CERTIFICATE
OF PCI COMPLIANCE

This is to certify that **Bidaiondo** , has successfully completed an ASV External Quarterly Vulnerability Scan according to, and in compliance with, the Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 Requirement 11.2.2, as set forth by the PCI Security Standards Council (PCI SSC) and endorsed by the major payment brands.

The scan customer attests that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section A.3, “Scan Status”) includes all components which should be in scope for PCI DSS, any component considered out of scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions—including compensating controls if applicable—is accurate and complete. The scan customer also acknowledges 1) accurate and complete scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

The scan and report was prepared and conducted according to internal processes that meet PCI DSS Requirement 11.2.2 and the PCI ASV Program Guide, including manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by PCI ASV certified professionals.

It is the scan customer responsibility to continually review and assess the effect of changing or adding any new systems components that could stores, processes, or transmits cardholder data in their environment or that could affect the security of the cardholder data environment, so that these newly added system components could be included in the scope of the validation process. This certificate is valid through the expiration date stated herewith and is limited to the extent of the scan customer’s accuracy of the information provided regarding the system components to be considered in scope for PCI DSS, and their ability to complete all the steps required for validation.

GM Sectec makes no representation or warranty to any third party as to whether the scan customer's systems are in fact secure from either internal or external attacks nor data breaches, or whether the cardholder data is at risk of being compromised, nor the that scan results represent the scan customer’s overall compliance status with PCI DSS, nor provides any indication of compliance with other PCI DSS requirements. GM Sectec accepts no liability to any third party in the event of loss or damage of any description, caused by any failure of or data breach to, the scan customer’s system components that could stores, processes, or transmits cardholder data or that could affect the security of the cardholder data environment. This certificate is for the sole purpose of identifying the scan customer compliance status with the standard and is not intended nor can it be used for any other purpose. For a complete list of requirements for the PCI ASV standard please visit www.pcisecuritystandards.org.

GM sectec

AWARDED TO:
Bidaiondo

CERTIFICATE NUMBER:
02202406172501

OPERATION:
Vizcaya, Spain

BUSINESS:
E-Commerce

DATE COMPLETED:
02/06/2024

EXPIRATION DATE:
05/06/2024

VERSION COMPLETED:
PCI ASV v3.1

CONTACT:
Teresita Espino
info@bidaiondo.com

ASV Scan Report - Attestation of Scan Compliance

1. Scan Customer Information

Company: Bidaiondo S.L.	**Contact Name:** Teresita Espino	
Job Title: Administrator	**Telephone:** 34 944530466	
E-mail: info@bidaiondo.com	**Business Address:** Gesuraga 50 Sondika 48150	
City: Vizcaya	**State/Province:**	**ZIP:** 48150
Country:	**URL:**	

2. Approved Scanning Vendor Information

Company: SAINT Corporation	**Contact Name:** SAINT ASV Staff	
Job Title: IT Security Consultant	**Telephone:** 301-656-0521	
E-mail: asvstaff@saintcorporation.com	**Business Address:** 4720 Montgomery Lane Suite 800	
City: Bethesda	**State/Province:** MD	**ZIP:** 20814
Country: US	**URL:** http://www.saintcorporation.com	

3. Scan Status

Date scan completed: Feb. 6, 2024	**Scan expiration date (90 days from scan date):** May 6, 2024
Compliance Status: PASS	**Scan Report Type:** Full scan
Number of unique in-scope components scanned: 1	**Number of identified failing vulnerabilities:** 0
Number of components found by ASV but not scanned because scan customer confirmed they were out of scope: 1	

4. Scan Customer Attestation

Bidaiondo S.L. attests on February 6, 2024 that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section 3, "Scan Status") includes all components which should be in scope for PCI DSS, any component considered out of scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions including compensating controls if applicable is accurate and complete. Bidaiondo S.L. also acknowledges 1) accurate and complete scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

Signature:_____ Name:_____ Title:_____

5. ASV Attestation

This scan and report was prepared and conducted by SAINT Corporation under certificate number 4268-01-16, according to internal processes that meet PCI DSS Requirement 11.2.2 and the ASV Program Guide.
SAINT Corporation attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by SAINT ASV Staff.

