رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Day: Tuesday

Date: 22/10/2024

AMIT

Vulnerability Assessment and remediation report

Prepared by:

Osama Ahmed Montaser

Instructor:

Eng. Mohamed Ammar

Table of Contents

1. Technical Summary

- **Company**: Purple Amit
- **IP Address:** 192.168.50.7
- **Scope**: Web Application and Web Server
- **Tools Used**: WPScan, Nmap, Nikto, Nessus

2. Executive Summary

2.1. Date Range of the Assessment

The vulnerability assessment was conducted between **October 21, 2024**, and **October 22, 2024**

2.2. Purpose and Scope of the Assessment

The primary purpose of this assessment was to identify vulnerabilities in Purple Amit's infrastructure following a recent data breach. The goal was to assess the organization's current security posture and provide actionable recommendations to mitigate the risks discovered. The assessment focused on both web applications and web servers, utilizing multiple tools to conduct thorough scans across relevant systems.

2.3. General Status of Assessment and Summary of Findings

The assessment identified several vulnerabilities across the infrastructure, categorized by their severity: critical, high, medium, and low. The most critical findings include an outdated and vulnerable version of OpenSSH that allows remote code execution, exposure of sensitive backup files, and improperly configured HTTP methods. These vulnerabilities, if left unresolved, could lead to further exploitation, unauthorized access, or data loss.

2.4. Disclaimer

This report presents a comprehensive analysis based on the tools and methodologies used during the assessment. The findings and recommendations are based on the systems and services that were accessible during the scanning period. It is the responsibility of the client to ensure continuous monitoring and patching of any newly discovered vulnerabilities in the future.

3. Scan Results

3.1. Explanation of the Scan Results

The vulnerability scan was conducted using four primary tools: **Nmap**, **WPScan**, **Nikto**, and **Nessus**. These tools were used to identify vulnerabilities across the client's web server and web application. The vulnerabilities identified were classified based on their potential impact and exploitability.

- **Critical:** Requires immediate action to prevent severe risks like remote code execution.
- **High:** High-priority issues that expose sensitive data or weaken the system significantly.
- **Medium:** Moderate risk, usually requiring specific conditions for exploitation.
- **Low:** Low-risk issues often related to misconfigurations that do not pose immediate threats.

3.2. Overview of the Types of Reports Provided

- **Nmap:** Scanned for open ports, services, and known vulnerabilities based on the software versions detected.
- **WPScan:** Focused on identifying vulnerabilities within the WordPress installation, including exposed files and user enumeration.
- **Nikto:** Identified web server misconfigurations and missing security headers.
- **Nessus:** Provided a comprehensive vulnerability scan, detecting network and application-based vulnerabilities. Detailed results of the Nessus scan are provided in the **Appendix**.

4. Methodology

4.1. Tools and Tests Used for Vulnerability Scanning

- **Nmap:** Used to detect open ports, running services, and service versions, followed by scanning for vulnerabilities associated with those services.
- **WPScan:** Focused on WordPress-specific vulnerabilities, such as plugin and theme issues, user enumeration, and backup file exposure.
- **Nikto:** Scanned the web server for misconfigurations, security-related headers, and directory indexing issues.
- **Nessus:** A comprehensive tool for identifying both network and application vulnerabilities. Nessus provided a deeper analysis of potential threats, configuration issues, and exposures, covering a broader range of vulnerabilities.

4.2. Specific Purpose of Each Scan, Tool, and Test

- **Nmap:** Identified the exposed services and their respective vulnerabilities, focusing on services like SSH and HTTP.
- **WPScan:** Scanned for WordPress-specific weaknesses that could lead to a breach or unauthorized access.
- **Nikto:** Inspected the web server for common misconfigurations, missing security headers, and other security issues.
- **Nessus:** Identified vulnerabilities across the network and application layers, including missing patches, misconfigurations, and weak security settings.

4.3. Testing Environments for Each Tool Used

The assessment was performed on the web application hosted at 192.168.50.7. Both the HTTP service running on port 80 and the SSH service running on port 22 were scanned for vulnerability. The WordPress installation and underlying Apache web server were the primary targets for application and host-based assessments.

5. Findings

5.1. Systems Scanned

- **Web Server:** Apache 2.4.62 (CentOS Stream)
- **WordPress Application:** Hosted on the web server
- **SSH Service:** OpenSSH 8.7 (CentOS Stream)

All identified systems were successfully scanned, and no systems were left unscanned or inaccessible during the assessment.

5.2. Index of Vulnerabilities Identified

Risk Level	Number of Vulnerabilities
Critical Vulnerability	1
High Vulnerability	3
Medium Vulnerability	6
Low Vulnerability	3

5.3. Explanation of the Above Risk Categories

- **Critical vulnerabilities** pose immediate and severe risks and must be addressed immediately.
- **High vulnerabilities** expose sensitive data or have the potential for significant security impact.
- **Medium vulnerabilities** are potentially exploitable but require certain conditions to succeed.
- **Low vulnerabilities** pose minimal risk but should still be addressed for overall security posture improvement.
-

5.4. Details on Vulnerabilities

Vulnerability	Category	Risk Level	CVSS Score	Impact	Remediation
OpenSSH 8.7 Remote Code Execution (CVE-2023-38408)	Host-Based	Critical	**10**	Exploiting this can lead to full system compromise, allowing attackers to gain remote access.	Update OpenSSH to the latest version, disable password-based login, and implement key-based authentication.

Backup Directory Exposure	Application-Based	High	**7.5**	Exposing the backup directory allows attackers to access sensitive data like database backups.	Disable directory listing, restrict access using .htaccess, or move the backups outside the web root.
HTTP TRACE Method Enabled (XST)	Host-Based	High	**7.5**	Can lead to session hijacking and exposure of sensitive information via Cross-Site Tracing (XST).	Disable HTTP TRACE method in Apache (TraceEnable Off).
XML-RPC Enabled	Application-Based	High	**7.1**	XML-RPC can be abused for brute-force and DDoS attacks, as well as data theft.	Disable XML-RPC if not needed, or restrict its use via security plugins.

Missing Security Headers (X-Frame-Options, X-Content-Type-Options, X-XSS-Protection)	Host-Based	Medium	**6.8**	Absence of key headers makes the site vulnerable to clickjacking, XSS, and MIME sniffing attacks.	Add X-Frame-Options, X-Content-Type-Options, and X-XSS-Protection headers to the server configuration.
User Enumeration via WordPress REST API	Application-Based	Medium	**5.3**	Allows attackers to enumerate valid usernames, facilitating brute-force attacks.	Disable user enumeration via plugins or restrict access to REST API.
Directory Indexing in /icons/	Host-Based	Medium	**5.3**	Directory indexing allows attackers to view files, which can lead to sensitive data exposure.	Disable directory listing by adding Options -Indexes to your Apache configuration.

Public Backup and Configuration Exposure (Potential Backup and User Directory Browsing)	Application-Based	Medium	**5**	Exposes sensitive files like configuration backups, which can lead to server compromise.	Restrict access to backup/config files, and move them outside web-accessible directories.
Missing HTTPS (SSL/TLS)	Host-Based	Medium	**5**	All traffic is transmitted in cleartext, making it vulnerable to MITM attacks and eavesdropping.	Enable HTTPS and enforce redirection from HTTP to HTTPS.

Directory Listing in /wp-content/uploads/	Application-Based	Medium	**5**	Allows attackers to view and access uploaded files, which may include sensitive information.	Disable directory listing in the uploads directory using .htaccess or server configuration.
WordPress Readme File Found	Application-Based	Low	**3.7**	Exposing the WordPress readme file reveals unnecessary information about the WordPress version.	Remove the readme file or restrict access using .htaccess.

WordPress Registration Enabled	Application-Based	Low	**3.5**	Allows the creation of spam or malicious accounts, especially if user roles are misconfigured.	Disable registration if unnecessary or implement CAPTCHA and email verification for new registrations.
robots.txt Contains Sensitive Entries	Application-Based	Low	**3.2**	Attackers can gather information about the site's structure and sensitive directories.	Remove sensitive entries from robots.txt or restrict access using server configuration.

6. Risk Assessment

The vulnerabilities are categorized based on the **Common Vulnerability Scoring System (CVSS)**, providing a clear view of the most critical threats to the organization’s security.

A total of **13 vulnerabilities** were identified:

- **Critical:** 1
- **High:** 3
- **Medium:** 6
- **Low:** 3

The client should focus on remediating the **critical and high** vulnerabilities first, as these represent the most significant risks, including remote code execution and exposure of sensitive data.

7. Recommendations

Based on the vulnerabilities identified during the assessment, the following actions are recommended:

1. Immediate Patching:

- **Update OpenSSH** to the latest version to prevent remote code execution.
- **Disable the HTTP TRACE method** to avoid session hijacking attacks.
- **Remove or secure the backup directory** to protect sensitive data from unauthorized access.

2. Reinforce Web Security:

- **Add security headers**: Implement `X-Frame-Options`, `X-Content-Type-Options`, and `X-XSS-Protection` to protect the web server from common attacks such as clickjacking, MIME sniffing, and cross-site scripting (XSS).
- **Implement HTTPS** across the entire site to encrypt communications and ensure user data is protected from interception.

3. WordPress Hardening:

- **Disable XML-RPC** or restrict its use to trusted services to avoid brute-force and DDoS attacks.
- **Prevent user enumeration** through the REST API by using security plugins.
- **Disable unnecessary features** such as user registration or protect registration forms with CAPTCHAs to prevent spam and unauthorized user creation.

4. Ongoing Monitoring and Tools:

- **Deploy an IPS/IDS (Intrusion Prevention System/Intrusion Detection System):** Implement an IPS/IDS to monitor traffic for malicious activity and block or alert on detected threats in real-time.
- **Implement a SIEM (Security Information and Event Management) Solution:** Use a SIEM solution to aggregate and analyze logs from various sources across your network. This will help detect suspicious activity, identify persistent threats, and respond to potential incidents.
- **Use continuous vulnerability scanning tools** such as **Nessus** or **OpenVAS** to regularly check for new vulnerabilities in the network and applications.
- **Enforce strict file access permissions** to ensure that only authorized users can access sensitive files and directories.

5. Policy and Configuration Adjustments:

- **Update the robots.txt file** to remove sensitive directories (e.g., `/wp-admin/`) to limit exposure to attackers.
- **Establish a regular patch management policy** to ensure that all software and services are updated promptly with the latest security patches.
- **Encrypt and securely store backups** to protect them from unauthorized access. Ensure that backup files are not accessible via the public web and are stored in secure, off-site locations.

