Community Experience Distilled

Moodle Security

Learn how to install and configure Moodle in the most secure way possible

Darko Miletić

[PACKT] PUBLISHING open source* community experience distilled

Moodle Security

Learn how to install and configure Moodle in the most secure way possible

Darko Miletić

[PACKT] PUBLISHING open source community experience distilled

BIRMINGHAM - MUMBAI

Moodle Security

Copyright © 2011 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing, and its dealers and distributors will be held liable for any damages caused or alleged to be caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

First published: February 2011

Production Reference: 1070211

Published by Packt Publishing Ltd.
32 Lincoln Road
Olton
Birmingham, B27 6PA, UK.

ISBN 978-1-849512-64-0

www.packtpub.com

Cover Image by Asher Wishkerman (a.wishkerman@mpic.de)

Credits

Author
Darko Miletić

Reviewers
Mary Cooch
Ângelo Marcos Rigo
Susan Smith Nash

Acquisition Editor
Sarah Cullington

Development Editor
Neha Mallik

Technical Editor
Pallavi Kachare

Indexer
Hemangini Bari

Editorial Team Leader
Aanchal Kumar

Project Team Leader
Ashwin Shetty

Project Coordinator
Poorvi Nair

Proofreader
Lynda Sliwoski

Production Coordinator
Melwyn D'Sa

Cover Work
Melwyn D'Sa

About the Author

Darko Miletić has been enchanted by computers ever since he saw ZX Spectrum 48K back in 1985. From that moment his only goal was to learn as much as possible about these new contraptions. That dedication eventually led him to work as a part of the editorial staff of Serbian computer magazine "Personalni Računari" where he had a regular column about Microsoft Office. At the same time he studied Mechanical Engineering at the Belgrade University but decided he liked designing computer programs more than designing machines. In 2004, he moved to Argentina and soon started working with e-learning using various web technologies and, as of 2008, his focus is entirely on the Open Source Learning Management System, Moodle. He also led the development of IMS Common Cartridge v1 support for Moodle (1.9 and 2) which is now part of standard Moodle release. Currently, he is working as chief software architect in at Loom Inc. where he leads the development of Loom.

Loom is the Managed Open Source LMS developed specifically to provide a personalized, comprehensive, e-learning experience. It merges the benefits of Open Source technology with the reliability of enterprise support, the dynamic scaling of cloud hosting, and power of customization. It offers complete services including content development, implementation management, faculty and administrative training, and custom programming needs. It is dedicated to developing products and services such as Weaver that are focused on utilizing the data with the LMS to support student retention, to facilitate faculty performance, and to bring about learning outcomes that maximize the success and satisfaction of our clients.

In his spare time, Darko tries to promote electronic books, works on few open source projects, translates SF stories from Serbian to Spanish, and reads a lot.

Writing this book was not a simple task and I would like to thank all the people who helped me write it. First and foremost my thanks goes to Dr. Dietrichson, who had the patience to read and modify some parts of the text and to all the good folks at Loom and UVCMS. Many thanks to my wife who exercised a lot of patience. Thanks to Gustavo Cerati, Sting, Rambo Amadeus, Habib Koité, and *The Doors* who made this journey much more smooth and pleasant with their music.

About the Reviewers

Mary Cooch is the author of *Moodle 2.0 First Look* and *Moodle 1.9 For Teaching 7-14 Year Olds*, both published by Packt. A teacher for 25 years, Mary is based at Our Lady's High School Preston, Lancashire, UK but now spends part of her working week traveling Europe and showing others how to make the most of this popular Virtual Learning Environment. Known online as moodlefairy, Mary runs a blog on `www.moodleblog.org` and may be contacted for consultation on `mco@olchs.lancs.sch.uk`.

Ângelo Marcos Rigo is a 34 years-old web developer who has enjoyed creating customization and fixing web systems since the launching of the Internet in Brasil in 1995.

He has experience with languages PHP, ASP, JSP, Asp.net, ZOPE, and with the following databases: Mysql, Postgresql, Oracle, MSSql.

He has worked in the past for companies in the field of Telecom, for Primary Education, State Departments and also in the PUCRS faculty for the CEAD Department of Distance Learning.

I would like to thank my wife Janaína and daughter Lorena for their support, and for understanding how reviewing is fascinating.

