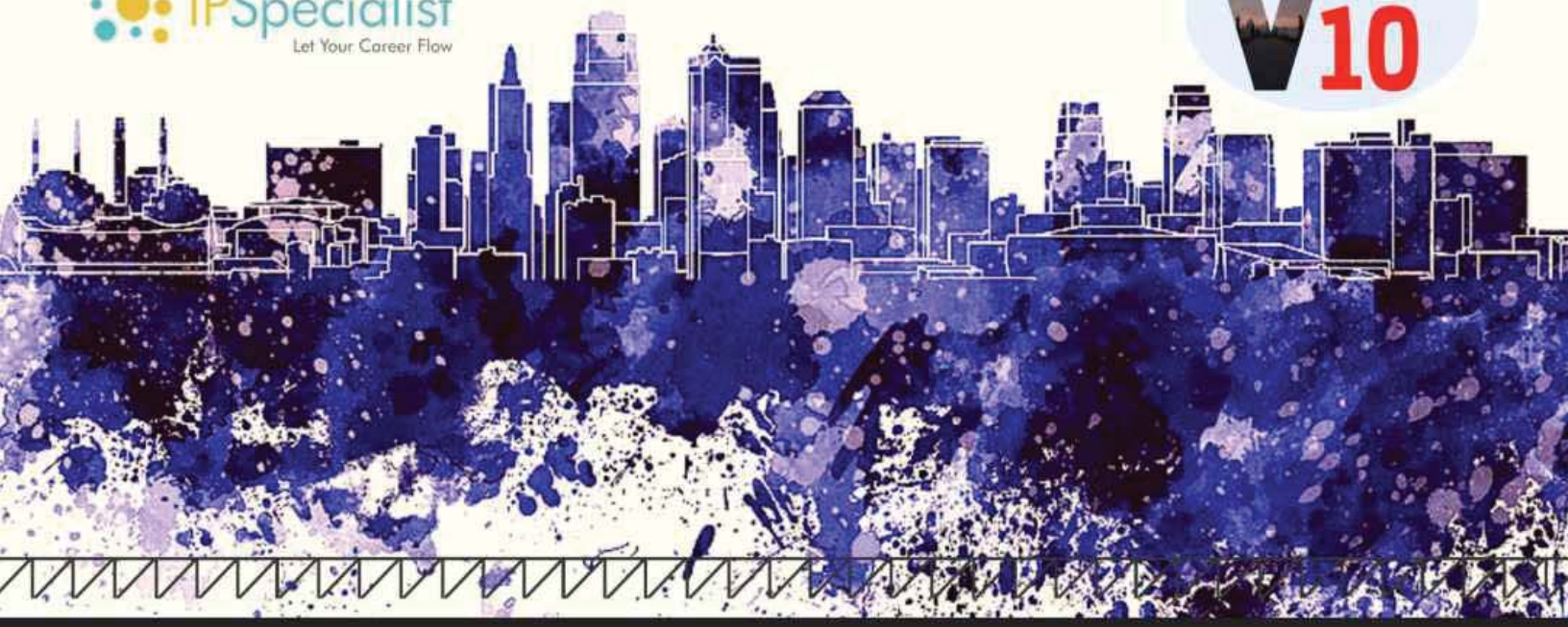
IPSpecialist
Let Your Career Flow

V10



CEH V10 EC-COUNCIL CERTIFIED ETHICAL HACKER

MOST DEMANDING COMPLETE HACKING GUIDE

EXAM: 312-50

C|EH
Certified Ethical Hacker

"To beat a hacker, you need to think like a hacker

MOST ADVANCED HACKING COURSE

www.ipspecialist.net

Chapter 13: Hacking Web Servers

Technology Brief

Web Servers are the programs that are used for hosting websites. Web servers may be deployed on a separate web server hardware or installed on a host as a program. Use of web applications is also increased over last few years. The upcoming web application is flexible and capable of supporting larger clients. In this chapter, we will discuss Web servers vulnerabilities, Web server attacking techniques and tools and their mitigation methods.

Web server Concepts

Web Server is a program that hosts Web sites, based on both Hardware and software. It delivers files and other content on the website over Hyper Text Transfer Protocol (HTTP). As we know, use of internet and intranet has raised, web services have become a major part of the internet. It is used for delivering files, email communication, and other purposes. Web server supports different types of application extensions whereas all of them support HTML for basic content delivery. Web Servers can be differentiated by the security models, operating systems and other factors.

Web Server Security Issue

Security Issue to a web server may include network-level attacks and Operating system-level attacks. Usually, an attacker targets any vulnerability and mistakes in the configuration of the web server and exploits these loopholes. These vulnerabilities may include: -

- Improper permission of file directories
- Default configuration
- Enabling Unnecessary services
- Lack of Security
- Bugs
- Misconfigured SSL Certificates
- Enabled debugging

Server administrator makes sure about eliminating all vulnerabilities and deploying network security measures such as IPS/IDS and Firewalls. Threats and attacks to a web server are described later in this chapter. Once a Web server is compromised, it will result in compromising all user accounts, denial of services offered by the server, defacement, launching further attacks through the compromised website, accessing the resources and data theft.

Open Source Web server Architecture

Open source web server architecture is the Web server model in which an open source web server is hosted on either a web server or a third-party host over the internet. Most popular and widely used open source web server are: -