8. Appendices

8.1. Web Application scanning

Webserver Scanning

Report generated by Tenable Nessus™ Tue, 22 Oct 2024 05:53:39 EDT

TABLE OF CONTENTS

Vulnerabilities by Plugin

Vulnerabilities by Plugin

58987 (1) - PHP Unsupported Version Detection

Synopsis

The remote host contains an unsupported version of a web application scripting language.

Description

According to its version, the installation of PHP on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

http://php.net/eol.php

https://wiki.php.net/rfc/releaseprocess

Solution

Upgrade to a version of PHP that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF IAVA:0001-A-0581

Plugin Information

Published: 2012/05/04, Modified: 2024/05/31

Plugin Output

192.168.50.7 (tcp/80/www)

```
  Source              : X-Powered-By: PHP/8.0.30
```

```
  Installed version   : 8.0.30
  End of support date : 2023/11/26
  Announcement        : http://php.net/supported-versions.php
  Supported versions  : 8.1.x / 8.2.x / 8.3.x
```

42424 (1) - CGI Generic SQL Injection (blind)

Synopsis

A CGI application hosted on the remote web server is potentially prone to SQL injection attack.

Description

By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a very different response, which suggests that it may have been able to modify the behavior of the application and directly access the underlying database.

An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.

See Also

http://www.securiteam.com/securityreviews/5DP0N1P76E.html

http://www.nessus.org/u?ed792cf5

http://www.nessus.org/u?11ab1866

Solution

Modify the affected CGI scripts so that they properly escape arguments.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	CWE:20
XREF	CWE:77
XREF	CWE:89
XREF	CWE:91
XREF	CWE:203
XREF	CWE:643
XREF	CWE:713

XREF	CWE:722
XREF	CWE:727
XREF	CWE:751
XREF	CWE:801
XREF	CWE:810
XREF	CWE:928
XREF	CWE:929

Plugin Information

Published: 2009/11/06, Modified: 2024/06/14

Plugin Output

192.168.50.7 (tcp/80/www)

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to blind SQL injection :

+ The 'woocommerce-login-nonce' parameter of the /my-account/ CGI :

/my-account/?_wp_http_referer=%2fmy-account%2f&username=&rememberme=fore
ver&password=&woocommerce-login-nonce=fdda44f10ezz%2fmy-account%2f&usern
ame=&rememberme=forever&password=&woocommerce-login-nonce=fdda44f10eyy

-------- output --------
<script type="text/javascript" id="lpData">
/* <![CDATA[ */
var lpData = {"site_url":"http:\/\/192.168.50.7","user_id":"0","theme":"
tutorstarter","lp_rest_url":"http:\/\/192.168.50.7\/wp-json\/","nonce":"
23987ba727","is_course_archive":"","courses_url":"http:\/\/192.168.50.7\
/courses\/","urlParams":{"_wp_http_referer":"\/my-account\/","user [...]
/* ]]> */
</script>
-------- vs --------
<script type="text/javascript" id="lpData">
/* <![CDATA[ */
var lpData = {"site_url":"http:\/\/192.168.50.7","user_id":"0","theme":"
tutorstarter","lp_rest_url":"http:\/\/192.168.50.7\/wp-json\/","nonce":"
23987ba727","is_course_archive":"","courses_url":"http:\/\/192.168.50.7\
/courses\/","urlParams":{"_wp_http_referer":"\/my-account\/","user [...]
/* ]]> */
</script>
------------------------

+ The 'username' parameter of the /my-account/ CGI :

/my-account/?_wp_http_referer=%2fmy-account%2f&woocommerce-login-nonce=f
dda44f10e&rememberme=forever&password=&username=zz%2fmy-account%2f&wooco
mmerce-login-nonce=fdda44f10e&rememberme=forever&password=&username=yy

-------- output --------
<script type="text/javascript" id="lpData">
/* <![CDATA[ */
var lpData = {"site_url":"http:\/\/192.168.50.7","user_id":"0","theme":"
tutorstarter","lp_rest_url":"http:\/\/192.168.50.7\/wp-json\/","nonce":"
23987ba727","is_course_archive":"","courses_url":"http:\/\/192.168.50.7\
/courses\/","urlParams":{"_wp_http_referer":"\/my-account\/","wooc [...]
/* ]]> */
```

```
</script>
-------- vs --------
<script type="text/javascript" id="lpData">
/* <![CDATA[ */
var lpData = {"site_url":"http:\/\/192.168.50.7","user_id":"0","theme":"
 [...]
```

11213 (1) - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

http://www.nessus.org/u?e979b5cb

http://www.apacheweek.com/issues/03-01-24

https://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these HTTP methods. Refer to the plugin output for more information.

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 v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

4.0

EPSS Score

0.0058

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information

Published: 2003/01/23, Modified: 2024/04/09

Plugin Output

192.168.50.7 (tcp/80/www)

```
To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request : \n\n------------------------------ snip
 ------------------------------\nTRACE /Nessus728647151.html HTTP/1.1
Connection: Close
Host: 192.168.50.7
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------\n\nand received the
 following response from the remote server :\n\n------------------------------ snip
 ------------------------------\nHTTP/1.1 200 OK
Date: Tue, 22 Oct 2024 08:13:49 GMT
Server: Apache/2.4.62 (CentOS Stream)
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http
```

```
TRACE /Nessus728647151.html HTTP/1.1
Connection: Keep-Alive
Host: 192.168.50.7
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------\n
```

40984 (1) - Browsable Web Directories

Synopsis

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

192.168.50.7 (tcp/80/www)

```
The following directories are browsable :

http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/
http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/
http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/css/
http://192.168.50.7/wp-content/plugins/elementor/
http://192.168.50.7/wp-content/plugins/elementor/app/
http://192.168.50.7/wp-content/plugins/elementor/assets/
http://192.168.50.7/wp-content/plugins/elementor/assets/css/
http://192.168.50.7/wp-content/plugins/elementor/assets/data/
http://192.168.50.7/wp-content/plugins/elementor/assets/images/
```

```
http://192.168.50.7/wp-content/plugins/elementor/assets/js/
http://192.168.50.7/wp-content/plugins/elementor/assets/lib/
http://192.168.50.7/wp-content/plugins/elementor/assets/mask-shapes/
http://192.168.50.7/wp-content/plugins/elementor/assets/shapes/
http://192.168.50.7/wp-content/plugins/elementor/assets/svg-paths/
http://192.168.50.7/wp-content/plugins/elementor/core/
http://192.168.50.7/wp-content/plugins/elementor/data/
http://192.168.50.7/wp-content/plugins/elementor/includes/
http://192.168.50.7/wp-content/plugins/elementor/modules/
http://192.168.50.7/wp-content/plugins/learnpress/assets/
http://192.168.50.7/wp-content/plugins/learnpress/assets/css/
http://192.168.50.7/wp-content/plugins/learnpress/assets/src/
http://192.168.50.7/wp-content/plugins/woocommerce/
http://192.168.50.7/wp-content/plugins/woocommerce/assets/
http://192.168.50.7/wp-content/plugins/woocommerce/assets/client/
http://192.168.50.7/wp-content/plugins/woocommerce/assets/css/
http://192.168.50.7/wp-content/plugins/woocommerce/assets/fonts/
http://192.168.50.7/wp-content/plugins/woocommerce/assets/images/
http://192.168.50.7/wp-content/plugins/woocommerce/assets/js/
http://192.168.50.7/wp-content/plugins/woocommerce/client/
http://192.168.50.7/wp-content/plugins/woocommerce/client/admin/
http://192.168.50.7/wp-content/plugins/woocommerce/i18n/
http://192.168.50.7/wp-content/plugins/woocommerce/i18n/languages/
http:/ [...]
```

85582 (1) - Web Application Potentially Vulnerable to Clickjacking

Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

See Also

http://www.nessus.org/u?399b1f56

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

https://en.wikipedia.org/wiki/Clickjacking

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.

This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

XREF CWE:693

Plugin Information

Published: 2015/08/22, Modified: 2017/05/16

Plugin Output

192.168.50.7 (tcp/80/www)

```
The following pages do not use a clickjacking mitigation response header and contain a clickable
 event :

  - http://192.168.50.7/
  - http://192.168.50.7/about-us/
  - http://192.168.50.7/blog/
  - http://192.168.50.7/cart/
  - http://192.168.50.7/contact-us/
  - http://192.168.50.7/course-category/embedded-system/
  - http://192.168.50.7/course-category/programming/
  - http://192.168.50.7/course-category/security/
  - http://192.168.50.7/courses/
  - http://192.168.50.7/courses/cybersecurity-diploma-soc/
  - http://192.168.50.7/courses/embedded-systems-diploma/
  - http://192.168.50.7/courses/flutter-diploma/
  - http://192.168.50.7/courses/full-stack-nodejs-diploma/
  - http://192.168.50.7/employment/
  - http://192.168.50.7/instructor-registration/
  - http://192.168.50.7/instructor/amit_admin/
  - http://192.168.50.7/shop/
```

90067 (1) - WordPress User Enumeration

Synopsis

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: 2024/06/05

Plugin Output

192.168.50.7 (tcp/80/www)

```
Nessus was able to enumerate the following WordPress users from the WordPress install at
 'http://192.168.50.7/' :
 amit
 user1
```

10114 (1) - ICMP Timestamp Request Remote Date Disclosure

Synopsis

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

Low

VPR Score

4.2

EPSS Score

0.8808

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

Plugin Output

192.168.50.7 (icmp/0)

```
The remote clock is synchronized with the local clock.
```

11219 (2) - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

192.168.50.7 (tcp/22/ssh)

```
Port 22/tcp was found to be open
```

192.168.50.7 (tcp/80/www)

```
Port 80/tcp was found to be open
```

22964 (2) - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

192.168.50.7 (tcp/22/ssh)

```
An SSH server is running on this port.
```

192.168.50.7 (tcp/80/www)

```
A web server is running on this port.
```

10107 (1) - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

192.168.50.7 (tcp/80/www)

```
The remote web server type is :

Apache/2.4.62 (CentOS Stream)
```

10267 (1) - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

Plugin Output

192.168.50.7 (tcp/22/ssh)

```
SSH version : SSH-2.0-OpenSSH_8.7
SSH supported authentication : publickey,gssapi-keyex,gssapi-with-mic,password
```

10287 (1) - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

192.168.50.7 (udp/0)

