues to take care of and to improve in the upcoming versions. Your feedback is the major input for future enhancements. Feel free to send your observations and comments including feature requests to **eshete@fbk.eu** or **sisai@fbk.eu**.