- Apache HTTP Server

- NGINX
- Apache Tomcat
- Lighttpd
- Node.js

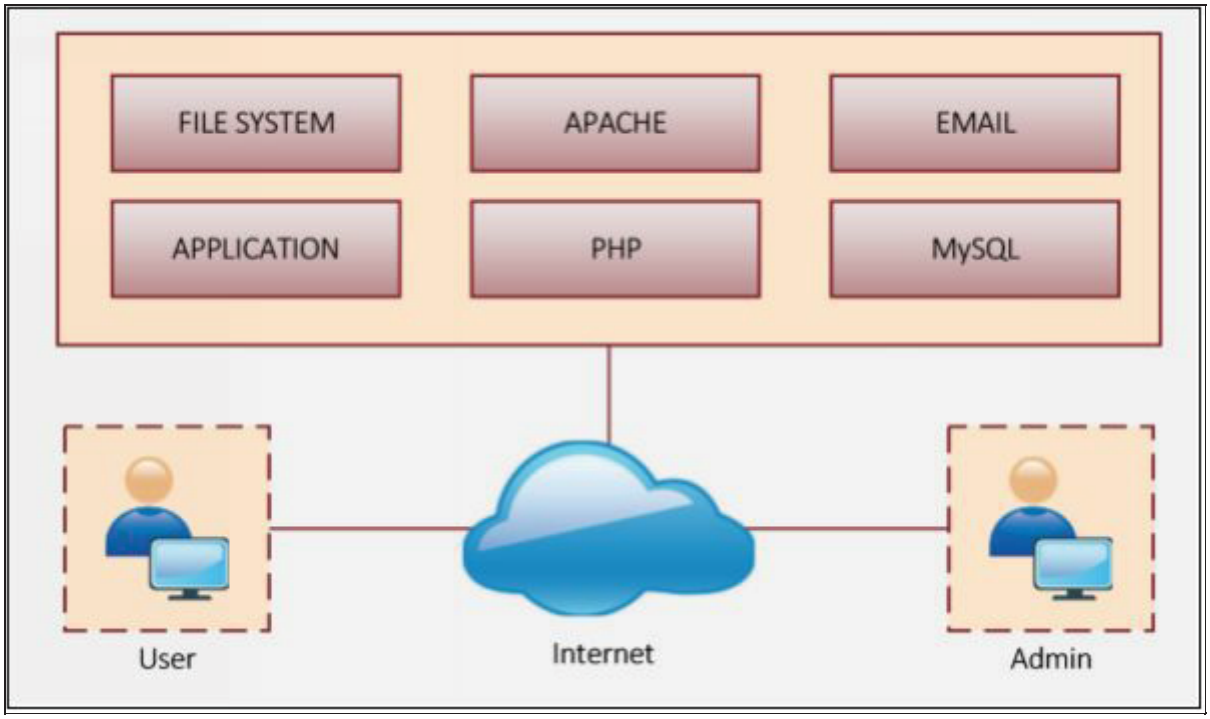


Figure 13-01 Open Web Server Architecture

IIS Web Server Architecture

Internet information services (IIS) is a Windows-based service which provides a request processing architecture. IIS latest version is 7.x. The architecture includes Windows Process Activation Services (WAS), Web Server Engine and Integrated request processing pipelines. IIS contains multiple components which are responsible for several functions such as listening to the request, managing processes, reading configuration files, etc.

Components of IIS

Components of IIS include: -

- ***Protocol Listener***

  Protocol listeners are responsible for receiving protocol-specific requests. They forward these requests to IIS for processing and then return responses to requestors.

- ***HTTP.sys***

HTTP listener is implemented as a kernel-mode device driver called the HTTP protocol stack (HTTP.sys). HTTP.sys is responsible for listening HTTP requests, forwarding these requests to IIS for processing, and then returns processed responses to client browsers.

- ***World Wide Web Publishing Service (WWW Service)***
- ***Windows Process Activation Service (WAS)***

In the previous version of IIS, World Wide Web Publishing Service (WWW Service) is handling the functionality, whereas in version 7 and later, WWW Service and WAS service are used. These services run svchost.exe on the local system and share same binaries.

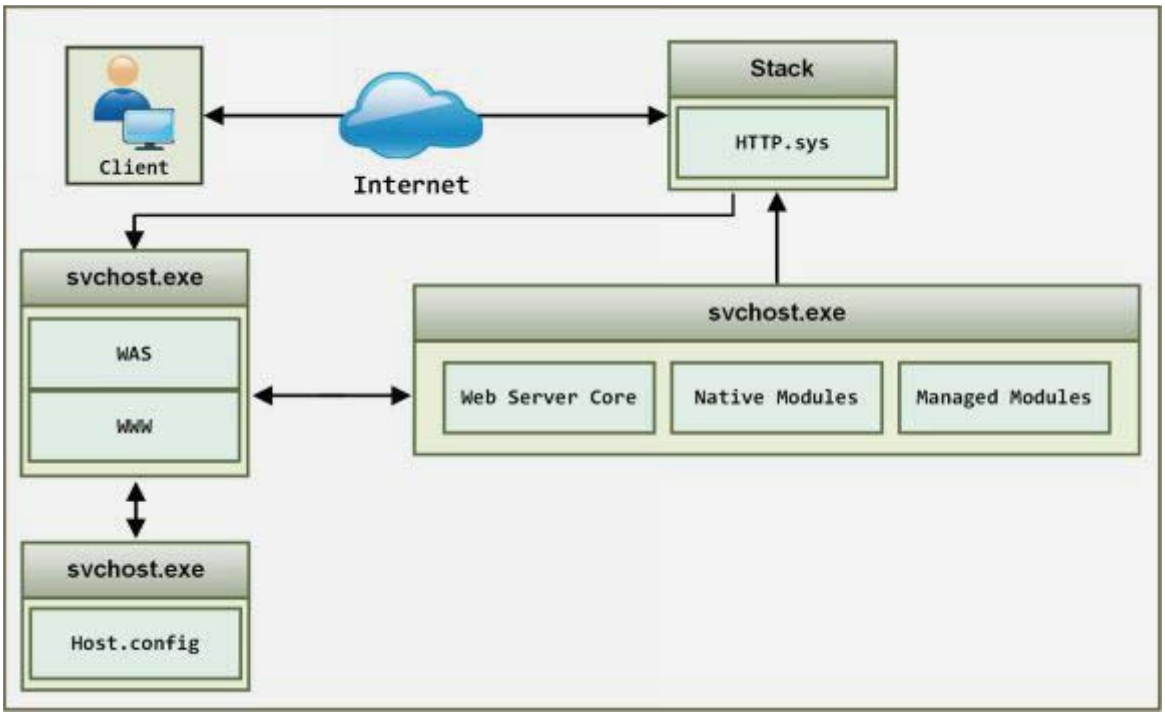


Figure 13-02 IIS Web Server Architecture

Web server Attacks

Web Server Attacking techniques includes several techniques, some of them are defined earlier in this book, remaining techniques are defined below: -

DoS/DDoS Attacks

DOS and DDOS attack, their attacking techniques are defined in detail in chapter 9. These DOS/DDOS attacks are used to flood fake request toward web server resulting in the crashing, unavailability or denial of service for all users.

DNS Server Hijacking

By compromising DNS server, attacker modifies the DNS configuration. The effect of modification results in terms of redirecting the request towards target web server to the malicious server owned or controlled by the attacker.

DNS Amplification Attack

DNS Amplification attack is performed with the help of DNS recursive method. Attacker takes advantage of this feature and spoofs the lookup request to DNS server. DNS server response the request to the spoofed address, i.e., the address of the target. By the amplification of the size of the request and using botnets, results Distributed Denial of Service attack.

Directory Traversal Attacks

In this type of attack, attacker attempt using trial and error method to access restricted directories using dots and slash sequences. By accessing the directories outside the root directory, attacker reveal sensitive information about the system

Man-in-the-Middle/Sniffing Attack

As defined in previous chapters, Using Man-in-the-Middle attack, the attacker places himself in between client and server and sniff the packets, extract sensitive information from the communication by intercepting and altering the packets.