```
For your information, here is the traceroute from 192.168.50.9 to 192.168.50.7 :
192.168.50.9
192.168.50.7

Hop Count: 1
```

10302 (1) - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

192.168.50.7 (tcp/80/www)

```
Contents of robots.txt :

User-agent: *
Disallow: /wp-content/uploads/wc-logs/
Disallow: /wp-content/uploads/woocommerce_transient_files/
Disallow: /wp-content/uploads/woocommerce_uploads/
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php

Sitemap: http://192.168.50.7/wp-sitemap.xml
```

10662 (1) - Web mirroring

Synopsis

Nessus can crawl the remote website.

Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/05/04, Modified: 2024/07/17

Plugin Output

192.168.50.7 (tcp/80/www)

```
Webmirror performed 1000 queries in 46s (21.0739 queries per second)

The following CGIs have been discovered :


+ CGI : /xmlrpc.php
  Methods : GET
  Argument :
   Value: rsd


+ CGI : /wp-json/oembed/1.0/embed
  Methods : GET
  Argument : format
   Value: xml
  Argument : url
   Value: http%3A%2F%2F192.168.50.7%2Fcart%2F


+ CGI : /
  Methods : GET
  Argument : p
   Value: 253
  Argument : s
```

```
+ CGI : /my-account/
  Methods : POST
  Argument : _wp_http_referer
   Value: /my-account/
  Argument : password
  Argument : rememberme
   Value: forever
  Argument : username
  Argument : woocommerce-login-nonce
   Value: fdda44f10e


+ CGI : /courses/cybersecurity-diploma-soc/
  Methods : POST
  Argument : purchase-course
   Value: 196


+ CGI : /courses/embedded-systems-diploma/
  Methods : POST
  Argument : purchase-course
   Value: 423


+ CGI : /courses/flutter-diploma/
  Methods : POST
  Argument : purchase-course
   Value: 307


+ CGI : /courses/full-stack-nodejs-diploma/
  Methods : POST
  Argument : purchase-course
   Value: 360


+ CGI : /my-account/lost-password/
  Methods : POST
  Argument : _wp_http_referer
   Value: /my-account/lost-password/
  Argument : user_login
  Argument : wc_reset_password
   Value: true
  Argument : woocommerce-lost-password-nonce
   Value: 3ca0703145

Directory index found at /wp-content/plugins/woocommerce/assets/css/
Directory index found at /wp-content/plugins/woocommerce/assets/
Directory index found at /wp-content/plugins/woocommerce/
Directory index found at /wp-content/plugins/elementor/assets/css/
Directory index found at /wp-content/plugins/elementor/assets/
Directory index found at /wp-content/plugins/elementor/
Directory index found at /wp-content/uploads/elementor/css/
Directory index found at /wp-content/uploads/elementor/
Directory index found at /wp-content/uploads/
Directory index found at /wp-content/plugins/learnpress/assets/css/
Directory index found at /wp-content/plugins/learnpress/assets/
Directory index found at /wp-content/uploads/2024/10/
Directory index [...]
```

10881 (1) - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2024/07/24

Plugin Output

192.168.50.7 (tcp/22/ssh)

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

11032 (1) - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

Solution

n/a

Risk Factor

None

References

XREF OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2024/06/07

Plugin Output

192.168.50.7 (tcp/80/www)

```
The following directories were discovered:
/cgi-bin, /cart, /icons, /shop, /blog

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

11419 (1) - Web Server Office File Inventory

Synopsis

The remote web server hosts office-related files.

Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Risk Factor

None

Plugin Information

Published: 2003/03/19, Modified: 2022/04/11

Plugin Output

192.168.50.7 (tcp/80/www)

```
The following office-related files are available on the remote server :

  - CSV Spreadsheet files (.csv) :
    /wp-content/plugins/woocommerce/sample-data/experimental_fashion_sample_9_products.csv
    /wp-content/plugins/woocommerce/sample-data/experimental_sample_9_products.csv
    /wp-content/plugins/woocommerce/sample-data/sample_products.csv
    /wp-content/plugins/woocommerce/sample-data/sample_tax_rates.csv
```

11936 (1) - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2024/10/14

Plugin Output

192.168.50.7 (tcp/0)

```
Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP


The remote host is running Linux Kernel 2.6
```

18297 (1) - WordPress Detection

Synopsis

The remote web server contains a blog application written in PHP.

Description

The remote host is running WordPress, a free blog application written in PHP with a MySQL back-end.

See Also

https://wordpress.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0747

Plugin Information

Published: 2005/05/18, Modified: 2023/05/24

Plugin Output

192.168.50.7 (tcp/80/www)

```
Nessus detected 2 installs of WordPress:

  URL     : http://192.168.50.7/
  Version : 6.6.2

  URL     : http://192.168.50.7/blog
  Version : 6.6.2
```

19506 (1) - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/10/04

Plugin Output

192.168.50.7 (tcp/0)

```
Information about this scan :

Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202410212332
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
```

```
Scan name : Webserver Scanning
Scan policy used : Basic Network Scan
Scanner IP : 192.168.50.9
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 171.282 ms
Thorough tests : yes
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : all_pairs
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 10 minutes.
Web app tests -  Stop at first flaw : param
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/10/22 4:05 EDT
Scan duration : 6462 sec
Scan for malware : no
```

24260 (1) - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

192.168.50.7 (tcp/80/www)

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Tue, 22 Oct 2024 08:44:02 GMT
  Server: Apache/2.4.62 (CentOS Stream)
  X-Powered-By: PHP/8.0.30
  Link: <http://192.168.50.7/wp-json/>; rel="https://api.w.org/", <http://192.168.50.7/wp-json/
wp/v2/pages/511>; rel="alternate"; title="JSON"; type="application/json", <http://192.168.50.7/>;
 rel=shortlink
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Transfer-Encoding: chunked
  Content-Type: text/html; charset=UTF-8

Response Body :

<!DOCTYPE html>
<html lang="en-US">
```

```
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="profile" href="http://gmpg.org/xfn/11">
<link rel="pingback" href="http://192.168.50.7/xmlrpc.php">
<script type="text/javascript" id="lpData">
/* <![CDATA[ */
var lpData = {"site_url":"http:\/
\/192.168.50.7","user_id":"0","theme":"tutorstarter","lp_rest_url":"http:\/\/192.168.50.7\/wp-
json\/","nonce":"23987ba727","is_course_archive":"","courses_url":"http:\/\/192.168.50.7\/courses
\/","urlParams":[],"lp_version":"4.2.7","lp_rest_load_ajax":"http:\/\/192.168.50.7\/wp-json\/lp\/
v1\/load_content_via_ajax\/"};
/* ]]> */
</script>
<style id="learn-press-custom-css">
:root {
--lp-container-max-width: 1290px;
--lp-cotainer-padding: 1rem;
--lp-primary-color: #ffb606;
--lp-secondary-color: #442e66;
}
</style>
<title>AMIT Learning &#8211; Best IT learning Platform Online/Offline</title>
<meta name='robots' content='max-image-preview:large' />
<link rel='dns-prefetch' href='//fonts.googleapis.com' />
<link rel="alternate" type="application/rss+xml" title="AMIT Learning &raquo; Feed"
 href="http://192.168.50.7/feed/" />
<link rel="alternate" type="application/rss+xml" title="AMIT Learning &raquo; Comments Feed"
 href="http://192.168.50.7/comments/feed/" />
<script type="text/javascript">
/* <![CDATA[ */
window._wpem [...]
```

25220 (1) - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

192.168.50.7 (tcp/0)

33817 (1) - CGI Generic Tests Load Estimation (all tests)

Synopsis

Load estimation for web application tests.

Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.

The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.

Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/26, Modified: 2022/04/11

Plugin Output

192.168.50.7 (tcp/80/www)

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

on site request forgery                  : S=15         SP=15        AP=27        SC=4         AC=30

SQL injection                            : S=476        SP=476       AP=812       SC=112
 AC=896
unseen parameters                        : S=595        SP=595       AP=1015      SC=140
 AC=1120
local file inclusion                     : S=68         SP=68        AP=116       SC=16
 AC=128
web code injection                       : S=17         SP=17        AP=29        SC=4         AC=32

XML injection                            : S=17         SP=17        AP=29        SC=4         AC=32

format string                            : S=34         SP=34        AP=58        SC=8         AC=64

script injection                         : S=15         SP=15        AP=27        SC=4         AC=30

cross-site scripting (comprehensive test): S=289        SP=289       AP=493       SC=68
 AC=544
```

```
injectable parameter                        : S=34          SP=34         AP=58         SC=8          AC=64

cross-site scripting (extended patterns) : S=90          SP=90         AP=162        SC=24
 AC=180
directory traversal (write access)       : S=34          SP=34         AP=58         SC=8          AC=64

SSI injection                               : S=51          SP=51         AP=87         SC=12         AC=96

header injection                            : S=30          SP=30         AP=54         SC=8          AC=60

HTML injection                              : S=75          SP=75         AP=135        SC=20
 AC=150
directory traversal                         : S=493         SP=493        AP=841        SC=116
 AC=928
arbitrary command execution (time based) : S=102         SP=102        AP=174        SC=24
 AC=192
persistent XSS                           [...]
```

35716 (1) - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

192.168.50.7 (tcp/0)

```
The following card manufacturers were identified :

08:00:27:DA:90:BA : PCS Systemtechnik GmbH
```

39470 (1) - CGI Generic Tests Timeout

Synopsis

Some generic CGI attacks ran out of time.

Description

Some generic CGI tests ran out of time during the scan. The results may be incomplete.

Solution

Consider increasing the 'maximum run time (minutes)' preference for the 'Web Applications Settings' in order to prevent the CGI scanning from timing out. Less ambitious options could also be used, such as :

- Test more that one parameter at a time per form :

'Test all combinations of parameters' is much slower than 'Test random pairs of parameters' or 'Test all pairs of parameters (slow)'.

- 'Stop after one flaw is found per web server (fastest)'

under 'Do not stop after the first flaw is found per web page' is quicker than 'Look for all flaws (slowest)'.

- In the Settings/Advanced menu, try reducing the value for 'Max number of concurrent TCP sessions per host' or 'Max simultaneous checks per host'.

