REPORT ON

VULNERABILITY ASSESSMENT & PENETRATION TESTING

(VAPT)

NAME => CHARCHIT SUBEDI

DATE => 2021/12/15

Content

Introduction

VAPT is a term used to describe security testing that is designed to identify and help address cyber security vulnerabilities. The meaning of VAPT can vary from one geographical region to another, either as a bracket for multiple distinct services, or a single, combined offering. VAPT as a whole could include anything from automated vulnerability assessments to human-led penetration testing and red team operations.

Why do you need VAPT?

⇒ The evolving tools, tactics and procedures used by cybercriminals to breach networks means that it's important to regularly test your organization's cyber security. VAPT helps to protect your organization by providing visibility of security weaknesses and guidance to address them. VAPT is increasingly important for organizations wanting to achieve compliance with standards including the GDPR, ISO 27001 and PCI DSS.

VAPT OBJECTIVES

⇒ Comprehensive security testing
⇒ Discover vulnerabilities of web app, internal, external network and other systems
⇒ Assist in meeting compliance requirements of Customer SAQ, PCI and GDPR

Introduction to nessus

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it.If you are an administrator in charge of any computer (or group of computers) connected to the internet, Nessus is a great tool help keep their domains free of the easy vulnerabilities that hackers and viruses commonly look to exploit.

To learn how Nessus and other port-scanning security tools work, it is necessary to understand different services (such as a web server, SMTP server, FTP server, etc) are accessed on a remote server. Most high-level network traffic, such as email, web pages, etc reach a server via a high-level protocol that is transmitted reliably by a TCP stream. To keep different streams from interfering with each other, a computer divides its physical connection to the network into thousands of logical paths, called ports. So if you want to talk to a web server on a given machine, you would connect to port #80 (the standard HTTP port), but if you wanted to connect to an SMTP server on that same machine you would instead connect to port #25.

Each computer has thousands of ports, all of which may or may not have services (ie: a server for a specific high-level protocol) listening on them. Nessus works by testing each port on a computer, determining what

service it is running, and then testing this service to make sure there are no vulnerabilities in it that could be used by a hacker to carry out a malicious attack. Nessus is called a "remote scanner" because it does not need to be installed on a computer for it to test that computer. Instead, you can install it on only one computer and test as many computers as you would like.

Vulnerability of host

192.168.0.100

CRITICAL HIGH MEDIUM LOW INFO

Scan Information

Start time: Thu Dec 16 00:22:34 2021

End time: Thu Dec 16 01:42:41 2021

Host Information

IP: 192.168.0.100

MAC Address: 00:2E:2D:63:1E:D2

Vulnerabilities

123643 - WP Google Maps for WordPress < 7.11.17 Unauthenticated SQL Injection (CVE-2019-10692)

Summary

The remote web server is running a PHP application that is affected by an unauthenticated SQL injection vulnerability.

Description

The WP Google Maps plugin for WordPress running on the remote web server is affected by an SQL injection
(SQL) vulnerability due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this to inject or manipulate SQL queries in the back-end database, resulting in the disclosure or manipulation of random data.

See Also

https://wpvulndb.com/vulnerabilities/9249

https://wordpress.org/plugins/wp-google-maps/

Solution

Upgrade the WP Google Maps plugin for WordPress to version 7.11.18 or later.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.8 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE CVE-2019-10692

Plugin Information

Published: 2019/04/03, Modified: 2019/10/30

Plugin Output

tcp/80
Nessus was able to exploit the issue using the following request :
GET
http://192.168.0.100//index.php?rest_route=/wpgmza/v1/markers/&filter=%7B%22nessus%22%3Atrue%7D&fields=user%28%29%20as%20user%5Fhostname%2Cversion%28%29%20as%20mysql%5Fversion%2Csysdate%28%29%20as%20nessus%5Fwas%5Fhere HTTP/1.1
Host: 192.168.0.100
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
This produced the following truncated output (limited to 10 lines) :

---------- snip ----------

[{"user_hostname":"wordpress@localhost","mysql_version":"10.1.41-

MariaDB-0+deb9u1","nessus_was_here":"2021-12-15 07:29:34"}]

---------- snip ----------

40984 - Browsable Web Directories

Summary

Some directories on the remote web server are browsable.

