|  |  |
| --- | --- |
| Information Security  PHP Penetration Testing | Abstract  This assignment investigates security vulnerabilities within PHP software commonly used for hosting forums from a local WAMP server. A variety of older PHPBB versions and WAMP server are explored to locate and understand security issues that could be exploited. Methods of these exploits are researched and tested in this Document.  Tom Bedford  SE3IS11 |

**Contents**

[Introduction 2](#_Toc445123120)

[Method 2](#_Toc445123121)

[Foot-Printing 2](#_Toc445123122)

[Enumeration 2](#_Toc445123123)

[Penetration/Attack 2](#_Toc445123124)

[Install back doors 2](#_Toc445123125)

[Covering Tracks 2](#_Toc445123126)

[Conclusion 3](#_Toc445123127)

# Introduction

The version of WAMP server used in this assignment is WAMP5 1.7.0. The main version of PHPBB focused on in this investigation is phpBB2-2.0.23 although other versions have also been explored. A forum has been set up to practice and execute these vulnerabilities.

The general attacker’s methodology is used to find and execute software exploits within the targeted system. The methodical steps are listed below with a brief description of each.

Infiltrate sensitive areas of the system or stop/deny services running.

1. Foot-printing
2. Scan
3. Enumerate
4. Penetrate
5. Attack
6. Cover Tracks
7. Install Back Doors

# Method

## Foot-Printing

* Session Hijacking exploit - <https://cxsecurity.com/issue/WLB-2009090082>

The possibility of the attacker carrying out CSRF (Cross Site Request Forgery) and gaining control of admin functionality.

* + PhpBB 2.0.19 Cross Site Request Forgeries and XSS Admin
* An analysis of the forum was carried using who.is. This delivered details of DNS and IP address details. Other details such as security updates and software version expiry. <http://who.is/whois/http://localhost/phpbb-2.0.23/phpbb2/index.php>

## Enumeration

## Penetration/Attack

## Install back doors

## Covering Tracks

# Conclusion

**Notes**

LAMP architecture is made up of LINUX, APACHE, MySQL database management and PHP.

Version of PHP installed - phpBB2.0.23

Local WAMP server installed and configured. This is just a windows based version of the LAMP server

Any version of phpBB2.x security can be exploited by a CRSF (Cross-site request forgery) attack. Looked this up briefly <https://www.intelligentexploit.com/view-details.html?id=7671>

# References

PHPBB 2.0.19 exploits. Available at: <https://www.intelligentexploit.com>

<https://threatpost.com/new-exploits-arrive-for-old-php-vulnerability/104881/>

# Appendix