Scan Session: mID257019; Scan Policy: PCI External; Scan Data Set: 6 February 2024 11:59

SAINTwriter Assessment Report

Report Generated: February 6, 2024

1 Introduction

On February 6, 2024, at 11:59 AM, a PCI External assessment was conducted using the SAINT 10.2.18 vulnerability scanner. The scan discovered a total of one live host, and detected zero critical problems, zero areas of concern, and two potential problems. The hosts and problems detected are discussed in greater detail in the following sections.

2 Summary

The following vulnerability severity levels are used to categorize the vulnerabilities:

CRITICAL PROBLEMS
Vulnerabilities which pose an immediate threat to the network by allowing a remote attacker to directly gain read or write access, execute commands on the target, or create a denial of service.

AREAS OF CONCERN
Vulnerabilities which do not directly allow remote access, but do allow privilege elevation attacks, attacks on other targets using the vulnerable host as an intermediary, or gathering of passwords or configuration information which could be used to plan an attack.

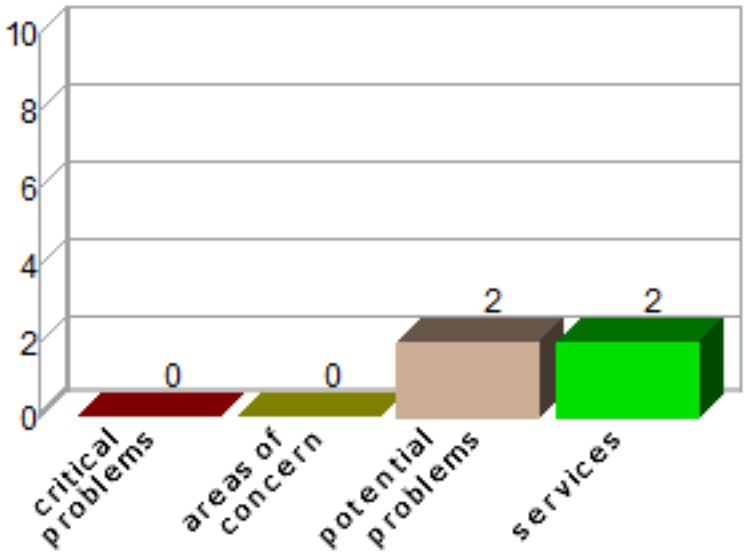
POTENTIAL PROBLEMS
Warnings which may or may not be vulnerabilities, depending upon the patch level or configuration of the target. Further investigation on the part of the system administrator may be necessary.

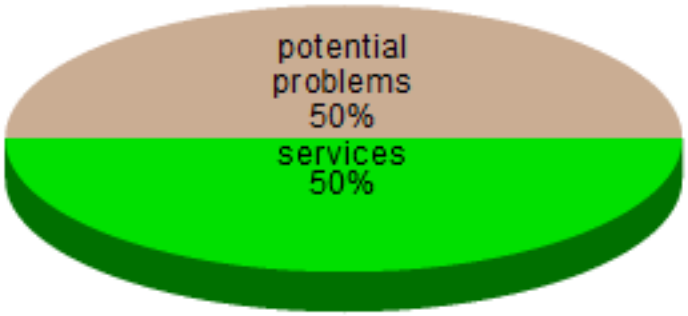
SERVICES
Network services which accept client connections on a given TCP or UDP port. This is simply a count of network services, and does not imply that the service is or is not vulnerable.

The sections below summarize the results of the scan.