Phishing Attacks

Using Phishing attacks, attacker attempt to extract login details from a fake website that looks like a legitimate website. This stolen information, mostly credentials, are used by the attacker to impersonate into a legitimate user on

the actual target server.

Website Defacement

Website defacement is the process in which attacker after successful intrusion into a legitimate website, alters and modify the content, appearance of the website. It can be performed by several techniques such as SQL injection to access the website and deface it.

Web server Misconfiguration

Another method of attack is by finding vulnerabilities in a website and exploiting them. An Attacker may look for misconfiguration and vulnerabilities of system and components of the web server. An attacker may identify weaknesses in terms of the default configuration, remote functions, misconfiguration, default certificates and debugging to exploit them.

HTTP Response Splitting Attack

HTTP Response Splitting attack the technique in which an attacker sends response splitting request to the server. By this way, an attacker can add the header response, resulting the server will split the response into two responses. The second response is under control of the attacker, so user can be redirected to the malicious website.

Web Cache Poisoning Attack

Web Cache poisoning attack in a technique in which attacker wipe the actual cache of the web server and store fake entries by sending a crafted request into the cache. This will redirect the users to the malicious web pages.

SSH Brute-force Attack

Brite forcing the SSH tunnel will allow the attacker to use encrypted tunnel. This encrypted tunnel is used for the communication between hosts. By brute forcing the SSH login credentials, an attacker can gain unauthorized access to SSH tunnel.

Web Application Attacks

Other web application related attacks may include: -

- Cookie Tampering
- DoS Attack
- SQL Injection

- Session hijacking
- Cross-Site Request Forgery (CSRF) attack
- Cross-Site Scripting (XSS) attack
- Buffer Overflow

Attack Methodology

Information Gathering

Information gathering includes a collection of information about target using different platforms either by social engineering, internet surfing, etc. An attacker may use different tools, networking commands for extract information. An attacker may navigate to robot.txt file to extract information about internal files.

Figure 13-03 Robots.txt file

Web server Footprinting

It includes footprinting focused on the web server using different tools such as Netcraft, Maltego, and httprecon, etc. Results of Web server footprinting brings server name, type, operating system and running application and other information about the target website.

Lab 13-1: Web Server Footprinting using Tool

Web Server Footprinting

Download and install ID Server tool.

1. Enter URL or IP address of the target server

Figure 13-04 ID Serve Application

2. Enter the **Query The Server**/button.

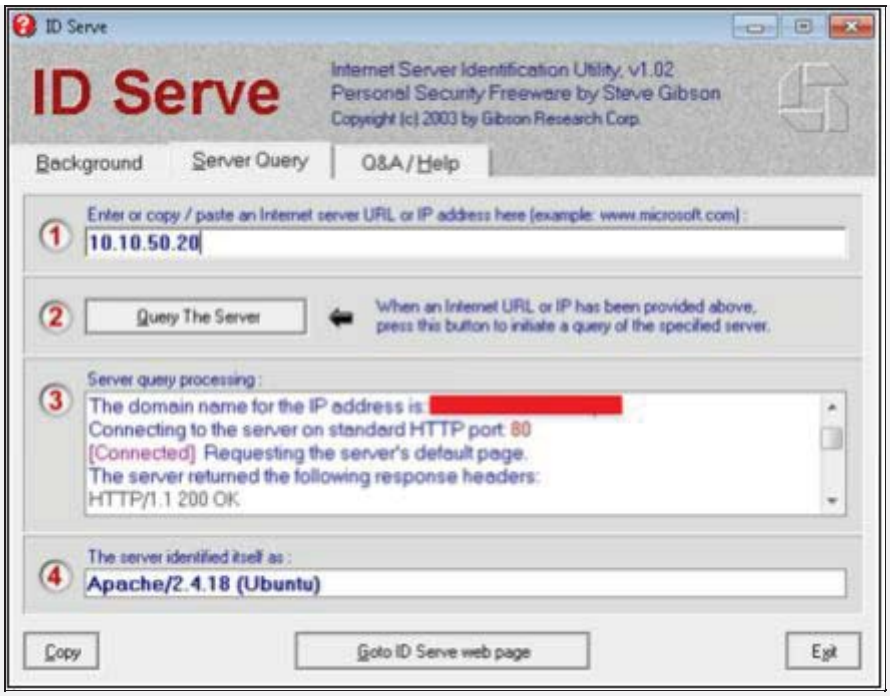


Figure 13-05 Generating Query

3. Copy the Extracted information.

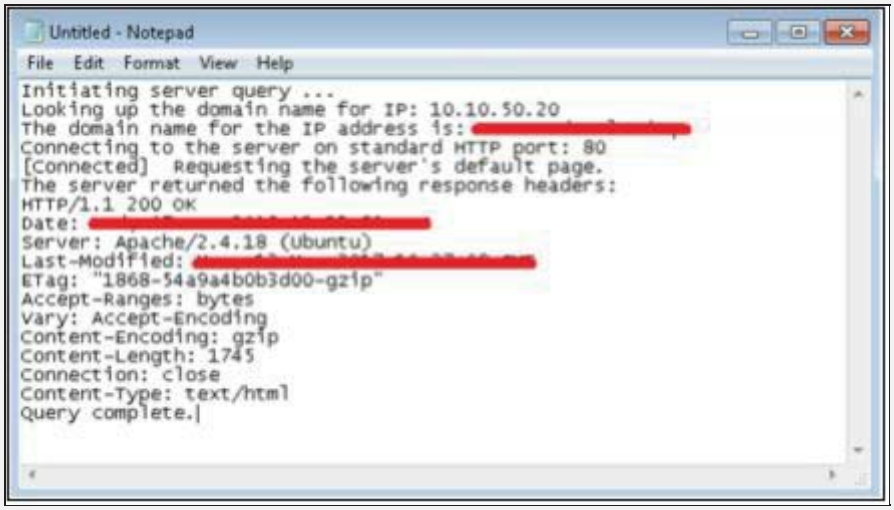


Figure 13-06 Extracted Information

Information such as Domain name, open ports, Server type and other information are extracted.

Mirroring a Website

As defined earlier, mirroring a website is the process mirroring the entire website in the local system. If the entire website is downloaded onto the system, it enables is attacker to use, inspect the website, directories, structure

and to find other vulnerabilities from this downloaded mirrored website copy. Instead of sending multiple copies to a web server, this is a way to find vulnerabilities on a website.

Vulnerability Scanning

Vulnerability Scanners are automated utilities which are specially developed to detect vulnerabilities, weakness, problems, and holes in an operating system, network, software, and applications. These scanning tools perform deep inspection of scripts, open ports, banners, running services, configuration errors, and other areas.