Description

Multiple Nessus plugins identified directories on the web server that are browsable.

See Also

http://www.nessus.org/u?0a35179e

Solution

Make sure that browsable directories do not leak confidential information or give access to sensitive resources.

Additionally, use access restrictions or disable directory indexing for any that do.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2009/09/15, Modified: 2021/01/19

Plugin Output

tcp/80

The following directories are browsable :

http://192.168.0.100/wp-includes/

http://192.168.0.100/wp-includes/css/

http://192.168.0.100/wp-includes/css/dist/

http://192.168.0.100/wp-includes/css/dist/block-library/

http://192.168.0.100/wp-includes/pomo/

http://192.168.0.100/wp-includes/random_compat/

http://192.168.0.100/wp-includes/rest-api/

http://192.168.0.100/wp-includes/sodium_compat/

90067 - WordPress User Enumeration

Summary

The remote web server contains a PHP application that is affected by an information disclosure vulnerability.

Description

The version of WordPress hosted on the remote web server is affected by a user enumeration vulnerability. An unauthenticated, remote attacker can exploit this to learn the names of valid WordPress users. This information could be used to mount further attacks.

See Also

https://hackertarget.com/wordpress-user-enumeration/

Solution

n/a

Risk Factor

Medium

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2016/03/21, Modified: 2018/05/16

Plugin Output

tcp/80

Nessus was able to enumerate the following WordPress users from the WordPress install at 'http://192.168.0.100/' :

Webmaster

26194 - Web Server Transmits Clear text Credentials

Summary

The remote web server might transmit credentials in clear text.

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in clear text. An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

XREF CWE:522

XREF CWE:523

XREF CWE:718

XREF CWE:724

XREF CWE:928

XREF CWE:930

Plugin Information

Published: 2007/09/28, Modified: 2016/11/29

Plugin Output

tcp/80

Page : /wp-login.php
Destination Page: /wp-login.php

48204 - Apache HTTP Server Version

Summary

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2020/09/22

Plugin Output

tcp/80

URL : http://192.168.0.100/
Version : 2.4.99
backported : 1
os : ConvertedDebian

39520 - Backported Security Patch Detection (SSH)

Summary

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

Give Nessus credentials to perform local checks.

39521 - Backported Security Patch Detection (WWW)

Summary

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number. Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/80

Give Nessus credentials to perform local checks.

45590 - Common Platform Enumeration (CPE)

Summary

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2021/12/08

Plugin Output

tcp/0

Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.4.25 -> Apache Software Foundation Apache HTTP Server 2.4.25

cpe:/a:apache:http_server:2.4.99

cpe:/a:jquery:jquery:1.12.4

cpe:/a:openbsd:openssh:7.4 -> OpenBSD OpenSSH 7.4

cpe:/a:wordpress:wordpress:5.2.3

85602 - Web Application Cookies Not Marked Secure

Summary

HTTP session cookies might be transmitted in cleartext.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticate session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Note that this plugin detects all general cookies missing the 'secure' cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

See Also

https://www.owasp.org/index.php/SecureFlag

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision. If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

Risk Factor

None

References

XREF CWE:522

XREF CWE:718

XREF CWE:724

XREF CWE:928

XREF CWE:930

Plugin Information

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/80
The following cookie does not set the secure cookie flag :
Name : wordpress_test_cookie
Path : /
Value : WP+Cookie+check
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :

10114 - ICMP Timestamp Request Remote Date Disclosure

Summary

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols. Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

CVSS v3.0 Base Score

0.0 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

CVSS v2.0 Base Score

0.0 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:N)

References

CVE CVE-1999-0524

XREF CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2019/10/04

Plugin Output

icmp/0

The difference between the local and remote clocks is 43182 seconds.

66334 - Patch Report

Summary

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2021/11/09

Plugin Output

tcp/0

. You need to take the following action :

[WP Google Maps for WordPress < 7.11.17 Unauthenticated SQL Injection (CVE-2019-10692) (123643)]

+ Action to take : Upgrade the WP Google Maps plugin for WordPress to version 7.11.18 or later.