2.1 Vulnerabilities by Severity

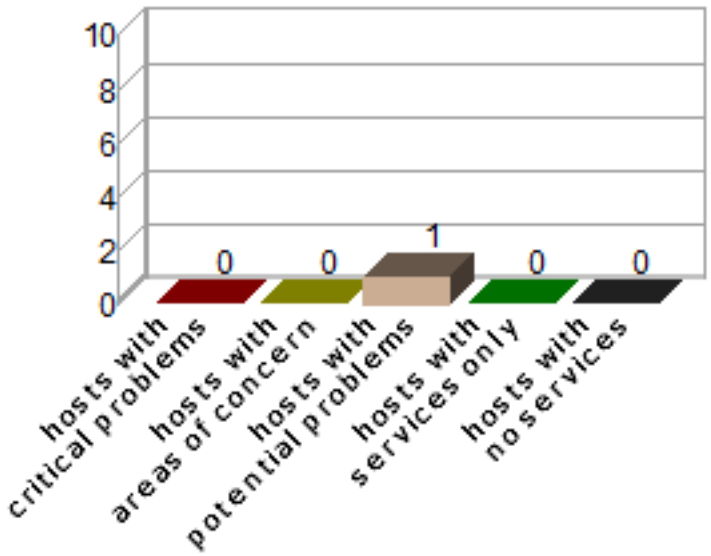
This section shows the overall number of vulnerabilities and services detected at each severity level.

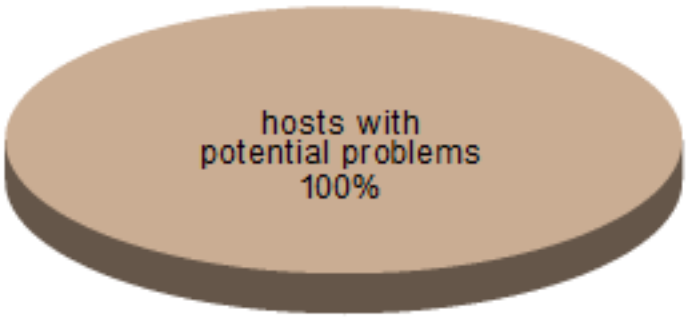




2.2 Hosts by Severity

This section shows the overall number of hosts detected at each severity level. The severity level of a host is defined as the highest vulnerability severity level detected on that host.