Session Hijacking

Attacker by intercepting, altering and using a Man-in-the-Middle attack to hijack a session. The attacker uses the authenticated session of a legitimate user without initiating a new session with the target.

Hacking Web Passwords

Password Cracking is the method of extracting the password to gain authorized access to the target system in the guise of a legitimate user. Password cracking may be performed by social engineering attack or cracking through tempering the communication and stealing the stored information.

Password Attacks are classified into the following types: -

- Non-Electronic Attacks
- Active Online Attacks
- Passive Online Attacks
- Default Password
- Offline Attack

Countermeasures

The basic recommendation for securing the web server from internal and external attacks and other threat is the place the web server in a secure zone where security devices such as firewalls, IPS, and IDS are deployed, filtering and inspecting the traffic destined to the web server. Placing the web server into an isolated environment such as DMZ protect it from threats.

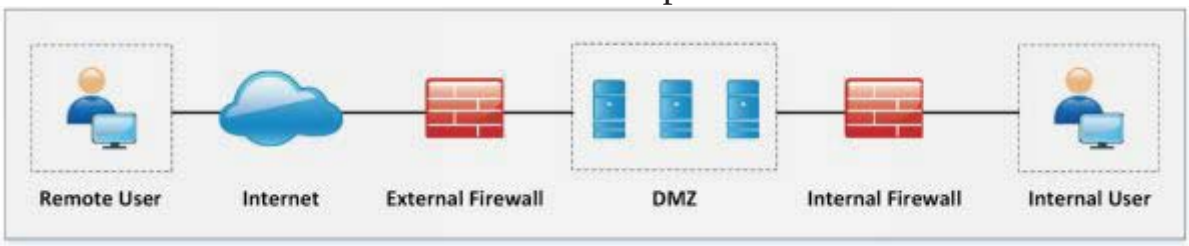


Figure 13-07 Web Server Deployment

Countermeasures

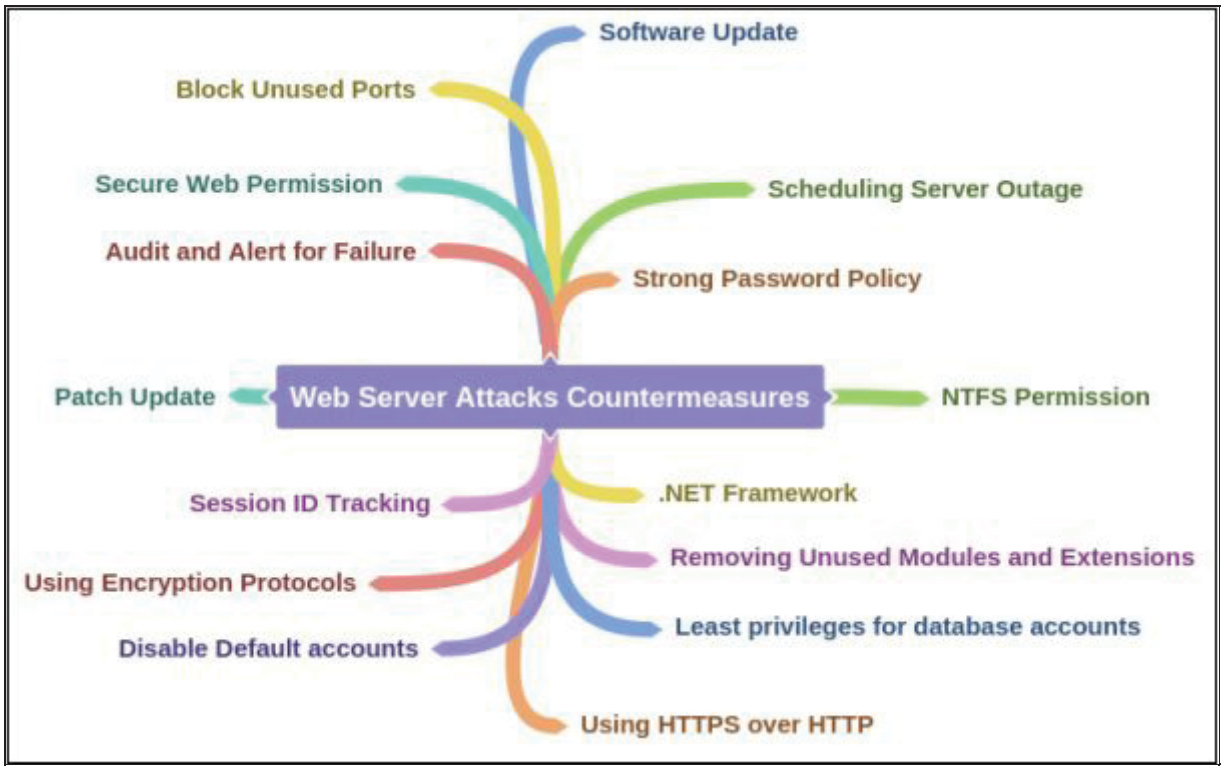
Detecting Web Server Hacking Attempts

There are several techniques that are being used to detect any intrusion or unexpected activity in a web server such as Website change detection system detects for a hacking attempt by using scripting which is focused on inspecting changes made by executable files. Similarly, hashes are periodically compared to detect modification.

Defending Against Web Server Attacks

- Auditing Ports.
- Disabling insecure and unnecessary ports.
- Using Port 443 HTTPS over port 80 HTTP.
- Encrypted traffic.
- Server Certificate
- Code Access Security Policy
- Disable tracing
- Disable Debug compiles

Mind Map


Software Update
Block Unused Ports
Secure Web Permission
Scheduling Server Outage
Audit and Alert for Failure
Strong Password Policy
Patch Update
Web Server Attacks Countermeasures
NTFS Permission
Session ID Tracking
.NET Framework
Removing Unused Modules and Extensions
Using Encryption Protocols
Least privileges for database accounts
Disable Default accounts
Using HTTPS over HTTP

Patch Management

Patches and Hotfixes

As we know, Patches and Hotfixes are required to remove vulnerabilities, bugs, and issues in a software release. Hotfixes are updates which fix these issues whereas patches are the pieces of software that is specially designed for fixing the issue. A hotfix is referred to a hot system, specially designed for a live production environment where fixes have been made outside a normal development and testing to address the issue.
Patches must be to download from official websites, home sites and application and Operating system vendors. The recommendation is to register or subscribe to receive alerts about latest patches and issues.

These patches can be download in the following way: -

- Manual Download from Vendor
- Auto-Update

Patch Management

Patch management is an automated process which ensures the installation of required or necessary patches on a system. Patch management process detects the missing security patches, find out a solution, downloads the patch, test the patch in an isolated environment, i.e., testing machine, and then deploy the patch onto systems.