Susan Smith Nash, is currently the Director of Education and Professional Development for the American Association of Petroleum Geologists (AAPG) in Tulsa, Oklahoma, and an adjunct professor at The University of Oklahoma. She was an associate dean for graduate programs at Excelsior College (Albany, NY). Previous to that, she was online courses manager at the Institute for Exploration and Development Geosciences, and director of curriculum development for the College of Liberal Studies at the University of Oklahoma, Norman, US, where she developed degree program curriculum for online courses at the university. She also developed an interface for courses as well as administrative and procedural support, support programmers, protocol and training manuals, and marketing approaches. She obtained her Ph.D. and M.A. in English and a B.S. in Geology from the University of Oklahoma. Nash blogs at E-Learning Queen (`http://www.elearningqueen.com`) and E-Learners (`http://www.elearner.com`), and has written articles and chapters on mobile learning, poetics, contemporary culture, and e-learning for numerous publications, including *Trends and issues in instructional design and technology (3rd ed)*, *Mobile Information Communication Technologies Adoption in Developing Countries: Effects and Implications, Talisman, Press1, International Journal of Learning Objects, GHR, World Literature,* and *Gargoyle*. Her latest books include *Moodle 1.9 Teaching Techniques* (Packt Publishing, 2010), *E-Learners Survival Guide* (Texture Press, 2009), and *Klub Dobrih Dejanj* (2008).

I'd like to express my appreciation to Poorvi Nair for demonstrating the highest level of professionalism and project guidance.

www.PacktPub.com

Support files, eBooks, discount offers and more

You might want to visit `www.PacktPub.com` for support files and downloads related to your book.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at `www.PacktPub.com` and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at `service@packtpub.com` for more details.

At `www.PacktPub.com`, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.

`http://PacktLib.PacktPub.com`

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can access, read, and search across Packt's entire library of books.

Why Subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print and bookmark content
- On demand and accessible via web browser

Free Access for Packt account holders

If you have an account with Packt at `www.PacktPub.com`, you can use this to access PacktLib today and view nine entirely free books. Simply use your login credentials for immediate access.

Table of Contents

Preface **1**

Chapter 1: Delving into the World of Security **7**

Moodle and security **7**

Weak points 8

The secure installation of Moodle **9**

Starting from scratch 9

Installation checklist 10

Quickly securing Moodle **17**

Review the Moodle security overview report 19

Summary **22**

Chapter 2: Securing Your Server – Linux **23**

Securing your Linux—the basics **24**

Firewall 24

User accounts and passwords 26

Removing unnecessary software packages 27

Patching 27

Apache configuration **28**

Where to start 28

Directory browsing 30

Load only a minimal number of modules 31

Install and configure ModSecurity 31

MySQL configuration **32**

PHP configuration **33**

Installation 33

File security permissions **35**

Discretionary Access Control—DAC 36

Directory permissions 36

Access Control Lists 37
Mandatory Access Control (MAC) 37
Adequate location for a Moodle installation 37
How to secure Moodle files 39
DAC 39
ACL 40
Summary 40
Chapter 3: Securing Your Server—Windows 41
Securing Windows—the basics 41
Firewall 42
Keeping OS updated 44
Configuring Windows update 44
Anti-virus 44
New security model 45
File security permissions 46
Adequate location for Moodle installation 47
Installing and securing PHP under Internet Information Server 48
Preparing IIS 49
Getting the right version of PHP 50
Configuring php.ini 51
Adding PHP to the IIS 52
Creating Application pool 52
Create new website 55
Adding PHP mapping 56
Securing MySQL 57
MySQL configuration wizard 58
Configure MySQL service to run under low/privileged user 61
Create a mysql account 61
Summary 63
Chapter 4: Authentication 65
Basics of authentication 65
Logon procedure 66
Common authentication attacks 67
Weak passwords 67
Enforcing a good password policy 68
Protecting user logon 68
Closing the security breach 69
Password change 70
Recover a forgotten password 70
User model in Moodle 74

Authentication types in Moodle **74**
Manual accounts 74
E-mail based self-registration 74
Specifying allowed or denied e-mail domains 75
Captcha 75
Session hijacking 76
No login 78
Summary **78**
Chapter 5: Roles and Permissions **79**
Roles and capabilities **79**
Capability 80
Context 80
Permissions 80
Role 81
How it all fits together 81
Standard Moodle roles **82**
Customizing roles **82**
Overriding roles 85
Best practices **87**
Risky capabilities 87
Summary **89**
Chapter 6: Protection Against Bots **91**
Internet bots **91**
Search engine content indexing 91
Harvesting email addresses 92
Website scraping 92
Spam generators 92
Protecting Moodle from unwanted search bots **92**
Search engines 93
Moodle and search engines 93
Moodle access check 94
Protection against spam bots **98**
User profiles 98
E-mail-based self-registration 99
User blogs 99
Moodle messaging system 100
Cleaning up spam 101
Protection against brute force attacks **102**
Summary **103**