Risk Factor

None

Plugin Information

Published: 2009/06/19, Modified: 2021/01/19

Plugin Output

192.168.50.7 (tcp/80/www)

```
The following tests timed out without finding any flaw :
- HTML injection
- directory traversal (extended test)
- directory traversal
- arbitrary command execution
- SQL injection
- web code injection
- uncontrolled redirection
- cross-site scripting (extended patterns)
- cross-site scripting (comprehensive test)
```

39520 (1) - Backported Security Patch Detection (SSH)

Synopsis

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

192.168.50.7 (tcp/22/ssh)

```
Give Nessus credentials to perform local checks.
```

40773 (1) - Web Application Potentially Sensitive CGI Parameter Detection

Synopsis

An application was found that may use CGI parameters to control sensitive information.

Description

According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. These parameters should be examined to determine what type of data is controlled and if it poses a security risk.

** This plugin only reports information that may be useful for auditors

** or pen-testers, not a real flaw.

Solution

Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.

Risk Factor

None

Plugin Information

Published: 2009/08/25, Modified: 2021/01/19

Plugin Output

192.168.50.7 (tcp/80/www)

```
Potentially sensitive parameters for CGI /my-account/ :

password : Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack
```

43111 (1) - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

192.168.50.7 (tcp/80/www)

```
Based on the response to an OPTIONS request :

  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /icons


Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT COPY DEBUG DELETE GET HEAD INDEX
    LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS
    ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /
    /about-us
    /blog
    /cart
    /cgi-bin
    /comments/feed
    /contact-us
    /course-category/embedded-system
    /course-category/embedded-system/feed
    /course-category/programming
    /course-category/programming/feed
    /course-category/security
    /course-category/security/feed
    /courses
    /courses/cybersecurity-diploma-soc
    /courses/embedded-systems-diploma
    /courses/flutter-diploma
    /courses/full-stack-nodejs-diploma
    /shop

  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /icons

  - Invalid/unknown HTTP methods are allowed on :

    /
    /about-us
    /blog
    /cart
    /cgi-bin
    /comments/feed
    /contact-us
    /course-category/embedded-system
    /course-category/embedded-system/feed
    /course-category/programming
    /course-category/programming/feed
    /course-category/security
    /course-category/security/feed
    /courses
    /courses/cybersecurity-diploma-soc
    /courses/embedded-systems-diploma
    /courses/flutter-diploma
    /courses/full-stack-nodejs-diploma
    /shop
```

45590 (1) - Common Platform Enumeration (CPE)

Synopsis

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: 2024/10/10

Plugin Output

192.168.50.7 (tcp/0)

```
The remote operating system matched the following CPE :

  cpe:/o:linux:linux_kernel -> Linux Kernel

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.4.62 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:jquery:jquery:3.7.1 -> jQuery
  cpe:/a:openbsd:openssh:8.7 -> OpenBSD OpenSSH
  cpe:/a:php:php:8.0.30 -> PHP PHP
  cpe:/a:wordpress:wordpress:6.6.2 -> WordPress
```

47830 (1) - CGI Generic Injectable Parameter

Synopsis

Some CGIs are candidate for extended injection tests.

Description

Nessus was able to to inject innocuous strings into CGI parameters and read them back in the HTTP response.

The affected parameters are candidates for extended injection tests like cross-site scripting attacks.

This is not a weakness per se, the main purpose of this test is to speed up other scripts. The results may be useful for a human pen-tester.

Solution

n/a

Risk Factor

None

References

XREF CWE:86

Plugin Information

Published: 2010/07/26, Modified: 2021/01/19

Plugin Output

192.168.50.7 (tcp/80/www)

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to injectable parameter :

+ The 'purchase-course' parameter of the /courses/full-stack-nodejs-diploma/ CGI :

/courses/full-stack-nodejs-diploma/?purchase-course=%00ztfpjh

-------- output --------
<script type="text/javascript" id="lpData">
/* <![CDATA[ */
var lpData = {"site_url":"http:\/\/192.168.50.7","user_id":"0","theme":"
tutorstarter","lp_rest_url":"http:\/\/192.168.50.7\/wp-json\/","nonce":"
23987ba727","is_course_archive":"","courses_url":"http:\/\/192.168.50.7\
/courses\/","urlParams":{"purchase-course":"ztfpjh"},"lp_version":"4.2.7
","lp_rest_load_ajax":"http:\/\/192.168.50.7\/wp-json\/lp\/v1\/load_cont
```

```
ent_via_ajax\/"};
/* ]]> */
</script>
-------------------------

+ The 'purchase-course' parameter of the /courses/flutter-diploma/ CGI :

/courses/flutter-diploma/?purchase-course=%00ztfpjh

-------- output --------
<script type="text/javascript" id="lpData">
/* <![CDATA[ */
var lpData = {"site_url":"http:\/\/192.168.50.7","user_id":"0","theme":"
tutorstarter","lp_rest_url":"http:\/\/192.168.50.7\/wp-json\/","nonce":"
23987ba727","is_course_archive":"","courses_url":"http:\/\/192.168.50.7\
/courses\/","urlParams":{"purchase-course":"ztfpjh"},"lp_version":"4.2.7
","lp_rest_load_ajax":"http:\/\/192.168.50.7\/wp-json\/lp\/v1\/load_cont
ent_via_ajax\/"};
/* ]]> */
</script>
-------------------------

+ The 'purchase-course' parameter of the /courses/embedded-systems-diploma/ CGI :

/courses/embedded-systems-diploma/?purchase-course=%00ztfpjh

-------- output --------
<script type="text/javascript" id="lpData">
/* <![CDATA[ */
var lpData = {"site_url":"http:\/\/192.168.50.7","user_id":"0","theme":"
tutorstarter","lp_rest_url":"http:\/\/192.168.50.7\/wp-json\/","nonce":"
23987ba727","is_course_archive":"","courses_url":"http:\/\/192.168.50.7\
/courses\/","urlParams":{"purchase-course":"ztfpjh"},"lp_version":"4.2.7
","lp_rest_load_ajax":"http:\/\/192.168.50.7\/wp-json\/lp\/v1\/load_cont
ent_via_ajax\/"};
/* ]]> */
</sc [...]
```

48204 (1) - Apache HTTP Server Version

Synopsis

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-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

192.168.50.7 (tcp/80/www)

```
URL         : http://192.168.50.7/
Version     : 2.4.62
Source      : Server: Apache/2.4.62 (CentOS Stream)
backported  : 0
os          : CentOS Stream
```

48243 (1) - PHP Version Detection

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0936

Plugin Information

Published: 2010/08/04, Modified: 2024/05/31

Plugin Output

192.168.50.7 (tcp/80/www)

```
Nessus was able to identify the following PHP version information :

  Version : 8.0.30
  Source  : X-Powered-By: PHP/8.0.30
```

49704 (1) - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

Plugin Output

192.168.50.7 (tcp/80/www)

```
11 external URLs were gathered on this web server :
URL...                                  - Seen on...


http://fonts.googleapis.com             - /
http://gmpg.org/xfn/11                  - /
https://#                               - /
https://fonts.googleapis.com/css2?family=Poppins%3Awght
%40100%3B300%3B400%3B500%3B700%3B900&display=swap&ver=1.2.0 - /
https://fonts.googleapis.com/css2?family=Sora%3Awght
%40100%3B300%3B400%3B500%3B700%3B900&display=swap&ver=1.2.0 - /
https://fonts.googleapis.com/css?family=Poppins%3A100%2C100italic%2C200%2C200italic
%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic
%2C800%2C800italic%2C900%2C900italic%7CRoboto%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic
%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic
%2C900%2C900italic%7CRoboto+Slab%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic
%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic
%2C900%2C900italic&display=swap&ver=6.6.2 - /about-us/
https://fonts.googleapis.com/css?family=Poppins%3A100%2C100italic%2C200%2C200italic
%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic
%2C800%2C800italic%2C900%2C900italic%7CRoboto%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic
%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic
%2C900%2C900italic&display=swap&ver=6.6.2 - /
https://fonts.gstatic.com/               - /
https://kitpapa.net/lms1/contact/        - /about-us/
https://kitpapa.net/lms1/instructor-registration/ - /about-us/
https://maps.google.com/maps?q=El%20Salam%20Tower%2C%20Next%20to%20As%20Salam%20International
%20Hospital%2C%20Second%20Floor%20Above%20Alfa%20Laboratory%2C%20Cornish%20El%20Maadi%2C%20Cairo%2C
%20Egypt&t=m&z=15&output=embed&iwloc=near - /contact-us/
```

50344 (1) - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

https://content-security-policy.com/

https://www.w3.org/TR/CSP2/

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

192.168.50.7 (tcp/80/www)

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - http://192.168.50.7/
  - http://192.168.50.7/about-us/
  - http://192.168.50.7/blog/
  - http://192.168.50.7/cart/
  - http://192.168.50.7/contact-us/
  - http://192.168.50.7/course-category/embedded-system/
  - http://192.168.50.7/course-category/programming/
  - http://192.168.50.7/course-category/security/
  - http://192.168.50.7/courses/
```

```
- http://192.168.50.7/courses/cybersecurity-diploma-soc/
- http://192.168.50.7/courses/embedded-systems-diploma/
- http://192.168.50.7/courses/flutter-diploma/
- http://192.168.50.7/courses/full-stack-nodejs-diploma/
- http://192.168.50.7/employment/
- http://192.168.50.7/instructor-registration/
- http://192.168.50.7/instructor/amit_admin/
- http://192.168.50.7/my-account/
- http://192.168.50.7/my-account/lost-password/
- http://192.168.50.7/shop/
- http://192.168.50.7/wp-content/
- http://192.168.50.7/wp-content/plugins/
- http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/
- http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/
- http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/css/
- http://192.168.50.7/wp-content/plugins/elementor/
- http://192.168.50.7/wp-content/plugins/elementor/app/
- http://192.168.50.7/wp-content/plugins/elementor/assets/
- http://192.168.50.7/wp-content/plugins/elementor/assets/css/
- http://192.168.50.7/wp-content/plugins/elementor/assets/data/
- http://192.168.50.7/wp-content/plugins/elementor/assets/images/
- http://192.168.50.7/wp-content/plugins/elementor/assets/js/
- http://192.168.50.7/wp-content/plugins/elementor/assets/lib/
- http://192.168.50.7/wp-content/plugins/elementor/assets/mask-shapes/
- http://192.168.50.7/wp-content/plugins/elementor/assets/shapes/
- http://192.168.50.7/wp-content/plugins/elementor/assets/svg-paths/
- http://192.168.50.7/wp-content/plugins/elementor/core/
- h [...]
```