Lab 13-2: Microsoft Baseline Security Analyzer (MBSA)

The Microsoft Baseline Security Analyzer is a Windows-based Patch management tool powered by Microsoft. MBSA identify the missing security updates and common security misconfigurations. MBSA 2.3 release adds support for Windows 8.1, Windows 8, Windows Server 2012 R2, and Windows Server 2012. Windows 2000 will no longer be supported with this release.

Procedure:

MBSA is capable of scanning Local system, remote system, and range of the computer.

Figure 13-08 Microsoft Baseline Security Analyzer

Select the scanning options as required

Figure 13-09 Scanning Local System using MBSA

MBSA will first get updates from Microsoft, Scan, and then download the security updates.

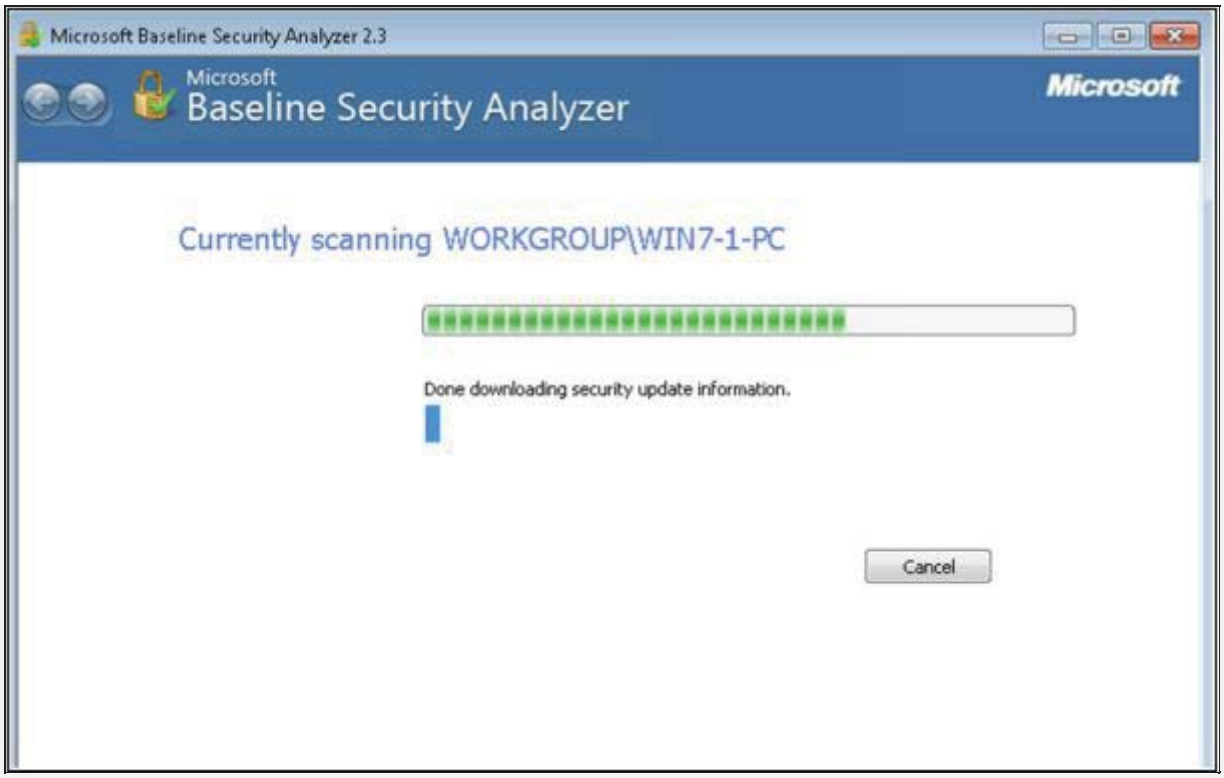


Figure 13-10 MBSA Scanning

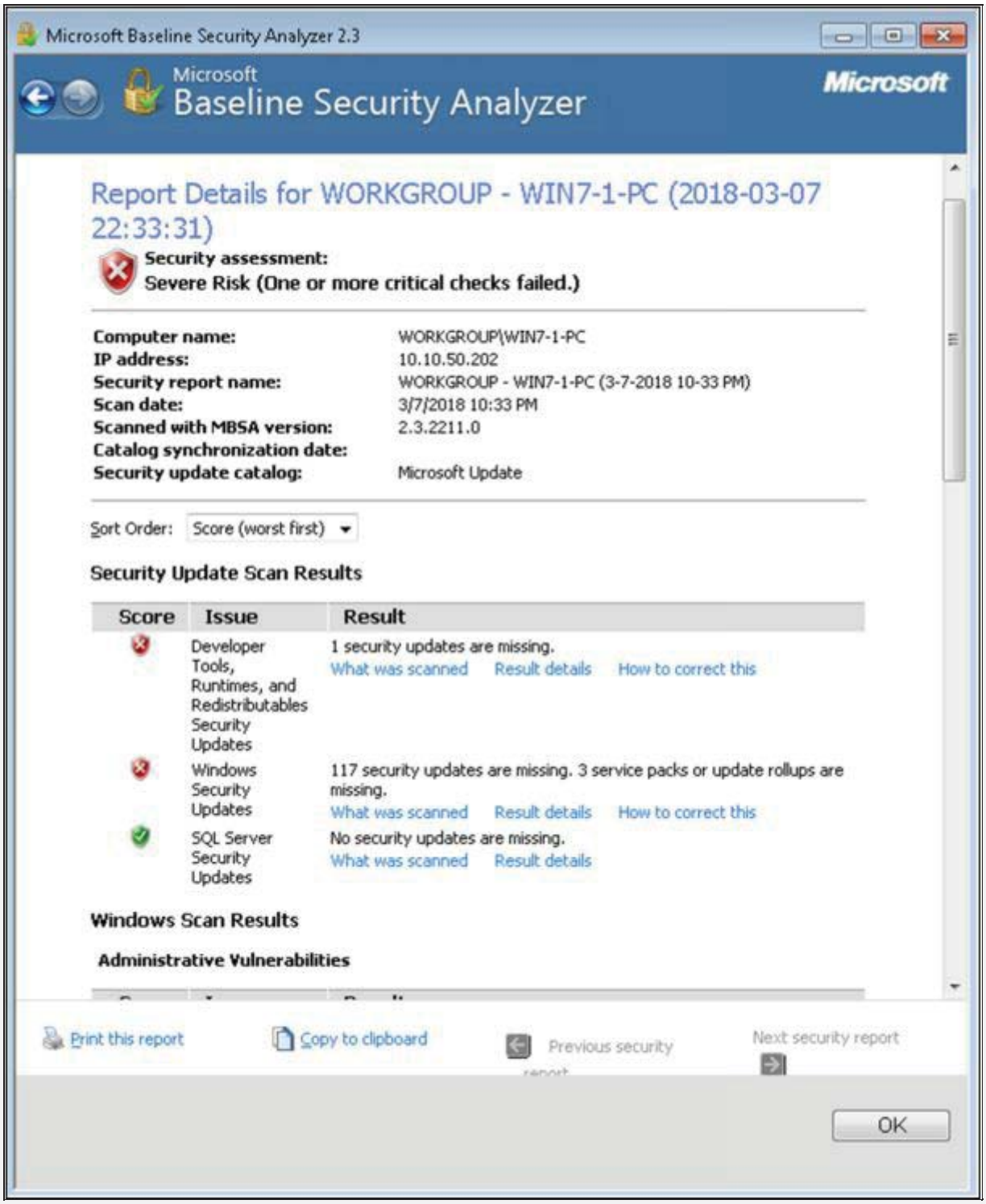


Figure 13-11 MBSA Scanning Result

In the above figure, MBSA Scanning result showing **Security Update Scan Results**. Security Update scan results are categorized by issue and results showing a number of missing updates.

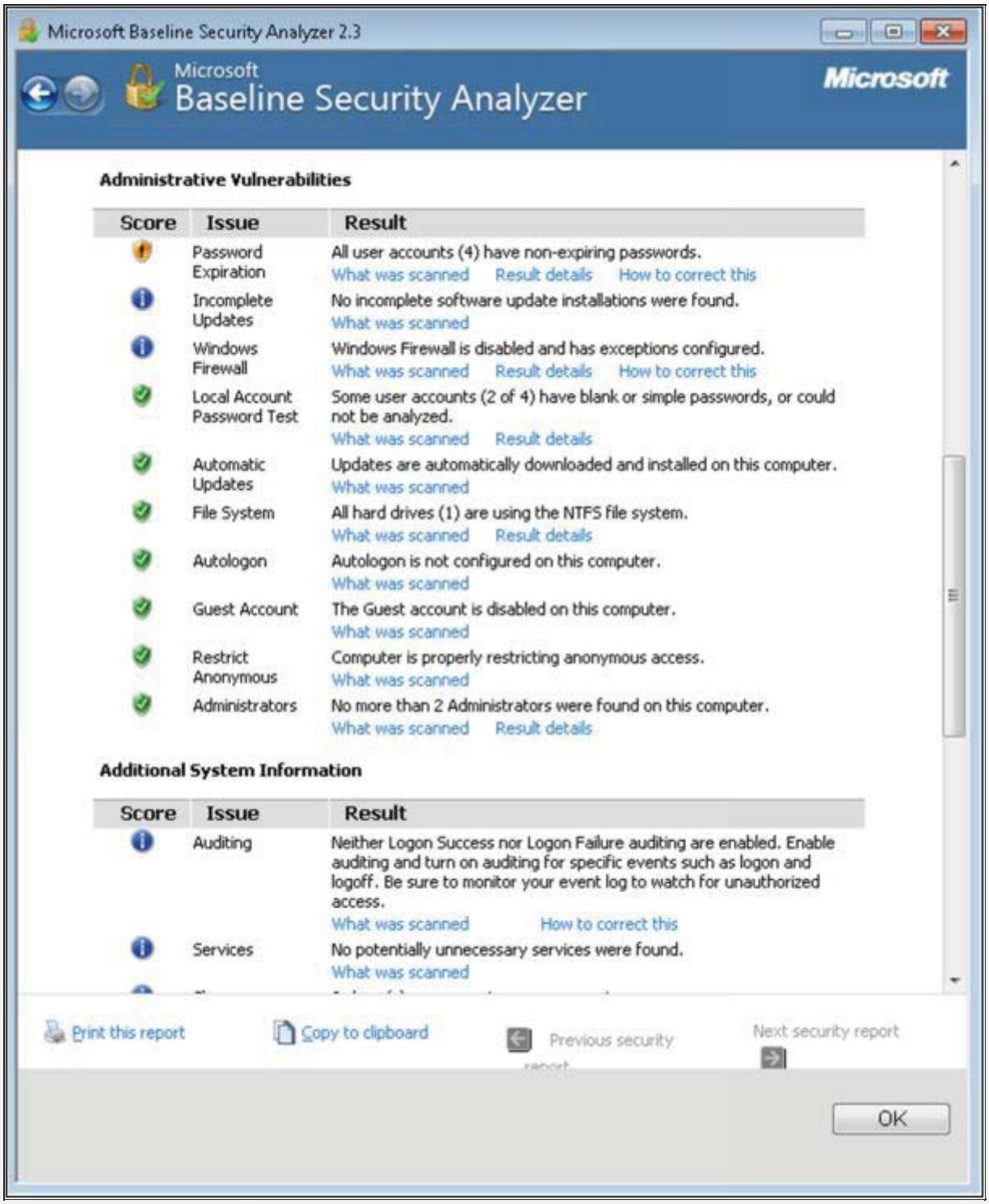


Figure 13-12 MBSA Scanning Result

In the figure above, MBSA Scanning result showing **Administrative Vulnerabilities**. Vulnerabilities such as Password expiry, updates, firewalls issues, accounts and other vulnerabilities are mentioned.