Chapter 7: Securing User Files 105
Uploading files into Moodle 105
How Moodle stores files 106
Points of submitting user files 106
WYSIWYG HTMLArea editor 106
Upload single file simple/advanced assignment 108
Forum 108
Database activity 108
Dangers and pitfalls 108
Classic viruses 108
Macro viruses 108
Applying protection measures 109
Anti-virus and Moodle 110
ClamAV on Linux 110
Configuring Moodle 111
ClamAV on Windows 112
Downloading 112
Configuring clamd service 113
Setting up virus signature database update 115
Scheduling updates 116
Final steps 120
Summary 121
Chapter 8: Securing Moodle Data 123
User information protection 123
User profile page 124
Reaching profile page 124
Protecting user profile information 127
Course information protection 129
Course backups 129
Important information for users of Moodle prior to 1.9.7 130
Security issues with course backups 134
Scheduled backups 135
Summary 136
Chapter 9: Monitoring User Activity 137
Activity monitoring using Moodle tools 137
Moodle log 138
Accessing the Moodle reports 138
Logs report 140
IP address look up page setup 142
Configuring Moodle to use GeoIP database 143
Live Logs report 144
Statistics report 145

Moodle cron 145
Moodle cron on Windows 145
Moodle cron on Linux 145
Enabling statistics report 146
Activity monitoring using OS native tools 148
Linux 148
Server load 148
Disk space 149
Web server load 149
Web server statistics 150
Windows 152
Server load 152
Summary 156
Chapter 10: Backup 157
Importance of backup 157
Backup tools in Moodle 158
Manual backup 158
Automatic backup 159
Content export options for automatic backup 159
Execution configuration options 160
When to use Moodle automated backup 161
Site backup 162
Database 162
Server log 163
Automating database backup—Linux 166
Automating database backup—Windows 168
Restoring database 169
Moodledata directory 170
Linux 170
Windows 172
Moodle directory 173
Disaster recovery scenario 174
Summary 174
Appendix: Authentication Plugins 175
Plugins less common in production servers 175
LDAP server 175
Configuring LDAP PHP extension 176
CAS server 176
FirstClass server 176
IMAP server 176
Moodle network authentication 177
NNTP server 177
No authentication 177

PAM (Pluggable Authentication Modules) 177
POP3 server 177
Shibboleth 177
Radius 177
Summary **178**
Index **179**

Preface

Moving your classes and resources online with a Learning Management System such as Moodle opens up a whole world of possibilities for teaching your students. However, it also opens up a number of threats as your students, private information, and resources become vulnerable to cyber attacks. Learn how to safeguard Moodle to keep the bad guys at bay.

Moodle Security will show you how to make sure that only authorized users can access the information on your Moodle site. This may seem simple, but every day, systems get hacked and information gets lost or misused. Imagine the consequences if that were to happen in your school. The straightforward examples in this book will help you to lock down those access routes one door at a time.

By learning about the different types of potential threats, reading this book will prepare you for the worst. Web robots can harvest your e-mail addresses to send spam e-mails from your account, which could have devastating effects. Moodle comes with a number of set roles and permissions—make sure these are assigned to the right people, and are set to keep out the spam bots, using Moodle's authentication features. Learn how to secure both Windows and Linux servers and to make sure that none of your system files are accessible to the wrong people. Many of the most dangerous web attacks come from inside your system, so once you have all of your security settings in place, you will learn to monitor user activity to make sure that there are no threats from registered users. You will learn to work with the tools that help you to do this and enable you to back up your settings so that even a crashed system can't bother you.

What this book covers

Chapter 1, *Delving into World of Security* opens the book with a basic introduction regarding the importance of security in web-based systems with total emphasis on Moodle. We expose weak points in every Moodle installation and offer a quick procedure for securely installing a new or securing an existing Moodle instance.

Chapter 2, *Securing your server – Linux* covers everything that helps securing typical Linux server starting with the OS basics and then moving on a web server configuration, PHP configuration, and database server configuration. Reader will be presented with a detailed explanation regarding inner workings of the file system on Linux and is offered a concrete examples on how to best utilize them regarding Moodle setup. If you do not use or plan on using Linux-based server for your Moodle setup you can skip this chapter.

Chapter 3, *Securing your server – Windows* covers the general subject of installing basic pieces needed for running Moodle and securing them on a server with Windows OS. We start with the basics related to the general OS issues and then offer explanation regarding file security and ways of getting, deploying, and securing Moodle files. Readers will also be presented with recommended installation and configuration process of PHP under Windows web server and recommended installation and configuration of MySQL.

