Web Application Penetration Testing

Contents

Information Gathering 4
1. Conduct Search Engine Discovery and Reconnaissance for Information Leakage 4
2. Fingerprint Web Server 5
3. Review Webserver Metafiles for Information Leakage 7
4. Enumerate Applications on Webserver 8
5. Review Webpage Comments and Metadata for Information Leakage 11
6. Identify Application Entry Points 11
7. Map execution paths through application 13
8. Fingerprint Web Application & Web Application Framework 14

Configuration and Deployment Management Testing 18
1. Test Network/Infrastructure Configuration 18
2. Test Application Platform Configuration 23
3. Test File Extensions Handling for Sensitive Information 29
4. Review Old, Backup and Unreferenced Files for Sensitive Information 32
5. Enumerate Infrastructure and Application Admin Interfaces 34
6. Test HTTP Methods 39
7. Test HTTP Strict Transport Security 41
8. Test RIA cross domain policy 43

Identity Management Testing 45
1. Test Role Definition 45
2. Test User Registration Process 47
3. Test Account Provisioning Process 49
4. Testing for Account Enumeration and Guessable User Account 51

Authentication Testing 56
1. Testing for Credentials Transported over an Encrypted Channel 56
2. Testing for default credentials 59
3. Testing for Weak lock out mechanism 62
4. Testing for bypassing authentication schema 68
5. Test remember password functionality 73
6. Testing for Browser cache weakness 75
7. Testing for Weak password policy 80
8. Testing for weak security Question/Answer 85
9. Testing for weak password change or reset function 86
Authorization Testing 86
1. Testing Directory traversal / file include 86
2. Testing for Privilege Escalation 87
3. Testing for Insecure Direct Object References 90
Session Management Testing 94
1. Testing for Bypassing Session Management Schema 94
2. Testing for Cookies attributes 96
3. Testing for Session Fixation 98
4. Testing for Exposed Session Variables 100
5. Testing for Cross Site Request Forgery (CSRF) 101
6. Testing for logout functionality 104
7. Test Session Timeout 106
Input Validation Testing 108
1. Testing for Reflected Cross Site Scripting 108
2. Testing for Stored Cross Site Scripting 113
3. Testing for HTTP Verb Tampering 117
4. Testing for HTTP Parameter pollution 117
5. Testing for SQL Injection 121
6. Testing for LDAP Injection 134
7. Testing for XML Injection 136
8. Testing for XPath Injection 139
9. Testing for Code Injection 140
10. Testing for Command Injection 142

Testing for Error Handling.....143
1. Analysis of Error Codes.....143
2. Analysis of Stack Traces.....146
Testing for weak Cryptography.....147
1. SSL/TLS Testing.....147
2. Testing for Padding Oracle.....153
Business Testing Logic.....157
1. Test Business Logic Data Validation.....157
2. Test Ability to Forge Requests.....159
3. Test Integrity Checks.....159
4. Test for Process Timing.....162
5. Test Defense Against Application Misuse.....162
6. Test Upload of Unexpected File Types.....162
7. Test Upload of Malicious Files.....170
Client Side Testing.....172
1. Testing for Client Side URL Redirect.....172
2. Testing for Clickjacking.....175
3. Test Cross Origin Resource Sharing.....177
4. Testing for Spoofable Client IP address.....177