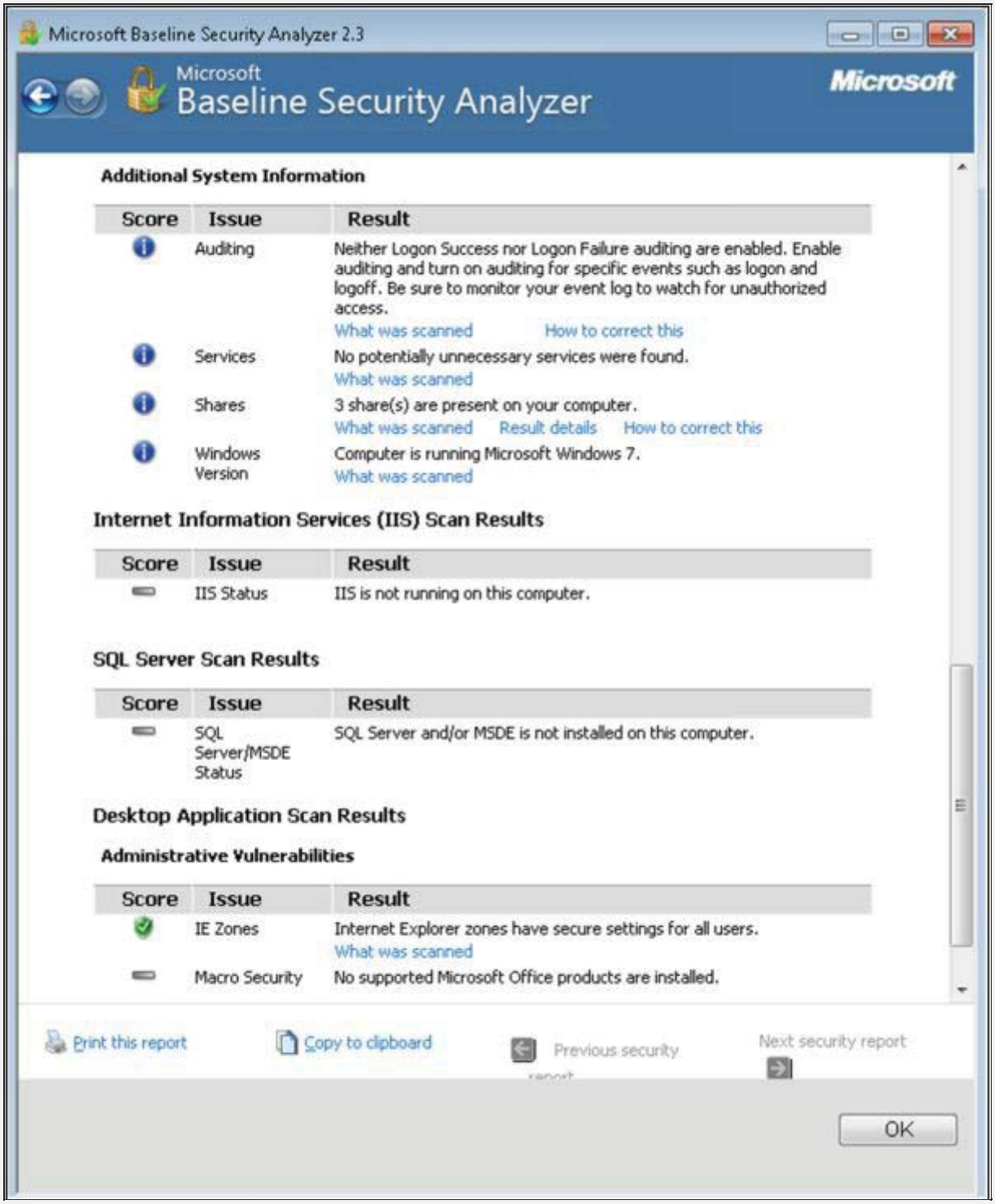


Figure 13-13 MBSA Scanning Result

In the above figure, MBSA Scanning result showing **System information, IIS scan results, SQL Server Result and Desktop application results**.

Lab 13-3: Web server Security Tool

Procedure:

Using **Syhunt Hybrid,** go to Dynamic Scanning. This package also supports Code Scanning and Log Scanning.

Figure 13-14 Syshunt Dynamic Scanning

Enter the URL or IP address

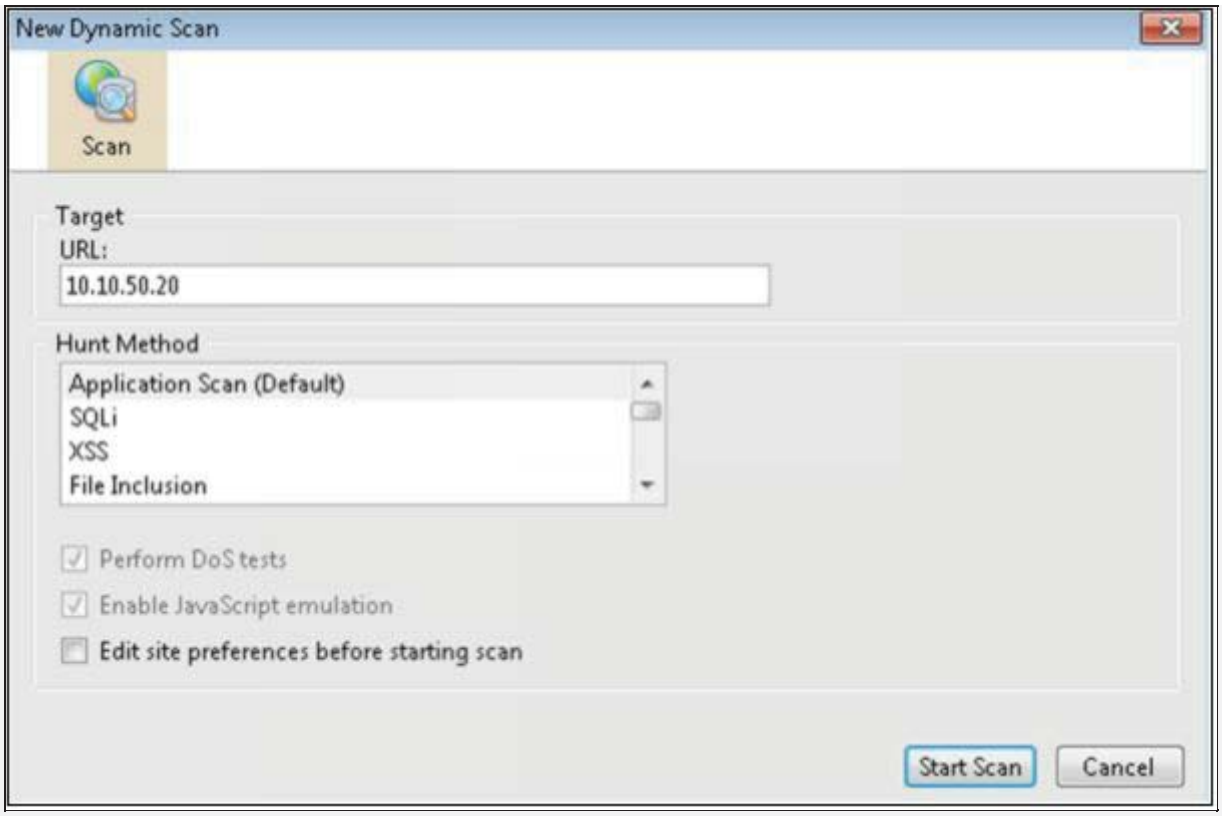


Figure 13-15 Syshunt Dynamic Scanning

Showing Scanning Results, you click on the vulnerability to check the issue and its solution.