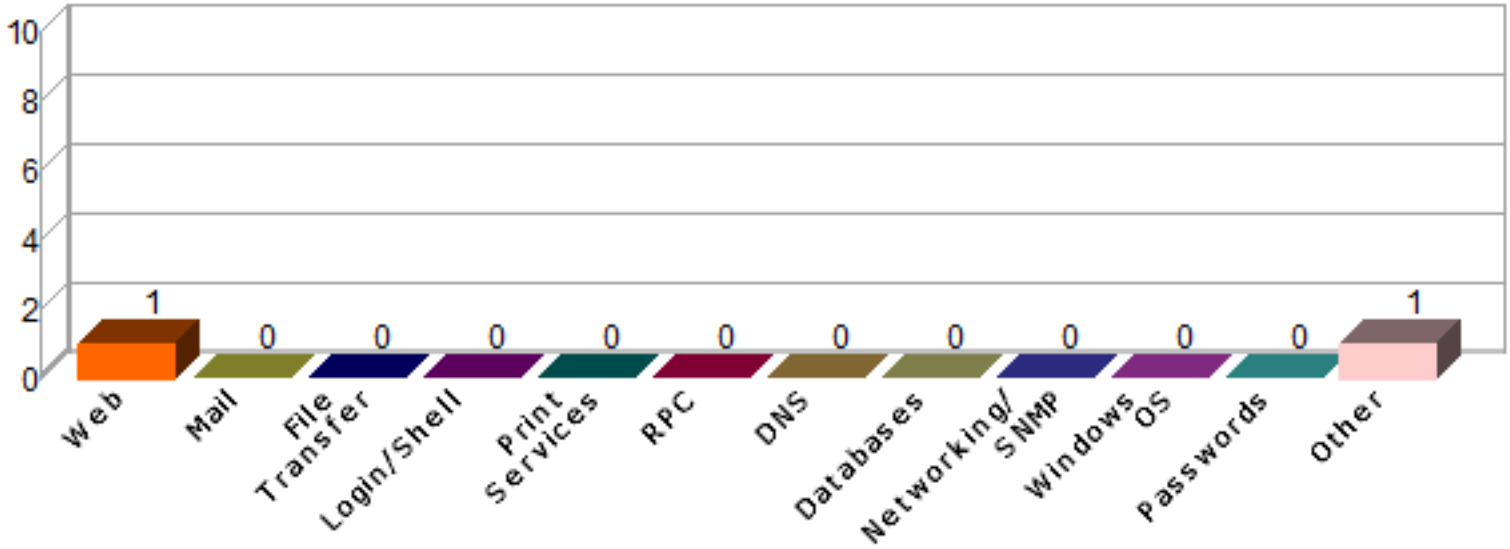


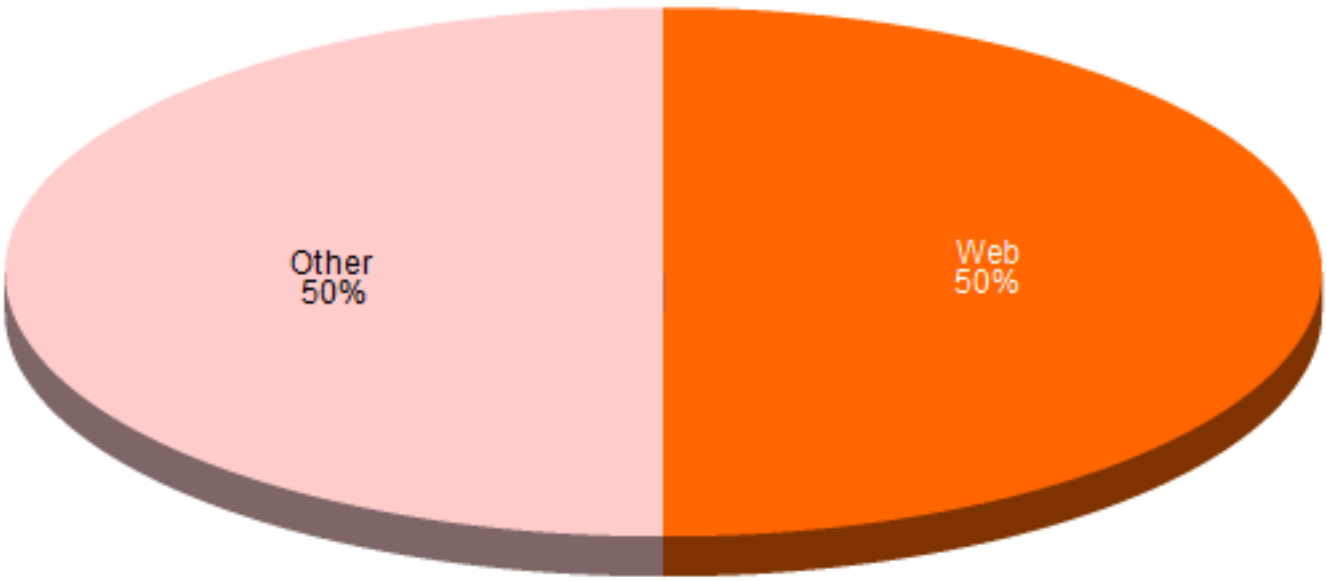


2.3 Vulnerabilities by Class

This section shows the number of vulnerabilities detected in each vulnerability class.

