replace title

replace author

replace date

Contents

List of Figures

Chapter 1

Introduction

Chapter 2

Executive Summary

2.1 Planning

2.1.1 Approach

2.1.2 Scope

2.1.3 Objectives

2.2 Methodology

2.2.1 Information Gathering

2.2.2 System Attacks

2.3 Summary of Findings

Chapter 3

Key Findings

3.1 Auction Site

3.1.1 Path Traversal

Security Implications / Risk Level

Path traversal allows for arbitrary file read across the system, for any files readable by the apache user (www-data). This is dangerous as it could potentially leak sensitive company data, as well as user data. If combined with other vulnerabilities, such as incorrect permissions on log files, it is possible to achieve Remote Code Execution through malicious log read/write.
Overall, the execution of this exploit is trivial, and the repercussions are potentially serious but not disasterous. Due to this, the risk level of this exploit is evaluated to be **medium**.

Cause of Vulnerability

The vulnerability is caused by the method used to retrieve and display image files on the website. Instead of directly referencing the image file through the 'src' field on an 'img' HTML tag, a PHP script is instead used to include the file.
While using PHP include scripts may not normally be dangerous, the file name to be retrieved can be edited by the user, allowing them to easily select which file should be displayed. A lack of filter/extension whitelist makes this even more potent.

Steps to Replicate

The vulner

3.1.2 SQL Injection

Security Implications / Risk Level

Cause of Vulnerability

Steps to Replicate

3.1.3 Weak Authentication

Security Implications / Risk Level

Cause of Vulnerability

Steps to Replicate

3.2 SRV1

3.3 SRV2

3.4 Ubuntu Client

Chapter 4

Recommendations

4.1 Auction Site

4.2 SRV1

4.3 SRV2

4.4 Ubuntu Client

Chapter 5

Conclusion

Chapter 6

References