

# INTERNAL NETWORK PENETRATION TESTING REPORT

**CONFIDENTIAL**

*SAFEBANK CORPORATION*

Target IP(s):	192.168.1.3, 10.10.10.0/24, 10.0.0.3
Prepared By:	CyberZee
Date of Issue:	03 <sup>rd</sup> July, 2024

## Table of Contents

<b>Disclaimer .....</b>	<b>4</b>
<b>1. Executive Summary.....</b>	<b>5</b>
1.1 Scope of the Assessment.....	5
1.2 Overall Security Status of the Safe Bank Corporate .....	6
1.3 Vulnerability Distribution .....	7
<b>2. Risk Level Information and Necessary Actions .....</b>	<b>8</b>
<b>3. Vulnerability Summary .....</b>	<b>9</b>
3.1 10.0.0.3 .....	9
3.2 10.10.10.10 .....	9
3.3 192.168.1.3 .....	10
<b>4. Assessment Methodology .....</b>	<b>10</b>
4.1 Information Gathering .....	10
4.1.1 Host Discovery .....	10
4.2 Enumeration .....	11
4.2.1 Service Enumeration .....	11
4.2.2 Directory Enumeration.....	12
4.3 Vulnerability Assessment.....	13
4.4 Exploitation.....	13
<b>5. Detailed Security Findings .....</b>	<b>13</b>
5.1 10.0.0.3 .....	13
5.1.1 Inadequate path management .....	13
5.1.2 Deprecated or weak security ciphers are supported (TLS 1.0) ...	14
5.1.3 PHP allow_url_fopen enabled .....	16
5.1.4 PHP open_basedir is not set .....	17
5.1.5 Deprecated or weak security ciphers are supported (TLS 1.1) ...	18
5.1.6 PHP info page.....	19
5.1.7 HTTP strict transport security (HSTS) not implemented .....	20
5.1.8 X-Frame-Options header missing.....	21
5.1.9 Content Security Policy (CSP) not implemented .....	22
5.2 10.10.10.10 .....	24

5.2.1	Insufficient LLMNR configuration .....	24
5.2.2	Insufficient password policy implementation.....	25
5.3	192.168.1.3 .....	26
5.3.1	DNS Server Spoofed Request Amplification DDoS.....	26
5.3.2	SSL 64-bit Block Size Cipher Suites Supported (SWEET32) .....	27
5.3.3	Deprecated or weak security ciphers are supported (TLS 1.0) ...	29
5.3.4	Deprecated or weak security ciphers are supported (TLS 1.1) ...	30

## Disclaimer

This document contains Client Confidential information and may not be copied without written permission. The contents of this report are classified as proprietary and confidential information belonging to **Safe Bank**. Any unauthorized or inappropriate disclosure of this report or its contents may lead to substantial harm or loss for **Safe Bank**. Therefore, it is imperative that this report is shared only with individuals who have a legitimate need to know. In the case of physical copies, they should be securely stored and locked when not in use. Electronic copies must be kept offline and safeguarded with appropriate security measures.

## 1. Executive Summary

**Safe Bank** engaged with us to conduct internal network penetration testing against **Safe Bank** corporate network. The purpose of the engagement was to utilize active exploitation techniques to evaluate the security of the network and application against best practise criteria, validate its security mechanisms, and identify possible threats and vulnerabilities. The assessment provides insight into the resilience of the application to withstand attacks from unauthorized users and the potential for valid users to abuse their privileges and access. All the activities were conducted in manner which simulates a real life threats and attackers targeting the organization infrastructure of **Safe Bank** corporate.

This current report details the scope of the testing conducted and all significant findings along with detailed remedial advice. The summary below provides non-technical audience with a summary of the key findings and section two of this report relates the key findings and contains technical details of each vulnerability that was discovered during the assessment along with tailored necessary steps and best practices to fix.

