phpBB penetration testing

SE3IS14 Coursework 2014-15

DEADLINE: Week 10

# Overview

PhpBB is a widely used open-source bulletin board software package. Like most popular free open source packages it is a tempting target for attack and although a recently released major patch (v3) closed many security holes, servers running older versions of phpBB are still highly vulnerable to intrusion.

As phpBB - along with many other small ‘off the shelf’ web solutions such as Wordpress - usually runs on a shared server, this is a matter of concern; one poorly secured distribution can expose all other hosted programs to attack. This is compounded by phpBBs large amount of potential entry points and the fact that it is built on PHP, another very popular target for attackers.

For this coursework, you will be experimenting with phpBB security by doing the following:

# Install a local version of phpBB along with PHP, MySQL and Apache on a PC or Mac.

Do some research, and find a vulnerable version of phpBB. I recommend any version 2.x, although later, more secure versions will receive more marks. You can find a link to some older versions of phpBB here: <http://sourceforge.net/projects/phpbb/files/?source=navbar>. You may include any appropriate MODs (phpBB extensions) that are compatible.

You will also need a web stack to run your test site on. The recommended stack is the LAMP/WAMP/XAMP (Linux/Windows/cross - Apache - MySQL - PHP) stack, depending on your OS. Due to a security update, older distributions of phpBB may not run on the latest version of PHP due to depreciated functions; you may have to use an older version of WAMP. (Hint: you might want to look into why those functions were depreciated.) Links to these programs will be placed on Blackboard.

1. **Footprint and enumerate your system, identifying the different entry points you could use to break into your bulletin board. (9 marks)**

Potential vulnerabilities could include poorly secured user input, a badly configured web server, old and vulnerable versions of PHP improper validation, ect. Identify the different entry points and compile a list of the ones that you could attempt to exploit. Include this list in your report together with a description of the exploits that can be used to gain access into these entry points.

1. **Using the identified exploits for the version of PhpBB you’ve installed, break into your bulletin board. (12 marks)**

Using the entry points and exploits you’ve identified in 2), show how you can break into phpBB. Describe the methods and provide code examples and screenshots where applicable. Show what’s happening in the server log file at each stage.

1. **Harden phpBB to prevent the attack you just launched. (9 marks)**

Alter phpPP, your server settings, or whatever else is required to harden your forum against the attack you just launched. Describe the methods you used to harden your forum and how they prevent the attack you just carried out.

You should hand in a report that describes stages 2-4 above; describe the attack(s) you have carried out, provide the code that does the penetration and explain how it works. You should also describe in detail how you hardened phpBB to prevent the attacks you carried out.

Your work should concentrate on depth over breadth; an in-depth explanation of two or three attacks will get you better marks than a cursory examination of a dozen. In particular, take care that you demonstrate a proper understanding of the attacks you use, documenting how and why it works in this particular instance.

Please submit your work as a physical copy to G47 and a digital copy using the link on Blackboard.