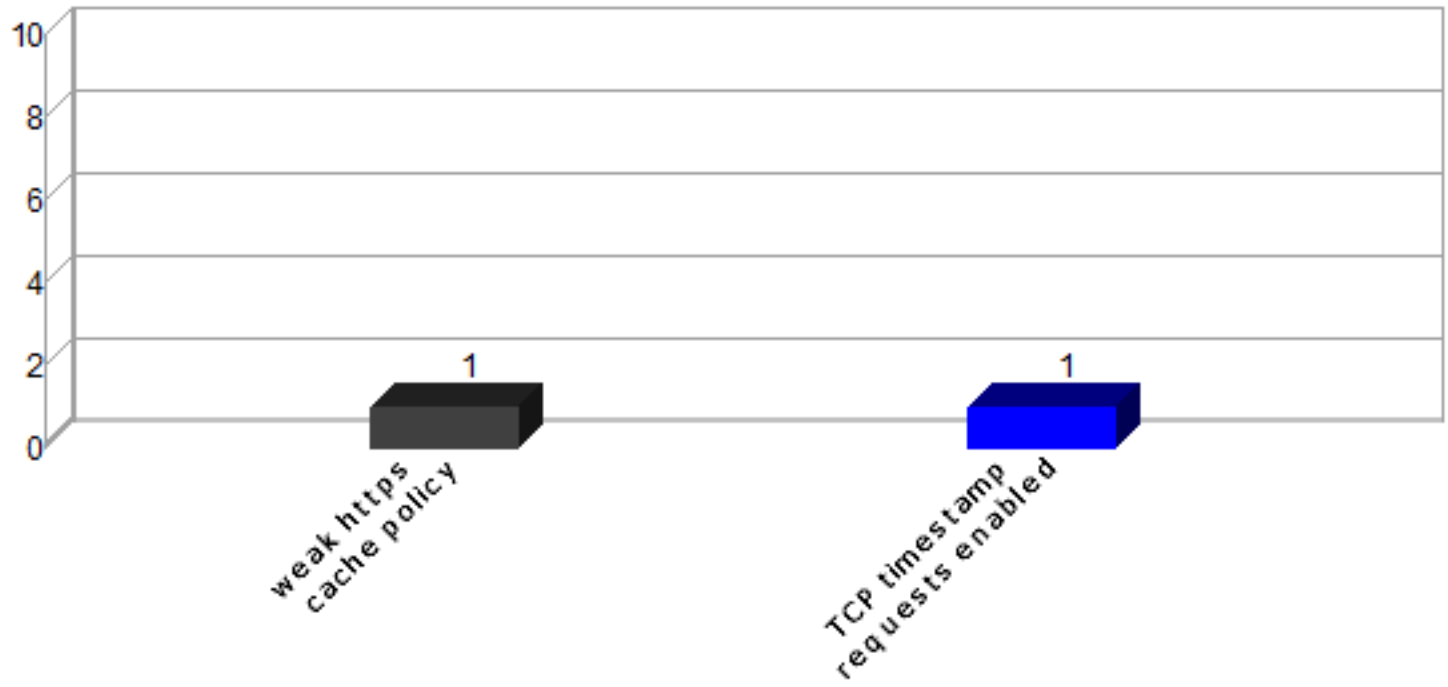
Class	Description
Web	Vulnerabilities in web servers, CGI programs, and any other software offering an HTTP interface
Mail	Vulnerabilities in SMTP, IMAP, POP, or web-based mail services
File Transfer	Vulnerabilities in FTP and TFTP services
Login/Shell	Vulnerabilities in ssh, telnet, rlogin, rsh, or rexec services
Print Services	Vulnerabilities in lpd and other print daemons
RPC	Vulnerabilities in Remote Procedure Call services
DNS	Vulnerabilities in Domain Name Services
Databases	Vulnerabilities in database services
Networking/SNMP	Vulnerabilities in routers, switches, firewalls, or any SNMP service
Windows OS	Missing hotfixes or vulnerabilities in the registry or SMB shares
Passwords	Missing or easily guessed user passwords
Other	Any vulnerability which does not fit into one of the above classes