Information Gathering

1. Conduct Search Engine Discovery and Reconnaissance for Information Leakage

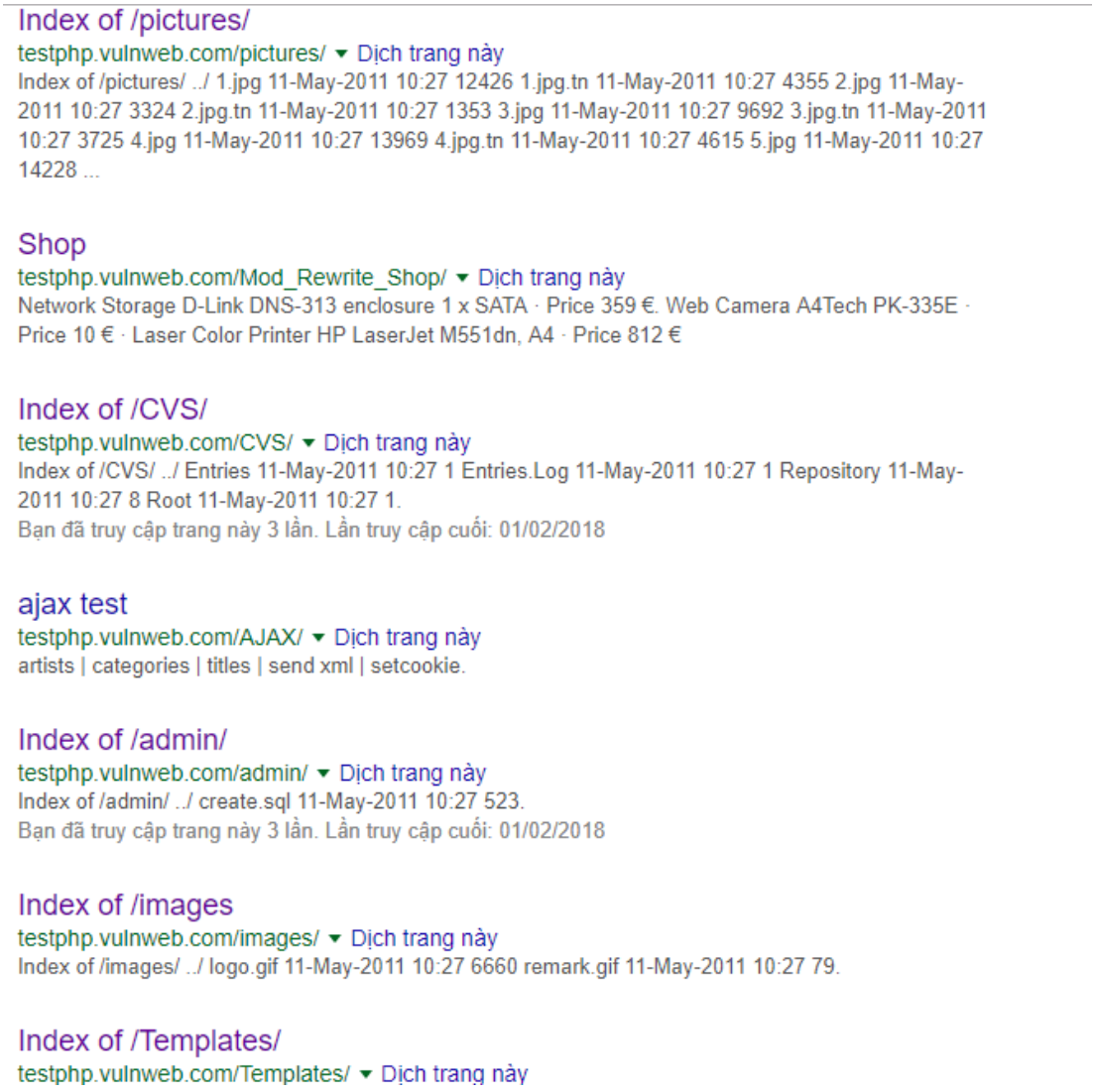
Google hacking technique

Evident:

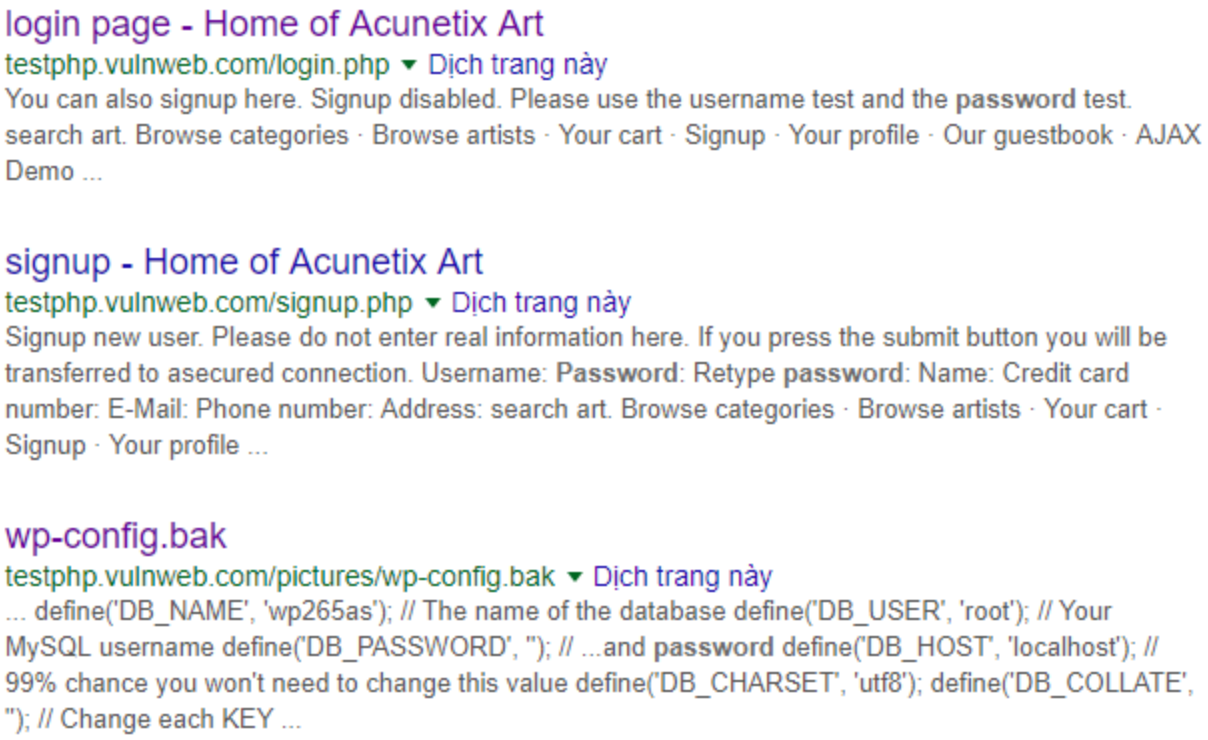
With: testphp.vulnweb.com

I have try google hack with search field parameter as: “site: testphp.vulnweb.com”

After this, I got basic crawling result below:



I used some query to discovering more interested information :



References:

- http://www.mrjoeyjohnson.com/Google.Hacking.Filters.pdf

2. Fingerprint Web Server

Web server fingerprinting is a critical task for the Penetration tester. Knowing the version and type of a running web server allows testers to determine known vulnerabilities and the appropriate exploits to use during testing.

Black box test:

The simplest and most basic form of identify a web server is look at the server field in the HTTP response header with netcat

Example:

nc google.com 80

GET / HTTP/1.1

Host: google.com

enter

enter