50345 (1) - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

https://en.wikipedia.org/wiki/Clickjacking

http://www.nessus.org/u?399b1f56

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

192.168.50.7 (tcp/80/www)

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - http://192.168.50.7/
  - http://192.168.50.7/about-us/
  - http://192.168.50.7/blog/
  - http://192.168.50.7/cart/
  - http://192.168.50.7/contact-us/
  - http://192.168.50.7/course-category/embedded-system/
  - http://192.168.50.7/course-category/programming/
  - http://192.168.50.7/course-category/security/
  - http://192.168.50.7/courses/
  - http://192.168.50.7/courses/cybersecurity-diploma-soc/
  - http://192.168.50.7/courses/embedded-systems-diploma/
  - http://192.168.50.7/courses/flutter-diploma/
  - http://192.168.50.7/courses/full-stack-nodejs-diploma/
  - http://192.168.50.7/employment/
  - http://192.168.50.7/instructor-registration/
```

```
- http://192.168.50.7/instructor/amit_admin/
- http://192.168.50.7/shop/
- http://192.168.50.7/wp-content/
- http://192.168.50.7/wp-content/plugins/
- http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/
- http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/
- http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/css/
- http://192.168.50.7/wp-content/plugins/elementor/
- http://192.168.50.7/wp-content/plugins/elementor/app/
- http://192.168.50.7/wp-content/plugins/elementor/assets/
- http://192.168.50.7/wp-content/plugins/elementor/assets/css/
- http://192.168.50.7/wp-content/plugins/elementor/assets/data/
- http://192.168.50.7/wp-content/plugins/elementor/assets/images/
- http://192.168.50.7/wp-content/plugins/elementor/assets/js/
- http://192.168.50.7/wp-content/plugins/elementor/assets/lib/
- http://192.168.50.7/wp-content/plugins/elementor/assets/mask-shapes/
- http://192.168.50.7/wp-content/plugins/elementor/assets/shapes/
- http://192.168.50.7/wp-content/plugins/elementor/assets/svg-paths/
- http://192.168.50.7/wp-content/plugins/elementor/core/
- http://192.168.50.7/wp-content/plugins/elementor/data/
- http://192.168.50.7/wp-content/plugins/elementor/ele [...]
```

54615 (1) - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

192.168.50.7 (tcp/0)

```
Remote device type : general-purpose
Confidence level : 65
```

70657 (1) - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

192.168.50.7 (tcp/22/ssh)

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256
  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha256
  diffie-hellman-group16-sha512
  diffie-hellman-group18-sha512
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521
  kex-strict-s-v00@openssh.com

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  rsa-sha2-256
  rsa-sha2-512
  ssh-ed25519

The server supports the following options for encryption_algorithms_client_to_server :

  aes128-ctr
  aes128-gcm@openssh.com
  aes256-ctr
  aes256-gcm@openssh.com
```

```
  chacha20-poly1305@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

  aes128-ctr
  aes128-gcm@openssh.com
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

85602 (1) - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated 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

192.168.50.7 (tcp/80/www)

```
The following cookie does not set the secure cookie flag :

Name : lp_session_guest
Path : /
Value : g-67175de0e24d6
Domain :
Version : 1
Expires : Thu, 24-Oct-2024 08:10:08 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

86420 (1) - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

192.168.50.7 (tcp/0)

```
The following is a consolidated list of detected MAC addresses:
  - 08:00:27:DA:90:BA
```

91815 (1) - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

http://www.nessus.org/u?5496c8d9

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

Plugin Output

192.168.50.7 (tcp/80/www)

```
The following sitemap was created from crawling linkable content on the target host :

  - http://192.168.50.7/
  - http://192.168.50.7/about-us/
  - http://192.168.50.7/blog/
  - http://192.168.50.7/cart/
  - http://192.168.50.7/comments/feed/
  - http://192.168.50.7/contact-us/
  - http://192.168.50.7/course-category/embedded-system/
  - http://192.168.50.7/course-category/embedded-system/feed/
  - http://192.168.50.7/course-category/programming/
  - http://192.168.50.7/course-category/programming/feed/
  - http://192.168.50.7/course-category/security/
  - http://192.168.50.7/course-category/security/feed/
  - http://192.168.50.7/courses/
  - http://192.168.50.7/courses/cybersecurity-diploma-soc/
  - http://192.168.50.7/courses/embedded-systems-diploma/
  - http://192.168.50.7/courses/flutter-diploma/
  - http://192.168.50.7/courses/full-stack-nodejs-diploma/
  - http://192.168.50.7/employment/
  - http://192.168.50.7/feed/
  - http://192.168.50.7/instructor-registration/
  - http://192.168.50.7/instructor/amit_admin/
```

```
  - http://192.168.50.7/my-account/
  - http://192.168.50.7/my-account/lost-password/
  - http://192.168.50.7/shop/
  - http://192.168.50.7/shop/feed/
  - http://192.168.50.7/wp-content/
  - http://192.168.50.7/wp-content/plugins/
  - http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/
  - http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/
  - http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/css/
  - http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/css/checkoutcom-
styles.css
  - http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/css/
normalize.css
  - http://192.168.50.7/wp-content/plugins/elementor/
  - http://192.168.50.7/wp-content/plugins/elementor/app/
  - http://192.168.50.7/wp-content/plugins/elementor/assets/
  - http://192.168.50.7/wp-content/plugins/elementor/assets/css/
  - http://192.168.50.7/wp-content/plugins/elementor/assets/css/admin-bar.css
 [...]
```

106658 (1) - JQuery Detection

Synopsis

The web server on the remote host uses JQuery.

Description

Nessus was able to detect JQuery on the remote host.

See Also

https://jquery.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/07, Modified: 2024/02/08

Plugin Output

192.168.50.7 (tcp/80/www)

```
URL     : http://192.168.50.7/wp-includes/js/jquery/jquery.min.js?ver=3.7.1
Version : 3.7.1
```

110723 (1) - Target Credential Status by Authentication Protocol - No Credentials Provided

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2024/04/19

Plugin Output

192.168.50.7 (tcp/0)

```
SSH was detected on port 22 but no credentials were provided.
```

```
SSH local checks were not enabled.
```

117886 (1) - OS Security Patch Assessment Not Available

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

192.168.50.7 (tcp/0)

```
The following issues were reported :

  - Plugin      : no_local_checks_credentials.nasl
    Plugin ID   : 110723
    Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
    Message     :
Credentials were not provided for detected SSH service.
```

132634 (1) - Deprecated SSLv2 Connection Attempts

Synopsis

Secure Connections, using a deprecated protocol were attempted as part of the scan

Description

This plugin enumerates and reports any SSLv2 connections which were attempted as part of a scan. This protocol has been deemed prohibited since 2011 because of security vulnerabilities and most major ssl libraries such as openssl, nss, mbed and wolfssl do not provide this functionality in their latest versions. This protocol has been deprecated in Nessus 8.9 and later.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/01/06, Modified: 2020/01/06

Plugin Output

192.168.50.7 (tcp/0)

```
Nessus attempted the following SSLv2 connection(s) as part of this scan:

Plugin ID: 42476
Timestamp: 2024-10-22 08:06:23
Port: 22
```

149334 (1) - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

192.168.50.7 (tcp/22/ssh)

153588 (1) - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

192.168.50.7 (tcp/22/ssh)

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com
```

181418 (1) - OpenSSH Detection

Synopsis

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

https://www.openssh.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2024/10/17

Plugin Output

192.168.50.7 (tcp/22/ssh)

```
Service : ssh
Version : 8.7
Banner  : SSH-2.0-OpenSSH_8.7
```

8.2. Web server scanning

Website Scan

Report generated by Tenable Nessus™ Tue, 22 Oct 2024 01:24:19 EDT

TABLE OF CONTENTS

Vulnerabilities by Plugin

Vulnerabilities by Plugin

58987 (1) - PHP Unsupported Version Detection

Synopsis

The remote host contains an unsupported version of a web application scripting language.

Description

According to its version, the installation of PHP on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

http://php.net/eol.php

https://wiki.php.net/rfc/releaseprocess

Solution

Upgrade to a version of PHP that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF IAVA:0001-A-0581

Plugin Information

Published: 2012/05/04, Modified: 2024/05/31

Plugin Output

192.168.50.7 (tcp/80/www)

```
  Source              : X-Powered-By: PHP/8.0.30
```

```
  Installed version   : 8.0.30
  End of support date : 2023/11/26
  Announcement        : http://php.net/supported-versions.php
  Supported versions  : 8.1.x / 8.2.x / 8.3.x
```

42424 (1) - CGI Generic SQL Injection (blind)

Synopsis

A CGI application hosted on the remote web server is potentially prone to SQL injection attack.

Description

By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a very different response, which suggests that it may have been able to modify the behavior of the application and directly access the underlying database.

An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.

See Also

http://www.securiteam.com/securityreviews/5DP0N1P76E.html

http://www.nessus.org/u?ed792cf5

http://www.nessus.org/u?11ab1866

Solution

Modify the affected CGI scripts so that they properly escape arguments.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF	CWE:20
XREF	CWE:77
XREF	CWE:89
XREF	CWE:91
XREF	CWE:203
XREF	CWE:643
XREF	CWE:713

XREF	CWE:722
XREF	CWE:727
XREF	CWE:751
XREF	CWE:801
XREF	CWE:810
XREF	CWE:928
XREF	CWE:929

Plugin Information

Published: 2009/11/06, Modified: 2024/06/14

Plugin Output

192.168.50.7 (tcp/80/www)

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to blind SQL injection :

+ The 'woocommerce-login-nonce' parameter of the /my-account/ CGI :

/my-account/?_wp_http_referer=%2fmy-account%2f&username=&rememberme=fore
ver&password=&woocommerce-login-nonce=fdda44f10ezz%2fmy-account%2f&usern
ame=&rememberme=forever&password=&woocommerce-login-nonce=fdda44f10eyy

-------- output --------
<script type="text/javascript" id="lpData">
/* <![CDATA[ */
var lpData = {"site_url":"http:\/\/192.168.50.7","user_id":"0","theme":"
tutorstarter","lp_rest_url":"http:\/\/192.168.50.7\/wp-json\/","nonce":"
23987ba727","is_course_archive":"","courses_url":"http:\/\/192.168.50.7\
/courses\/","urlParams":{"_wp_http_referer":"\/my-account\/","user [...]
/* ]]> */
</script>
-------- vs --------
<script type="text/javascript" id="lpData">
/* <![CDATA[ */
var lpData = {"site_url":"http:\/\/192.168.50.7","user_id":"0","theme":"
tutorstarter","lp_rest_url":"http:\/\/192.168.50.7\/wp-json\/","nonce":"
23987ba727","is_course_archive":"","courses_url":"http:\/\/192.168.50.7\
/courses\/","urlParams":{"_wp_http_referer":"\/my-account\/","user [...]
/* ]]> */
</script>
------------------------

+ The 'username' parameter of the /my-account/ CGI :

/my-account/?_wp_http_referer=%2fmy-account%2f&woocommerce-login-nonce=f
dda44f10e&rememberme=forever&password=&username=zz%2fmy-account%2f&wooco
mmerce-login-nonce=fdda44f10e&rememberme=forever&password=&username=yy

-------- output --------
<script type="text/javascript" id="lpData">
/* <![CDATA[ */
var lpData = {"site_url":"http:\/\/192.168.50.7","user_id":"0","theme":"
tutorstarter","lp_rest_url":"http:\/\/192.168.50.7\/wp-json\/","nonce":"
23987ba727","is_course_archive":"","courses_url":"http:\/\/192.168.50.7\
/courses\/","urlParams":{"_wp_http_referer":"\/my-account\/","wooc [...]
/* ]]> */
```

```
</script>
-------- vs --------
<script type="text/javascript" id="lpData">
/* <![CDATA[ */
var lpData = {"site_url":"http:\/\/192.168.50.7","user_id":"0","theme":"
 [...]
```

