|  |  |
| --- | --- |
| 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](#_Toc446495758)

[Method 2](#_Toc446495759)

[Foot-Printing 2](#_Toc446495760)

[Entry points 2](#_Toc446495761)

[ **Apache Server** 2](#_Toc446495762)

[ **PHP Functionality** 3](#_Toc446495763)

[Enumerating Exploits 3](#_Toc446495764)

[ **DOS (Denial of service attack)** 3](#_Toc446495765)

[ **Session Hijacking exploit** 3](#_Toc446495766)

[Penetration/Attack 3](#_Toc446495767)

[Hardening exploits 3](#_Toc446495768)

[Conclusion 3](#_Toc446495769)

[References 4](#_Toc446495770)

[Appendix 4](#_Toc446495771)

# Introduction

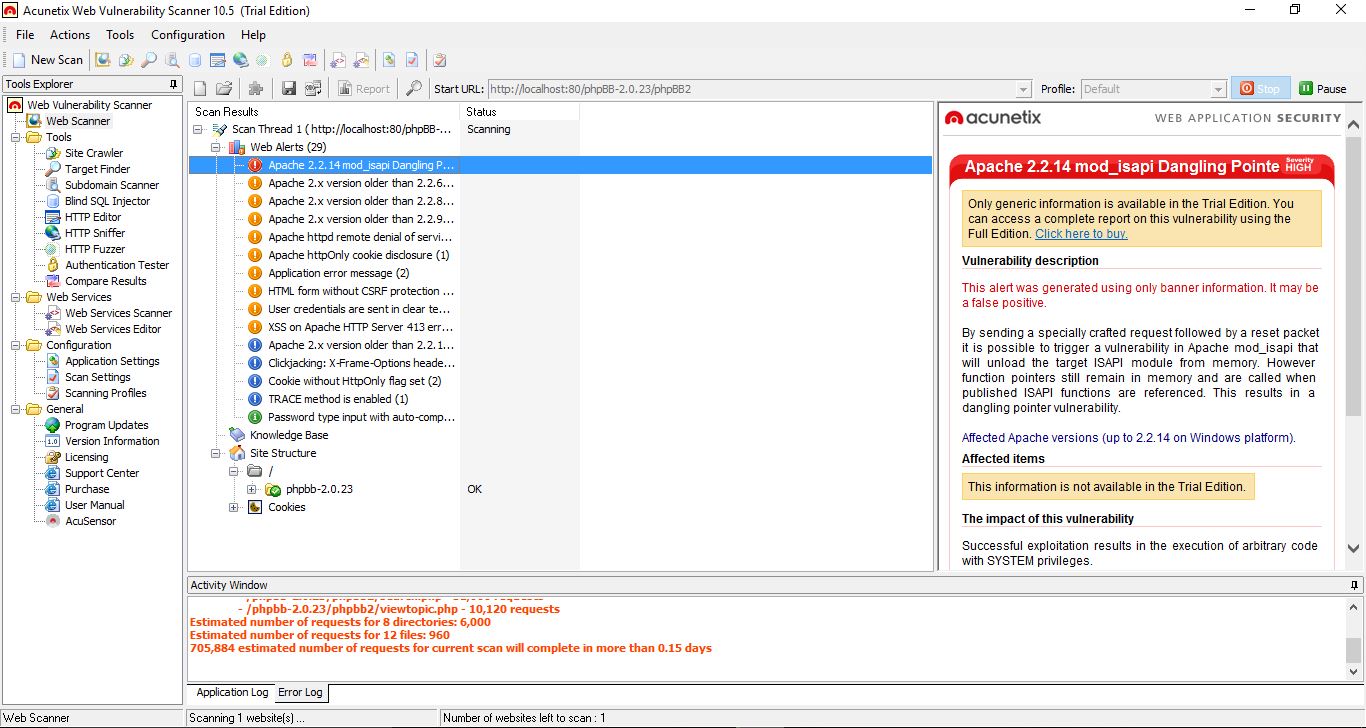
For the purpose of this experiment version 1.7.0 of WAMP has been installed. A PHP forum has been configured on the locally hosted WAMP to practice and test vulnerability exploits of the PHP forum. The main version of PHPBB focused on in this investigation is phpBB2-2.0.23 and 2.0.19 although vulnerabilities of other versions have also been explored.

There are a wide range of readily available third party software and net based vulnerability scanning tools available for penetration testing a targeted site. The majority of these tools can be used unlawfully without the proper permissions to scan the target website.

# Method

## Foot-Printing

A free version of Acunetrix vulnerabilities scanning tool was downloaded and used to scan the locally hosted PHP forum. This image in figure.1 below illustrates the scan results.

**Figure.1 Results of Acunetrix scan on http://localhost/phpBB-2.0.23/phpBB2/**

## Entry points

### **Apache Server**

The http protocol is handled by the WAMP packages apache server. Any user attempting to connect will pass through this web server. It is the initial target of attackers attempting to carry out DDOS or DOS attack as it manages http services.

The server’s buffer can be exceeded by calling methods with a particular input that can overload the buffer. This in turn can allow the user to access and manipulate arbitrary memory outside the scope of original method.

### **PHP Functionality**

The majority of 2.0 PHPBB versions house severe security weaknesses. These points of attack have been hardened by later and safer versions of PHP. There are many outdated and potentially unsecure versions of PHP still being used in systems today.

Injecting SQL statements into the server side language can potentially allow the hacker to retrieve sensitive data. This form of attack is more difficult than a DOS attack but allows the hacker to target specific functionality of the site opposed to bringing it down.

## Enumerating Exploits

### **DOS (Denial of service attack)**

Denial of service is the most common form of attack and essentially looks to flood the server with resource intensive requests to deny services to its users.

**phpBB versions effected:** phpBB\_2.0.19 and below.

**Vulnerability:**

This exploit exhausts the user registration functionality of the site and performs malformed search queries that demand network resources. This exploit targets the profile.php and search.php files that reside on the apache server.

**Methods of execution:** Referenced in the Appendix of this report is a Perl script to perform the method of attack discussed above.

DOS (Denial of Service attack), phpBB 2.0.19. search.php and profile.php DOS Vulnerability.

* **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

<http://joshduck.com/blog/2008/04/05/securing-your-php-code-xss/>

## Penetration/Attack

* **DOS (Denial of Service attack)**

# Hardening exploits

# Conclusion

DDOS and DOS attacks are very resource intensive. As this is the most common form of hack software and systems are been hardened to increase the difficulty of performing such an attack. Injecting SQL code to the server side language is more a challenge to carry out although it is an ideal method for retrieve

**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