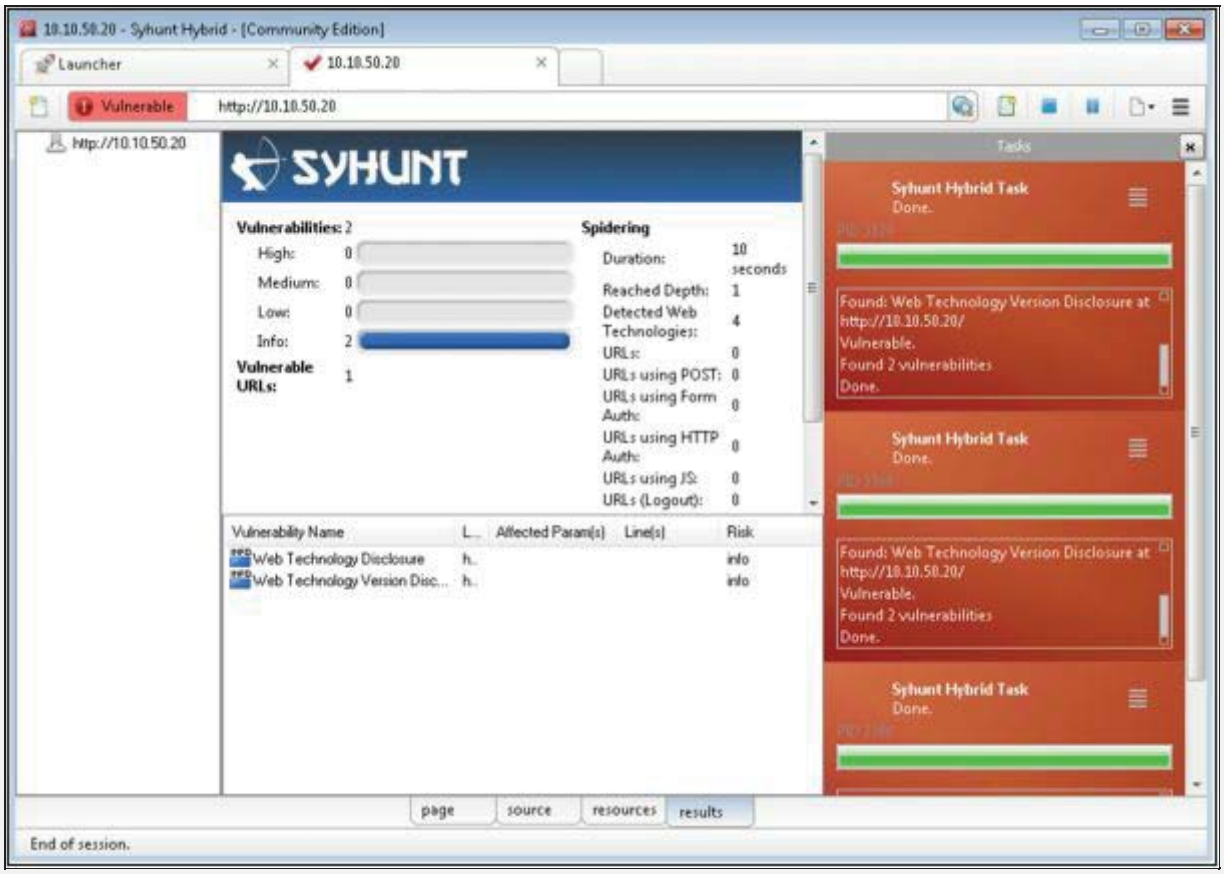


Figure 13-16 Syshunt Dynamic Scanning

Showing Description of vulnerability detected by the tool. Solution tool will provide a recommendation to resolve the issue.

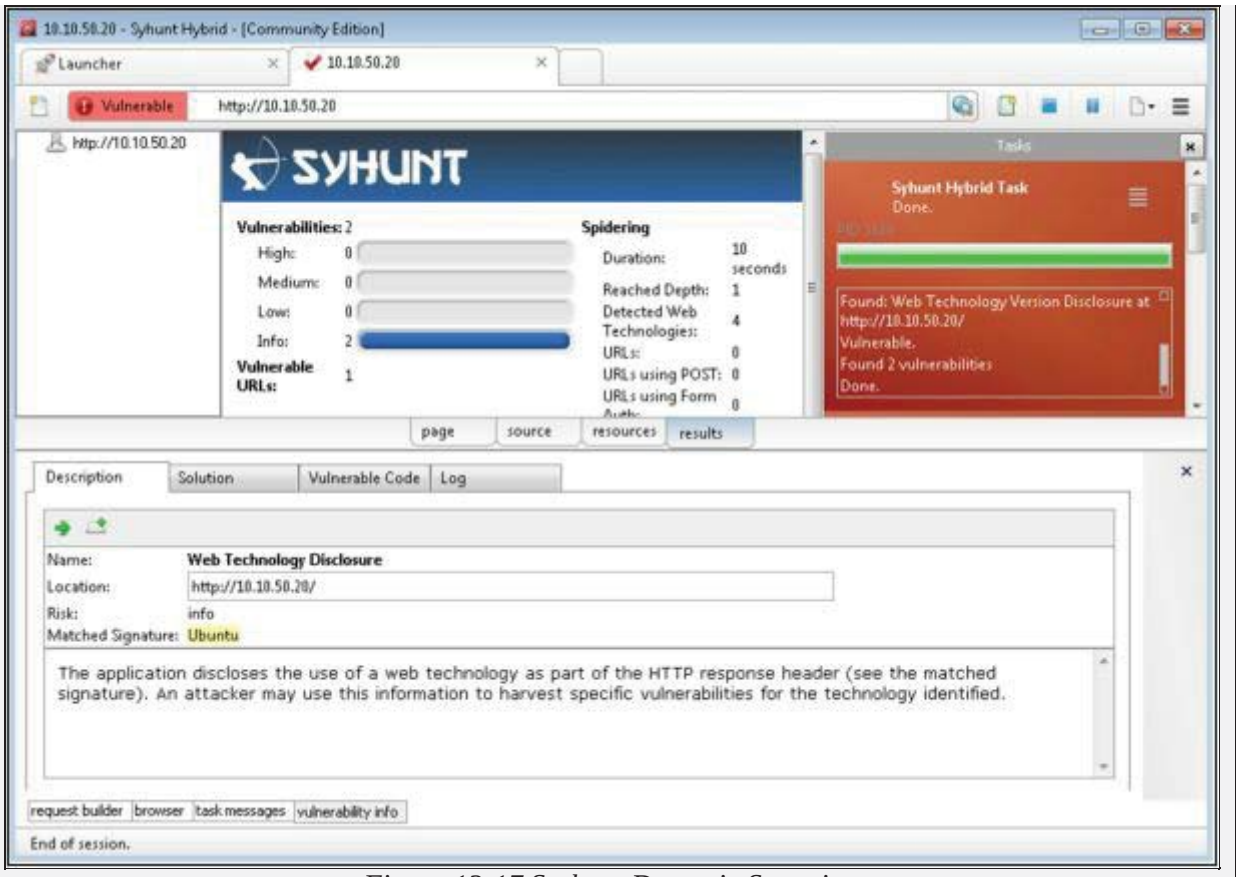


Figure 13-17 Syshunt Dynamic Scanning