11213 (1) - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

See Also

http://www.nessus.org/u?e979b5cb

http://www.apacheweek.com/issues/03-01-24

https://download.oracle.com/sunalerts/1000718.1.html

Solution

Disable these HTTP methods. Refer to the plugin output for more information.

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 v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

4.0

EPSS Score

0.0058

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information

Published: 2003/01/23, Modified: 2024/04/09

Plugin Output

192.168.50.7 (tcp/80/www)

```
To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request : \n\n------------------------------ snip
 ------------------------------\nTRACE /Nessus419318283.html HTTP/1.1
Connection: Close
Host: 192.168.50.7
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------\n\nand received the
 following response from the remote server :\n\n------------------------------ snip
 ------------------------------\nHTTP/1.1 200 OK
Date: Tue, 22 Oct 2024 03:44:36 GMT
Server: Apache/2.4.62 (CentOS Stream)
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http
```

```
TRACE /Nessus419318283.html HTTP/1.1
Connection: Keep-Alive
Host: 192.168.50.7
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------\n
```

40984 (1) - Browsable Web Directories

Synopsis

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

192.168.50.7 (tcp/80/www)

```
The following directories are browsable :

http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/
http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/
http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/css/
http://192.168.50.7/wp-content/plugins/elementor/
http://192.168.50.7/wp-content/plugins/elementor/app/
http://192.168.50.7/wp-content/plugins/elementor/assets/
http://192.168.50.7/wp-content/plugins/elementor/assets/css/
http://192.168.50.7/wp-content/plugins/elementor/assets/data/
http://192.168.50.7/wp-content/plugins/elementor/assets/images/
```

```
http://192.168.50.7/wp-content/plugins/elementor/assets/js/
http://192.168.50.7/wp-content/plugins/elementor/assets/lib/
http://192.168.50.7/wp-content/plugins/elementor/assets/mask-shapes/
http://192.168.50.7/wp-content/plugins/elementor/assets/shapes/
http://192.168.50.7/wp-content/plugins/elementor/assets/svg-paths/
http://192.168.50.7/wp-content/plugins/elementor/core/
http://192.168.50.7/wp-content/plugins/elementor/data/
http://192.168.50.7/wp-content/plugins/elementor/includes/
http://192.168.50.7/wp-content/plugins/elementor/modules/
http://192.168.50.7/wp-content/plugins/learnpress/assets/
http://192.168.50.7/wp-content/plugins/learnpress/assets/css/
http://192.168.50.7/wp-content/plugins/learnpress/assets/src/
http://192.168.50.7/wp-content/plugins/woocommerce/
http://192.168.50.7/wp-content/plugins/woocommerce/assets/
http://192.168.50.7/wp-content/plugins/woocommerce/assets/client/
http://192.168.50.7/wp-content/plugins/woocommerce/assets/css/
http://192.168.50.7/wp-content/plugins/woocommerce/assets/fonts/
http://192.168.50.7/wp-content/plugins/woocommerce/assets/images/
http://192.168.50.7/wp-content/plugins/woocommerce/assets/js/
http://192.168.50.7/wp-content/plugins/woocommerce/client/
http://192.168.50.7/wp-content/plugins/woocommerce/client/admin/
http://192.168.50.7/wp-content/plugins/woocommerce/i18n/
http://192.168.50.7/wp-content/plugins/woocommerce/i18n/languages/
http:/ [...]
```

85582 (1) - Web Application Potentially Vulnerable to Clickjacking

Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

See Also

http://www.nessus.org/u?399b1f56

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

https://en.wikipedia.org/wiki/Clickjacking

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.

This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

XREF CWE:693

Plugin Information

Published: 2015/08/22, Modified: 2017/05/16

Plugin Output

192.168.50.7 (tcp/80/www)

```
The following pages do not use a clickjacking mitigation response header and contain a clickable
 event :

  - http://192.168.50.7/
  - http://192.168.50.7/about-us/
  - http://192.168.50.7/blog/
  - http://192.168.50.7/cart/
  - http://192.168.50.7/contact-us/
  - http://192.168.50.7/course-category/embedded-system/
  - http://192.168.50.7/course-category/programming/
  - http://192.168.50.7/course-category/security/
  - http://192.168.50.7/courses/
  - http://192.168.50.7/courses/cybersecurity-diploma-soc/
  - http://192.168.50.7/courses/embedded-systems-diploma/
  - http://192.168.50.7/courses/flutter-diploma/
  - http://192.168.50.7/courses/full-stack-nodejs-diploma/
  - http://192.168.50.7/employment/
  - http://192.168.50.7/instructor-registration/
  - http://192.168.50.7/instructor/amit_admin/
  - http://192.168.50.7/shop/
```

90067 (1) - WordPress User Enumeration

Synopsis

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: 2024/06/05

Plugin Output

192.168.50.7 (tcp/80/www)

```
Nessus was able to enumerate the following WordPress users from the WordPress install at
 'http://192.168.50.7/' :
 amit
 user1
```

11219 (2) - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

192.168.50.7 (tcp/22/ssh)

```
Port 22/tcp was found to be open
```

192.168.50.7 (tcp/80/www)

```
Port 80/tcp was found to be open
```

10107 (1) - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

192.168.50.7 (tcp/80/www)

```
The remote web server type is :

Apache/2.4.62 (CentOS Stream)
```

10302 (1) - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

192.168.50.7 (tcp/80/www)

```
Contents of robots.txt :

User-agent: *
Disallow: /wp-content/uploads/wc-logs/
Disallow: /wp-content/uploads/woocommerce_transient_files/
Disallow: /wp-content/uploads/woocommerce_uploads/
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php

Sitemap: http://192.168.50.7/wp-sitemap.xml
```

10662 (1) - Web mirroring

Synopsis

Nessus can crawl the remote website.

Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/05/04, Modified: 2024/07/17

Plugin Output

192.168.50.7 (tcp/80/www)

```
Webmirror performed 1000 queries in 36s (27.0777 queries per second)

The following CGIs have been discovered :


+ CGI : /xmlrpc.php
  Methods : GET
  Argument :
   Value: rsd


+ CGI : /wp-json/oembed/1.0/embed
  Methods : GET
  Argument : format
   Value: xml
  Argument : url
   Value: http%3A%2F%2F192.168.50.7%2Fcart%2F


+ CGI : /
  Methods : GET
  Argument : p
   Value: 253
  Argument : s
```

```
+ CGI : /my-account/
  Methods : POST
  Argument : _wp_http_referer
   Value: /my-account/
  Argument : password
  Argument : rememberme
   Value: forever
  Argument : username
  Argument : woocommerce-login-nonce
   Value: fdda44f10e


+ CGI : /courses/cybersecurity-diploma-soc/
  Methods : POST
  Argument : purchase-course
   Value: 196


+ CGI : /courses/embedded-systems-diploma/
  Methods : POST
  Argument : purchase-course
   Value: 423


+ CGI : /courses/flutter-diploma/
  Methods : POST
  Argument : purchase-course
   Value: 307


+ CGI : /courses/full-stack-nodejs-diploma/
  Methods : POST
  Argument : purchase-course
   Value: 360


+ CGI : /my-account/lost-password/
  Methods : POST
  Argument : _wp_http_referer
   Value: /my-account/lost-password/
  Argument : user_login
  Argument : wc_reset_password
   Value: true
  Argument : woocommerce-lost-password-nonce
   Value: 3ca0703145

Directory index found at /wp-content/plugins/woocommerce/assets/css/
Directory index found at /wp-content/plugins/woocommerce/assets/
Directory index found at /wp-content/plugins/woocommerce/
Directory index found at /wp-content/plugins/elementor/assets/css/
Directory index found at /wp-content/plugins/elementor/assets/
Directory index found at /wp-content/plugins/elementor/
Directory index found at /wp-content/uploads/elementor/css/
Directory index found at /wp-content/uploads/elementor/
Directory index found at /wp-content/uploads/
Directory index found at /wp-content/plugins/learnpress/assets/css/
Directory index found at /wp-content/plugins/learnpress/assets/
Directory index found at /wp-content/uploads/2024/10/
Directory index [...]
```

11032 (1) - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

Solution

n/a

Risk Factor

None

References

XREF OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2024/06/07

Plugin Output

192.168.50.7 (tcp/80/www)

```
The following directories were discovered:
/cgi-bin, /cart, /icons, /shop, /blog

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

11419 (1) - Web Server Office File Inventory

Synopsis

The remote web server hosts office-related files.

Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Risk Factor

None

Plugin Information

Published: 2003/03/19, Modified: 2022/04/11

Plugin Output

192.168.50.7 (tcp/80/www)

```
The following office-related files are available on the remote server :