Chapter 4, *Authentication* is dedicated to the topic of authentication. What it is and the way it is implemented in Moodle. We present the most used authentication methods and the detailed explanation regarding potential security issues and ways of handling them.

Chapter 5, *Roles and Permissions* explains that every complex system offers various usage patterns based on user needs and obligations. Based on such use cases we can identify specific roles. Moodle is no different in this respect. By assigning users to one of the predefined or custom roles we are defining spectrum of the options and actions available to them at every location within LMS. It is paramount for every administrator to understand the access rights as they are implemented. Therefore, in this chapter we will focus on access rights to resources and functions within Moodle starting with Roles and Capabilities, Standard Roles, ways of customizing roles, and our take on best practices regarding roles.

Chapter 6, *Protection against bots* explains how with search engines we—the common users, can find almost anything that is of our personal interest but as a website owner and/or administrator we must know what amount of information is available to the general public and if that amount surpasses our intention or allow boundaries, then we must know how to detect such case and remedy the situation. In this chapter we will dedicate to the exposing the danger of Internet bots. What they are and how they work and how to combat against them.

Chapter 7, *Securing user files* speaks about potential dangers that can be introduced into Moodle by the users. We list all points where one user can upload a custom file. How that file can affect other users (virus infection, inappropriate content, etc.). What can we do to protect our system and other users against these undesired introductions into system. We also explain in detail how to install, configure, and integrate ClamAV anti-virus in Moodle.

Chapter 8, *Securing Moodle Data* explains that when we talk about Moodle data we are referring to both user and course information that is within the platform. In the previous chapter we were talking about user files only. Now we will focus our attention to the protection and separation of internal Moodle data between valid platform users. The topics we will cover are user information protection, course information protection, and best practices for using and applying the techniques presented.

Chapter 9, *Monitoring User Activity* explains that an administrator's work does not end with installation and configuration of Moodle and an operating system. He should constantly monitor the server state and react as quickly as possible. In this chapter we will talk about ways of monitoring the status of Moodle and underlying OS components. We offer list of tools and utilities that can be used on both Linux and Windows for performing these tasks and also a separate section that deals with reports and other elements offered by Moodle for monitoring system activity. We explain how to set up and configure Google maps with Moodle, how to configure Moodle cron and how to configure and use statistics report. The reader is also offered a detailed step by step guide to setting up Webalizer—web traffic analyzer.

Chapter 10, *Backup* is the cornerstone of every well maintained production server. This chapter will try to explain the importance of such procedures regarding Moodle and present tools available both within the platform and outside of it. We will also try to offer some guidelines for what to do in case of total server failure. The reader will be presented with scripts for Linux and Windows that can be used for performing reliable backup procedures.

Appendix offers a list of less used authentication plugins within Moodle, with their short description and potential uses.

Who this book is for

If you are in charge of Moodle—whether you are an administrator or lead teacher—then securing it is one of the most important things that you can do. You need to know the basics of working with Moodle, but no previous experience of system administration is required.

Conventions

In this book, you will find a number of styles of text that distinguish between different kinds of information. Here are some examples of these styles, and an explanation of their meaning.

Code words in text are shown as follows: "Create a directory called `moodledata` somewhere on the disk."

A block of code is set as follows:

```
DatabaseDirectory Z:\clamav\db
DatabaseMirror clamav.edebris.com
DatabaseMirror database.clamav.net
NotifyClamd Z:\clamav\clamd.conf
```

Any command-line input or output is written as follows:

```
CREATE DATABASE moodle CHARSET 'utf8' COLLATION 'utf8_general_ci';
CREATE USER 'moodle'@'localhost' IDENTIFIED BY 'somepass';
```

New terms and **important words** are shown in bold. Words that you see on the screen, in menus or dialog boxes for example, appear in the text like this: "Make sure you check **Unattended operation** at the bottom".

Warnings or important notes appear in a box like this.

Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book—what you liked or may have disliked. Reader feedback is important for us to develop titles that you really get the most out of.

To send us general feedback, simply send an e-mail to `feedback@packtpub.com`, and mention the book title via the subject of your message.

If there is a book that you need and would like to see us publish, please send us a note in the **SUGGEST A TITLE** form on `www.packtpub.com` or e-mail `suggest@packtpub.com`.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide on `www.packtpub.com/authors`.

Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Downloading the example code for this book

You can download the example code files for all Packt books you have purchased from your account at `http://www.PacktPub.com`. If you purchased this book elsewhere, you can visit `http://www.PacktPub.com/support` and register to have the files e-mailed directly to you.

Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books—maybe a mistake in the text or the code—we would be grateful if you would report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting `http://www.packtpub.com/support`, selecting your book, clicking on the **errata submission form** link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded on our website, or added to any list of existing errata, under the Errata section of that title. Any existing errata can be viewed by selecting your title from `http://www.packtpub.com/support`.

Piracy

Piracy of copyright material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works, in any form, on the Internet, please provide us with the location address or website name immediately so that we can pursue a remedy.

Please contact us at `copyright@packtpub.com` with a link to the suspected pirated material.

We appreciate your help in protecting our authors, and our ability to bring you valuable content.

Questions

You can contact us at `questions@packtpub.com` if you are having a problem with any aspect of the book, and we will do our best to address it.

1
Delving into the World of Security

Welcome to Moodle Security!

In the early days of the web, Internet was mostly used for academic purposes. Hence, all communications protocols had very little or no focus on security. The situation started changing as more and more public and commercial services started moving online and common users started actually using Internet in their daily routine. With the increase of user base we see the emerge of the malicious groups of users, the so-called hackers that are focused mostly on information theft and illegal usage. Nowadays it is quite common to be attacked by hacker(s). In fact it is so common and frequent that it is reported that only the USA's cyber attacks generate costs up to 10 billion dollars every year. The purpose of this book is to introduce you to web security while focusing on Moodle.

In this chapter we will cover the following topics:

- Moodle and security
- Weak points
- The secure Moodle installation
- Quickly securing Moodle

Moodle and security

Moodle is an open source **CMS** (**Course Management System**)/**LMS** (**Learning Management System**)/**VLE** (**Virtual Learning Environment**). Its primary purpose is to enable educational institutions and individuals to create and publish learning content in a coherent and pedagogically valuable manner, so that it can be used for successful knowledge transfer towards students.

That sounds harmless enough. Why would anybody want to illegally access an educational platform?

There are various motives of computer criminals. In general, they are people committed to the circumvention of computer security. This primarily concerns unauthorized remote computer break-ins via a communication network such as the Internet. Some of the motives could be:

- **Financial**: Stealing user and/or course information and selling it to other third-parties
- **Personal**: Personal grudge, infantile display of power, desire to alter assigned grades, and so on

Weak points

Moodle is a web application and as such must be hosted on a computer connected to some kind of network (private or public—Internet / Intranet). This computer must have the following components:

- Operating System (OS)
- Web server
- PHP
- Database server
- Moodle

Each of these pieces can be used as a point of attack by a malicious user(s) in order to obtain access to the protected information. Therefore, it is our task to make all of them as secure as possible. The main focus will be directed towards our Moodle and PHP configuration. At the end of the book you can find some recommended literature for additional reading.

The secure installation of Moodle

In this section we follow a secure installation of Moodle. In case you do not already have an installed instance of Moodle, we will show you the quickest way to do that, and at the same time focus on security. If you already have Moodle installed, go to the following section where you will see how to secure an existing installation of Moodle.

Starting from scratch

In order to install Moodle on your server you need to install and configure the web server with support for PHP and the database server. We will not go into the specifics of setting up a particular web server, PHP, and/or database server right now, since it depends on the OS your server has installed. Also we will not explain in detail tasks like creating directories, setting up file permissions, etc as they are OS specific. Later in this book we will address them in detail for both Linux and Windows. If you need to know that right now then I suggest you go directly to the chapter dedicated to the Operating System you plan on using. This section assumes you already know about your OS and have already configured your web server with an empty database. Every installation of Moodle must have:

- Web server with PHP support
- Dedicated database
- Two dedicated directories—one for Moodle and another for platform data

We assume that your web server is Apache (Linux) or IIS (Windows), and that you use PHP 5.1.x or later and MySQL 5.0 or later.

sample content of Moodle Security

- Arthasastra: Selections from the Classic Indian Work on Statecraft pdf
- **click The Just Assassins**
- The Verbally Abusive Relationship: How to recognize it and how to respond pdf, azw (kindle)
- **Bakhtin and Genre Theory in Biblical Studies pdf**
- click Building Web Applications with SVG

- http://aneventshop.com/ebooks/Practical-Packet-Analysis--Using-Wireshark-to-Solve-Real-World-Network-Problems.pdf
- http://www.gateaerospaceforum.com/?library/A-Little-Lumpen-Novelita.pdf
- http://toko-gumilar.com/books/The-Verbally-Abusive-Relationship--How-to-recognize-it-and-how-to-respond.pdf
- http://yachtwebsitedemo.com/books/The-Spanish-Civil-War--History-in-Dispute-.pdf
- http://test1.batsinbelfries.com/ebooks/The-Girl-with-the-Windup-Heart--The-Steampunk-Chronicles--Book-4-.pdf