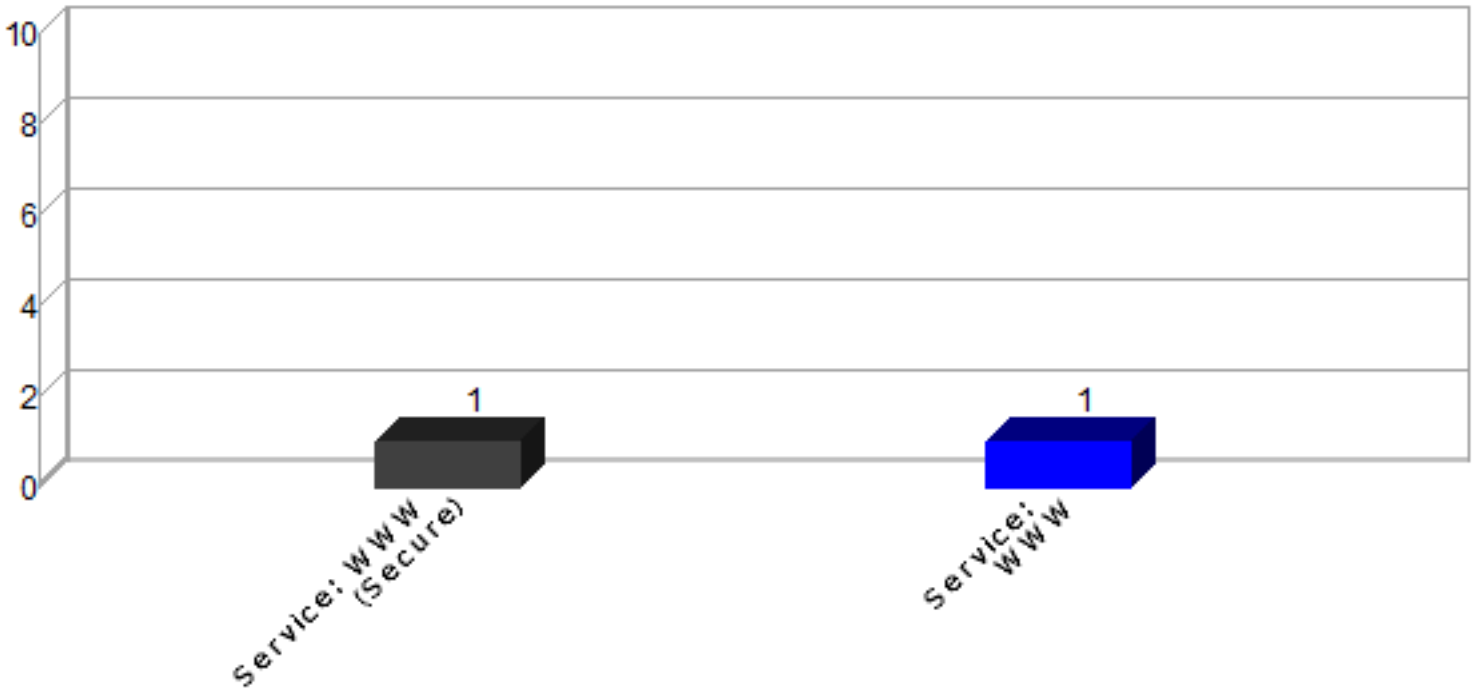
2.4 Top 10 Vulnerabilities

This section shows the most common vulnerabilities detected, and the number of occurrences.



2.5 Top 10 Services

This section shows the most common services detected, and the number of hosts on which they were detected.



3 Overview

The following tables present an overview of the hosts discovered on the network and the vulnerabilities contained therein.

3.1 Host List

This table presents an overview of the hosts discovered on the network.

Host Name	Netbios Name	IP Address	Host Type	Critical Problems	Areas of Concern	Potential Problems
www.bipay.eus		217.116.20.98	Linux 4.0	0	0	2

3.2 Vulnerability List

This table presents an overview of the vulnerabilities detected on the network.

Host Name	Severity	Vulnerability / Service	Class	CVE	Exploit Available?
www.bipay.eus	potential	weak https cache policy	Web		no
www.bipay.eus	potential	TCP timestamp requests enabled	Other		no
www.bipay.eus	service	Service: WWW			no
www.bipay.eus	service	Service: WWW (Secure)			no
www.bipay.eus	info	Certificate info: subject=www.bipay.eus issuer=Don Dominio / MrDomain RSA DV CA start=230508000000Z expires=240607235959Z			no
www.bipay.eus	info	Web Directory: /cgi-bin/			no
www.bipay.eus	info	Web Directory: /scripts/			no

4 Details

The following sections provide details on the specific vulnerabilities detected on each host.