  - CSV Spreadsheet files (.csv) :
    /wp-content/plugins/woocommerce/sample-data/experimental_fashion_sample_9_products.csv
    /wp-content/plugins/woocommerce/sample-data/experimental_sample_9_products.csv
    /wp-content/plugins/woocommerce/sample-data/sample_products.csv
    /wp-content/plugins/woocommerce/sample-data/sample_tax_rates.csv
```

18297 (1) - WordPress Detection

Synopsis

The remote web server contains a blog application written in PHP.

Description

The remote host is running WordPress, a free blog application written in PHP with a MySQL back-end.

See Also

https://wordpress.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0747

Plugin Information

Published: 2005/05/18, Modified: 2023/05/24

Plugin Output

192.168.50.7 (tcp/80/www)

```
Nessus detected 2 installs of WordPress:

  URL     : http://192.168.50.7/
  Version : 6.6.2

  URL     : http://192.168.50.7/blog
  Version : 6.6.2
```

19506 (1) - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/10/04

Plugin Output

192.168.50.7 (tcp/0)

```
Information about this scan :

Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202410212332
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
```

```
Scan name : Website Scan
Scan policy used : Web Application Tests
Scanner IP : 192.168.50.9
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Ping RTT : 156.736 ms
Thorough tests : yes
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : all_pairs
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 10 minutes.
Web app tests -  Stop at first flaw : param
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/10/21 23:40 EDT
Scan duration : 6242 sec
Scan for malware : no
```

24260 (1) - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

192.168.50.7 (tcp/80/www)

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Tue, 22 Oct 2024 04:12:01 GMT
  Server: Apache/2.4.62 (CentOS Stream)
  X-Powered-By: PHP/8.0.30
  Link: <http://192.168.50.7/wp-json/>; rel="https://api.w.org/", <http://192.168.50.7/wp-json/
wp/v2/pages/511>; rel="alternate"; title="JSON"; type="application/json", <http://192.168.50.7/>;
 rel=shortlink
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Transfer-Encoding: chunked
  Content-Type: text/html; charset=UTF-8

Response Body :

<!DOCTYPE html>
<html lang="en-US">
```

```
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="profile" href="http://gmpg.org/xfn/11">
<link rel="pingback" href="http://192.168.50.7/xmlrpc.php">
<script type="text/javascript" id="lpData">
/* <![CDATA[ */
var lpData = {"site_url":"http:\/
\/192.168.50.7","user_id":"0","theme":"tutorstarter","lp_rest_url":"http:\/\/192.168.50.7\/wp-
json\/","nonce":"23987ba727","is_course_archive":"","courses_url":"http:\/\/192.168.50.7\/courses
\/","urlParams":[],"lp_version":"4.2.7","lp_rest_load_ajax":"http:\/\/192.168.50.7\/wp-json\/lp\/
v1\/load_content_via_ajax\/"};
/* ]]> */
</script>
<style id="learn-press-custom-css">
:root {
--lp-container-max-width: 1290px;
--lp-cotainer-padding: 1rem;
--lp-primary-color: #ffb606;
--lp-secondary-color: #442e66;
}
</style>
<title>AMIT Learning &#8211; Best IT learning Platform Online/Offline</title>
<meta name='robots' content='max-image-preview:large' />
<link rel='dns-prefetch' href='//fonts.googleapis.com' />
<link rel="alternate" type="application/rss+xml" title="AMIT Learning &raquo; Feed"
 href="http://192.168.50.7/feed/" />
<link rel="alternate" type="application/rss+xml" title="AMIT Learning &raquo; Comments Feed"
 href="http://192.168.50.7/comments/feed/" />
<script type="text/javascript">
/* <![CDATA[ */
window._wpem [...]
```

33817 (1) - CGI Generic Tests Load Estimation (all tests)

Synopsis

Load estimation for web application tests.

Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.

The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.

Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/26, Modified: 2022/04/11

Plugin Output

192.168.50.7 (tcp/80/www)

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

on site request forgery                  : S=15         SP=15        AP=27        SC=4         AC=30

SQL injection                            : S=476        SP=476       AP=812       SC=112
 AC=896
unseen parameters                        : S=595        SP=595       AP=1015      SC=140
 AC=1120
local file inclusion                     : S=68         SP=68        AP=116       SC=16
 AC=128
web code injection                       : S=17         SP=17        AP=29        SC=4         AC=32

XML injection                            : S=17         SP=17        AP=29        SC=4         AC=32

format string                            : S=34         SP=34        AP=58        SC=8         AC=64

script injection                         : S=15         SP=15        AP=27        SC=4         AC=30

cross-site scripting (comprehensive test): S=289        SP=289       AP=493       SC=68
 AC=544
```

```
injectable parameter                        : S=34          SP=34         AP=58         SC=8          AC=64

cross-site scripting (extended patterns) : S=90          SP=90         AP=162        SC=24
 AC=180
directory traversal (write access)       : S=34          SP=34         AP=58         SC=8          AC=64

SSI injection                               : S=51          SP=51         AP=87         SC=12         AC=96

header injection                            : S=30          SP=30         AP=54         SC=8          AC=60

HTML injection                              : S=75          SP=75         AP=135        SC=20
 AC=150
directory traversal                         : S=493         SP=493        AP=841        SC=116
 AC=928
arbitrary command execution (time based) : S=102         SP=102        AP=174        SC=24
 AC=192
persistent XSS                           [...]
```

39470 (1) - CGI Generic Tests Timeout

Synopsis

Some generic CGI attacks ran out of time.

Description

Some generic CGI tests ran out of time during the scan. The results may be incomplete.

Solution

Consider increasing the 'maximum run time (minutes)' preference for the 'Web Applications Settings' in order to prevent the CGI scanning from timing out. Less ambitious options could also be used, such as :

- Test more that one parameter at a time per form :

'Test all combinations of parameters' is much slower than 'Test random pairs of parameters' or 'Test all pairs of parameters (slow)'.

- 'Stop after one flaw is found per web server (fastest)'

under 'Do not stop after the first flaw is found per web page' is quicker than 'Look for all flaws (slowest)'.

- In the Settings/Advanced menu, try reducing the value for 'Max number of concurrent TCP sessions per host' or 'Max simultaneous checks per host'.

Risk Factor

None

Plugin Information

Published: 2009/06/19, Modified: 2021/01/19

Plugin Output

192.168.50.7 (tcp/80/www)

```
The following tests timed out without finding any flaw :
- HTML injection
- directory traversal (extended test)
- directory traversal
- SQL injection
- uncontrolled redirection
- cross-site scripting (extended patterns)
- cross-site scripting (comprehensive test)
- arbitrary command execution
```

40773 (1) - Web Application Potentially Sensitive CGI Parameter Detection

Synopsis

An application was found that may use CGI parameters to control sensitive information.

Description

According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. These parameters should be examined to determine what type of data is controlled and if it poses a security risk.

** This plugin only reports information that may be useful for auditors

** or pen-testers, not a real flaw.

Solution

Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.

Risk Factor

None

Plugin Information

Published: 2009/08/25, Modified: 2021/01/19

Plugin Output

192.168.50.7 (tcp/80/www)

```
Potentially sensitive parameters for CGI /my-account/ :

password : Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack
```

43111 (1) - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

192.168.50.7 (tcp/80/www)

```
Based on the response to an OPTIONS request :

  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /icons


Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT COPY DEBUG DELETE GET HEAD INDEX
    LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS
    ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /
    /about-us
    /blog
    /cart
    /cgi-bin
    /comments/feed
    /contact-us
    /course-category/embedded-system
    /course-category/embedded-system/feed
    /course-category/programming
    /course-category/programming/feed
    /course-category/security
    /course-category/security/feed
    /courses
    /courses/cybersecurity-diploma-soc
    /courses/embedded-systems-diploma
    /courses/flutter-diploma
    /courses/full-stack-nodejs-diploma
    /shop

  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /icons

  - Invalid/unknown HTTP methods are allowed on :

    /
    /about-us
    /blog
    /cart
    /cgi-bin
    /comments/feed
    /contact-us
    /course-category/embedded-system
    /course-category/embedded-system/feed
    /course-category/programming
    /course-category/programming/feed
    /course-category/security
    /course-category/security/feed
    /courses
    /courses/cybersecurity-diploma-soc
    /courses/embedded-systems-diploma
    /courses/flutter-diploma
    /courses/full-stack-nodejs-diploma
    /shop
```

47830 (1) - CGI Generic Injectable Parameter

Synopsis

Some CGIs are candidate for extended injection tests.

Description

Nessus was able to to inject innocuous strings into CGI parameters and read them back in the HTTP response.

The affected parameters are candidates for extended injection tests like cross-site scripting attacks.

This is not a weakness per se, the main purpose of this test is to speed up other scripts. The results may be useful for a human pen-tester.

Solution

n/a

Risk Factor

None

References

XREF CWE:86

Plugin Information

Published: 2010/07/26, Modified: 2021/01/19

Plugin Output

192.168.50.7 (tcp/80/www)

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to injectable parameter :

+ The 'purchase-course' parameter of the /courses/full-stack-nodejs-diploma/ CGI :

/courses/full-stack-nodejs-diploma/?purchase-course=%00cxdpbv

-------- output --------
<script type="text/javascript" id="lpData">
/* <![CDATA[ */
var lpData = {"site_url":"http:\/\/192.168.50.7","user_id":"0","theme":"
tutorstarter","lp_rest_url":"http:\/\/192.168.50.7\/wp-json\/","nonce":"
23987ba727","is_course_archive":"","courses_url":"http:\/\/192.168.50.7\
/courses\/","urlParams":{"purchase-course":"cxdpbv"},"lp_version":"4.2.7
","lp_rest_load_ajax":"http:\/\/192.168.50.7\/wp-json\/lp\/v1\/load_cont
```

```
ent_via_ajax\/"};
/* ]]> */
</script>
-------------------------

+ The 'purchase-course' parameter of the /courses/flutter-diploma/ CGI :

/courses/flutter-diploma/?purchase-course=%00cxdpbv

-------- output --------
<script type="text/javascript" id="lpData">
/* <![CDATA[ */
var lpData = {"site_url":"http:\/\/192.168.50.7","user_id":"0","theme":"
tutorstarter","lp_rest_url":"http:\/\/192.168.50.7\/wp-json\/","nonce":"
23987ba727","is_course_archive":"","courses_url":"http:\/\/192.168.50.7\
/courses\/","urlParams":{"purchase-course":"cxdpbv"},"lp_version":"4.2.7
","lp_rest_load_ajax":"http:\/\/192.168.50.7\/wp-json\/lp\/v1\/load_cont
ent_via_ajax\/"};
/* ]]> */
</script>
-------------------------

+ The 'purchase-course' parameter of the /courses/embedded-systems-diploma/ CGI :

/courses/embedded-systems-diploma/?purchase-course=%00cxdpbv

-------- output --------
<script type="text/javascript" id="lpData">
/* <![CDATA[ */
var lpData = {"site_url":"http:\/\/192.168.50.7","user_id":"0","theme":"
tutorstarter","lp_rest_url":"http:\/\/192.168.50.7\/wp-json\/","nonce":"
23987ba727","is_course_archive":"","courses_url":"http:\/\/192.168.50.7\
/courses\/","urlParams":{"purchase-course":"cxdpbv"},"lp_version":"4.2.7
","lp_rest_load_ajax":"http:\/\/192.168.50.7\/wp-json\/lp\/v1\/load_cont
ent_via_ajax\/"};
/* ]]> */
</sc [...]
```