### 1.1 Scope of the Assessment

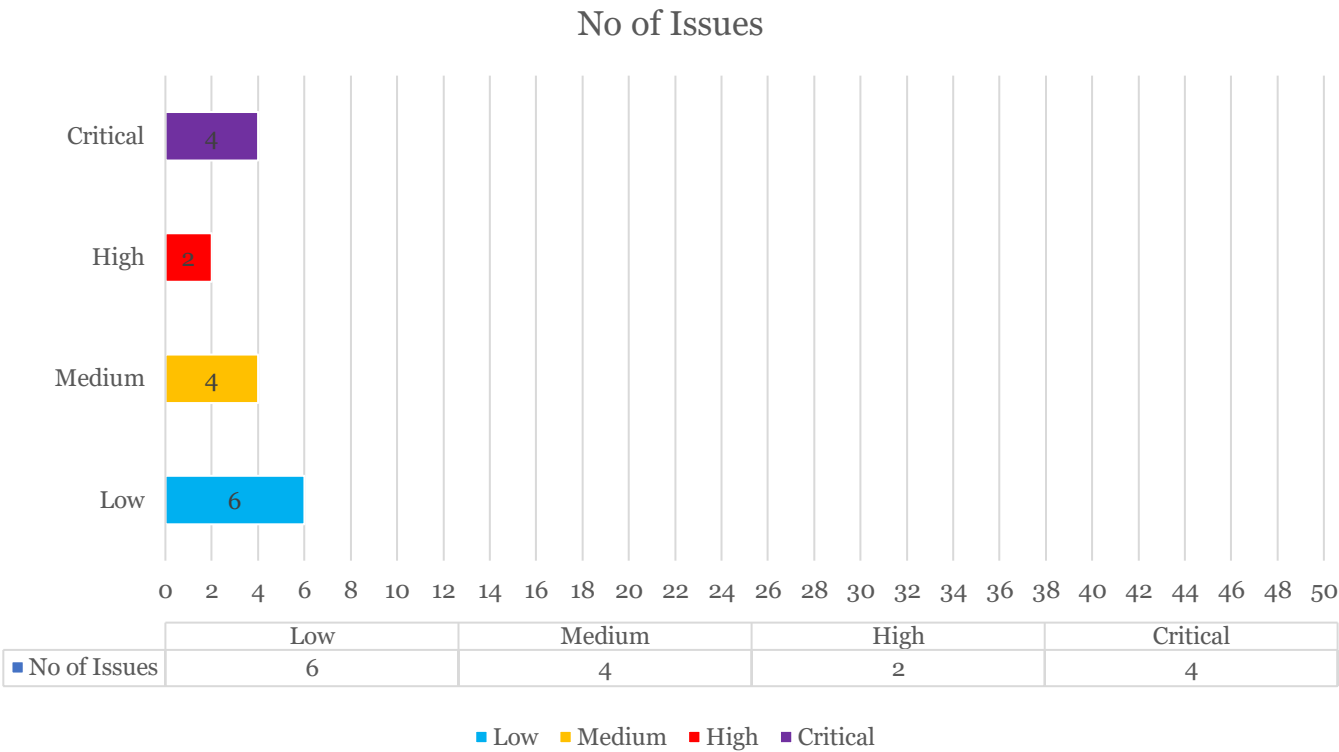
The penetration testing was conducted on the corporate infrastructure of **Safe Bank** organization. The web application of **Safe Bank** which was hosted in the URL **<https://www.safebank.local/>** also assessed during the process of penetration testing process.

10.0.0.3	Microsoft Windows Server 2022/2016	Web Application
10.10.10.10	Windows 10	Client
192.168.1.3	Microsoft Windows Server 2022/2016	host-3.test.net (Domain Controller)