4.1 www.bipay.eus

IP Address: 217.116.20.98
Host type: Linux 4.0
Scan time: Feb 06 11:59:03 2024

weak https cache policy

Severity: Potential Problem

Impact

The confidentiality provided by **`https`** sessions could be compromised due to stored copies of sensitive pages in a shared cache or browser cache.

Resolution

Set the **`Cache-Control`** header to one or more of the following values:

- **private**: allows caching in the browser, but not shared caches
- **no-cache**: forces the cache to re-validate the authenticated session with the server before delivering a cached page
- **no-store**: prohibits the storing of cached pages

Setting **`Cache-Control`** to **`no-cache, no-store`** provides the greatest protection.

The **`Cache-Control`** header can be set programmatically using PHP's **`header()`** function, Java's **`HttpServletResponse.addHeader()`** method, or ASP's **`Response.AddHeader()`** method.

The **`Cache-Control`** header can also be set in the web server's configuration as follows:

- **Apache**:
  Add the following directive to the configuration file:

```
Header set Cache-Control "no-cache, no-store"
```

It is also a good idea to set an **`Expires`** header along with the **`Cache-Control`** header for browsers and proxies which don't yet support HTTP

/1.1. **`Expires`** should be set to a date in the past or an invalid date to prevent caching. For example, **`Sat, 31 May 2014 08:00:00 GMT`**.

References

For more information, see the OWASP Application Security FAQ and Mark Nottingham's Caching Tutorial.

Technical Details

Service: https
Sent:
GET /scripts/ HTTP/1.0
Host: www.bipay.eus
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Received:
(no Cache-Control header)

TCP timestamp requests enabled

Severity: Potential Problem

Impact

A remote attacker could possibly determine the amount of time since the computer was last booted.

Resolution

TCP timestamps are generally only useful for testing, and support for them should be disabled if not needed.

References

More information on TCP timestamps and round-trip time measurement is available in RFC1323 and Microsoft Article 224829.

Technical Details

Service: http
timestamp=2935323631; uptime guess=34d 0h 11m 1s

Service: WWW

Severity: Service

Technical Details

HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Tue, 06 Feb 2024 16:42:04 GMT
Content-Type: text/html
Content-Length: 162
Connection: close
Location:

Service: WWW (Secure)

Severity: Service

Technical Details

HTTP/1.1 400 Bad Request
Server: nginx
Date: Tue, 06 Feb 2024 16:42:04 GMT
Content-Type: text/html
Content-Length: 248
Connection: close
<html>
<head><title>400 The

ASV Scan Report Executive Summary

Report Generated: February 6, 2024

Part 1. Scan Information

Scan Customer Company: Bidaiondo S.L.	**ASV Company:** SAINT Corporation
Date scan was completed: February 6, 2024	**Scan expiration date:** May 6, 2024

Part 2. Component Compliance Summary

Host Name	PCI Compliant?
www.bipay.eus	PASS

Part 3a. Vulnerabilities Noted for each Component

Component:Port	Vulnerability / Service	CVE	PCI Severity	CVSS Base Score	PCI Compliant?	Exceptions, False positives, or Compensating Controls Noted by the ASV for this Vulnerability
www.bipay.eus	nothing to report					

Part 3b. Special Notes to Scan Customer by Component

Component	Special Note to Scan Customer	Item Noted	Per section 7.2 of the ASV Program Guide, scan customer's description of action taken and declaration that software is either needed for business and implemented securely, or removed.

Part 3c. Special Notes - Full Text

Part 4a. Scope Submitted by Scan Customer for Discovery

- www.bipay.eus

Part 4b. Scan Customer Designated "In-Scope" Components (Scanned)

- 217.116.20.98 / www.bipay.eus

Part 4c. Scan Customer Designated "Out-of-Scope" Components (Not Scanned)

- 213.165.69.127 / mail.bidaiondo.com (mail exchanger for www.bipay.eus) - Scan customer attests that IP address is not in scope.

Scan Session: mID257019; Scan Policy: PCI External; Scan Data Set: 6 February 2024 11:59