48204 (1) - Apache HTTP Server Version

Synopsis

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-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

192.168.50.7 (tcp/80/www)

```
URL        : http://192.168.50.7/
Version    : 2.4.62
Source     : Server: Apache/2.4.62 (CentOS Stream)
backported : 0
os         : CentOS Stream
```

48243 (1) - PHP Version Detection

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0936

Plugin Information

Published: 2010/08/04, Modified: 2024/05/31

Plugin Output

192.168.50.7 (tcp/80/www)

```
Nessus was able to identify the following PHP version information :

  Version : 8.0.30
  Source  : X-Powered-By: PHP/8.0.30
```

49704 (1) - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

Plugin Output

192.168.50.7 (tcp/80/www)

```
11 external URLs were gathered on this web server :
URL...                                  - Seen on...


http://fonts.googleapis.com             - /
http://gmpg.org/xfn/11                  - /
https://#                               - /
https://fonts.googleapis.com/css2?family=Poppins%3Awght
%40100%3B300%3B400%3B500%3B700%3B900&display=swap&ver=1.2.0 - /
https://fonts.googleapis.com/css2?family=Sora%3Awght
%40100%3B300%3B400%3B500%3B700%3B900&display=swap&ver=1.2.0 - /
https://fonts.googleapis.com/css?family=Poppins%3A100%2C100italic%2C200%2C200italic
%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic
%2C800%2C800italic%2C900%2C900italic%7CRoboto%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic
%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic
%2C900%2C900italic%7CRoboto+Slab%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic
%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic
%2C900%2C900italic&display=swap&ver=6.6.2 - /about-us/
https://fonts.googleapis.com/css?family=Poppins%3A100%2C100italic%2C200%2C200italic
%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic
%2C800%2C800italic%2C900%2C900italic%7CRoboto%3A100%2C100italic%2C200%2C200italic%2C300%2C300italic
%2C400%2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic
%2C900%2C900italic&display=swap&ver=6.6.2 - /
https://fonts.gstatic.com/              - /
https://kitpapa.net/lms1/contact/       - /about-us/
https://kitpapa.net/lms1/instructor-registration/ - /about-us/
https://maps.google.com/maps?q=El%20Salam%20Tower%2C%20Next%20to%20As%20Salam%20International
%20Hospital%2C%20Second%20Floor%20Above%20Alfa%20Laboratory%2C%20Cornish%20El%20Maadi%2C%20Cairo%2C
%20Egypt&t=m&z=15&output=embed&iwloc=near - /contact-us/
```

50344 (1) - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

https://content-security-policy.com/

https://www.w3.org/TR/CSP2/

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

192.168.50.7 (tcp/80/www)

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - http://192.168.50.7/
  - http://192.168.50.7/about-us/
  - http://192.168.50.7/blog/
  - http://192.168.50.7/cart/
  - http://192.168.50.7/contact-us/
  - http://192.168.50.7/course-category/embedded-system/
  - http://192.168.50.7/course-category/programming/
  - http://192.168.50.7/course-category/security/
  - http://192.168.50.7/courses/
```

```
- http://192.168.50.7/courses/cybersecurity-diploma-soc/
- http://192.168.50.7/courses/embedded-systems-diploma/
- http://192.168.50.7/courses/flutter-diploma/
- http://192.168.50.7/courses/full-stack-nodejs-diploma/
- http://192.168.50.7/employment/
- http://192.168.50.7/instructor-registration/
- http://192.168.50.7/instructor/amit_admin/
- http://192.168.50.7/my-account/
- http://192.168.50.7/my-account/lost-password/
- http://192.168.50.7/shop/
- http://192.168.50.7/wp-content/
- http://192.168.50.7/wp-content/plugins/
- http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/
- http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/
- http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/css/
- http://192.168.50.7/wp-content/plugins/elementor/
- http://192.168.50.7/wp-content/plugins/elementor/app/
- http://192.168.50.7/wp-content/plugins/elementor/assets/
- http://192.168.50.7/wp-content/plugins/elementor/assets/css/
- http://192.168.50.7/wp-content/plugins/elementor/assets/data/
- http://192.168.50.7/wp-content/plugins/elementor/assets/images/
- http://192.168.50.7/wp-content/plugins/elementor/assets/js/
- http://192.168.50.7/wp-content/plugins/elementor/assets/lib/
- http://192.168.50.7/wp-content/plugins/elementor/assets/mask-shapes/
- http://192.168.50.7/wp-content/plugins/elementor/assets/shapes/
- http://192.168.50.7/wp-content/plugins/elementor/assets/svg-paths/
- http://192.168.50.7/wp-content/plugins/elementor/core/
- h [...]
```

50345 (1) - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

https://en.wikipedia.org/wiki/Clickjacking

http://www.nessus.org/u?399b1f56

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

192.168.50.7 (tcp/80/www)

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - http://192.168.50.7/
  - http://192.168.50.7/about-us/
  - http://192.168.50.7/blog/
  - http://192.168.50.7/cart/
  - http://192.168.50.7/contact-us/
  - http://192.168.50.7/course-category/embedded-system/
  - http://192.168.50.7/course-category/programming/
  - http://192.168.50.7/course-category/security/
  - http://192.168.50.7/courses/
  - http://192.168.50.7/courses/cybersecurity-diploma-soc/
  - http://192.168.50.7/courses/embedded-systems-diploma/
  - http://192.168.50.7/courses/flutter-diploma/
  - http://192.168.50.7/courses/full-stack-nodejs-diploma/
  - http://192.168.50.7/employment/
  - http://192.168.50.7/instructor-registration/
```

```
- http://192.168.50.7/instructor/amit_admin/
- http://192.168.50.7/shop/
- http://192.168.50.7/wp-content/
- http://192.168.50.7/wp-content/plugins/
- http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/
- http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/
- http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/css/
- http://192.168.50.7/wp-content/plugins/elementor/
- http://192.168.50.7/wp-content/plugins/elementor/app/
- http://192.168.50.7/wp-content/plugins/elementor/assets/
- http://192.168.50.7/wp-content/plugins/elementor/assets/css/
- http://192.168.50.7/wp-content/plugins/elementor/assets/data/
- http://192.168.50.7/wp-content/plugins/elementor/assets/images/
- http://192.168.50.7/wp-content/plugins/elementor/assets/js/
- http://192.168.50.7/wp-content/plugins/elementor/assets/lib/
- http://192.168.50.7/wp-content/plugins/elementor/assets/mask-shapes/
- http://192.168.50.7/wp-content/plugins/elementor/assets/shapes/
- http://192.168.50.7/wp-content/plugins/elementor/assets/svg-paths/
- http://192.168.50.7/wp-content/plugins/elementor/core/
- http://192.168.50.7/wp-content/plugins/elementor/data/
- http://192.168.50.7/wp-content/plugins/elementor/ele [...]
```

85602 (1) - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated 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

192.168.50.7 (tcp/80/www)

```
The following cookie does not set the secure cookie flag :

Name : lp_session_guest
Path : /
Value : g-67171eed84077
Domain :
Version : 1
Expires : Thu, 24-Oct-2024 03:41:33 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

91815 (1) - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

http://www.nessus.org/u?5496c8d9

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

Plugin Output

192.168.50.7 (tcp/80/www)

```
The following sitemap was created from crawling linkable content on the target host :

  - http://192.168.50.7/
  - http://192.168.50.7/about-us/
  - http://192.168.50.7/blog/
  - http://192.168.50.7/cart/
  - http://192.168.50.7/comments/feed/
  - http://192.168.50.7/contact-us/
  - http://192.168.50.7/course-category/embedded-system/
  - http://192.168.50.7/course-category/embedded-system/feed/
  - http://192.168.50.7/course-category/programming/
  - http://192.168.50.7/course-category/programming/feed/
  - http://192.168.50.7/course-category/security/
  - http://192.168.50.7/course-category/security/feed/
  - http://192.168.50.7/courses/
  - http://192.168.50.7/courses/cybersecurity-diploma-soc/
  - http://192.168.50.7/courses/embedded-systems-diploma/
  - http://192.168.50.7/courses/flutter-diploma/
  - http://192.168.50.7/courses/full-stack-nodejs-diploma/
  - http://192.168.50.7/employment/
  - http://192.168.50.7/feed/
  - http://192.168.50.7/instructor-registration/
  - http://192.168.50.7/instructor/amit_admin/
```

```
  - http://192.168.50.7/my-account/
  - http://192.168.50.7/my-account/lost-password/
  - http://192.168.50.7/shop/
  - http://192.168.50.7/shop/feed/
  - http://192.168.50.7/wp-content/
  - http://192.168.50.7/wp-content/plugins/
  - http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/
  - http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/
  - http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/css/
  - http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/css/checkoutcom-
styles.css
  - http://192.168.50.7/wp-content/plugins/checkout-com-unified-payments-api/assets/css/
normalize.css
  - http://192.168.50.7/wp-content/plugins/elementor/
  - http://192.168.50.7/wp-content/plugins/elementor/app/
  - http://192.168.50.7/wp-content/plugins/elementor/assets/
  - http://192.168.50.7/wp-content/plugins/elementor/assets/css/
  - http://192.168.50.7/wp-content/plugins/elementor/assets/css/admin-bar.css
 [...]
```

106658 (1) - JQuery Detection

Synopsis

The web server on the remote host uses JQuery.

Description

Nessus was able to detect JQuery on the remote host.

See Also

https://jquery.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/07, Modified: 2024/02/08

Plugin Output

192.168.50.7 (tcp/80/www)

```
URL     : http://192.168.50.7/wp-includes/js/jquery/jquery.min.js?ver=3.7.1
Version : 3.7.1
```