1.2 Overall Security Status of the Safe Bank Corporate

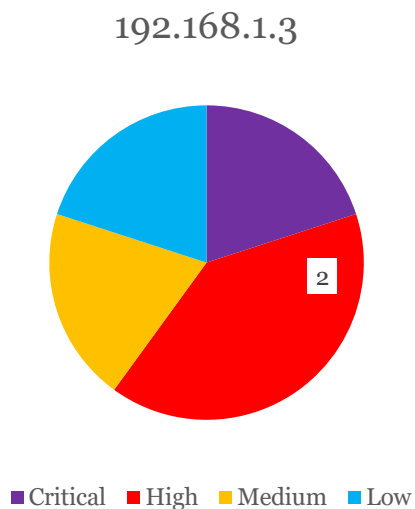
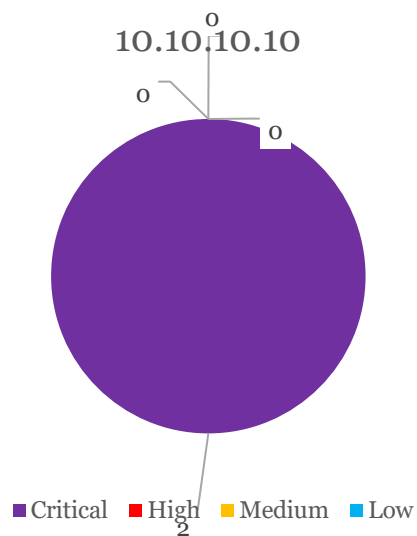
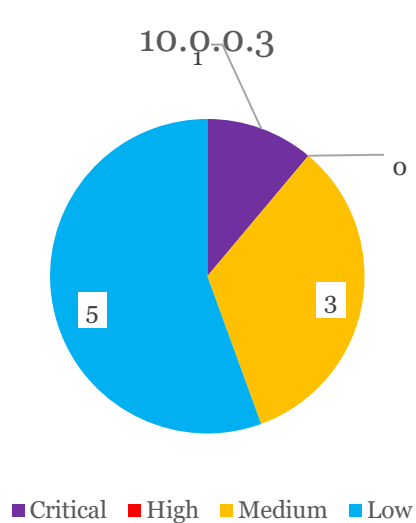
During the penetration testing, CyberZee executed test scenarios using licensed automated tools as well as manual/customized testing methodologies. Four (04) critical-risk security vulnerabilities, two (02) high-risk security vulnerabilities, four (04) medium-risk security vulnerabilities, and six (06) low-risk security vulnerabilities were discovered as security findings during the overall assessment. All the findings were carefully verified with manual intervention.

Based on the security assessment for **Safe Bank** infrastructure and web applications the current status of the identified vulnerabilities set the risk at a **CRITICAL** level.



### 1.3 Vulnerability Distribution

The below pie charts illustrate the vulnerability distribution of the each hosts of the organization.



## 2. Risk Level Information and Necessary Actions

CRITICAL	The critical-risk level shows the highest risk associated with a vulnerability, usually straightforward. Results in root/administrator-level access to the system.
HIGH	The high-risk level shows the high risk associated with a specific vulnerability. Successful exploitation can may lead to compromise the target application's data partially or completely.
MEDIUM	The medium risk level indicates considerable risk combine with a specific vulnerability. Exploiting medium vulnerability, an attacker can gain medium-level information about the application. After mitigating the High-risk vulnerabilities, medium risk vulnerabilities should be mitigated.
LOW	The low-risk level indicates the lowest risk associated with a specific vulnerability. This may lead to gain some information about the web application which is not intended to be known otherwise.



### 3. Vulnerability Summary

#### 3.1 10.0.0.3

#	Vulnerability Name	Severity	Recommendations
1	Inadequate path management.	Critical	Ensure the relevant services are up to date and upgrade to the latest versions that are supported.
2	Deprecated or weak security ciphers are supported (TLS 1.0).	Medium	Disable TLS 1.0 and replace it with TLS 1.2 or higher.
3	PHP allow_url_fopen enabled	Medium	Disable allow_url_fopen
4	PHP open_basedir is not set	Medium	Set open_basedir from php.ini
5	Deprecated or weak security ciphers are supported (TLS 1.1).	Low	Disable TLS 1.1 and replace it with TLS 1.2 or higher.
6	PHP info page.	Low	Disable PHP info page.
7	HTTP strict transport security (HSTS) not implemented	Low	Implement the HTTP strict transport security (HSTS) header.
8	X-Frame-Options header missing	Low	Implement X-Frame-Options security header.
9	Content Security Policy (CSP)	Low	Implement Content Security Policy (CSP) security header.

#### 3.2 10.10.10.10

#	Vulnerability Name	Severity	Recommendations
1	Insufficient LLMNR configuration	Critical	Disable multicast name resolution via GPO.
2	Insufficient password policy implementation	Critical	Implement CIS Benchmark password requirements / PAM solution.

### 3.3 192.168.1.3

#	Vulnerability Name	Severity	Recommendations
1	DNS Server Spoofed Request Amplification DDoS	High	Restrict access to your DNS server from public network or reconfigure it to reject such queries.
2	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	High	Reconfigure the affected application, if possible, to avoid use of all 64-bit block ciphers. Alternatively, place limitations on the number of requests that are allowed to be processed over the same TLS connection to mitigate this vulnerability.
3	Deprecated or weak security ciphers are supported (TLS 1.0).	Medium	Disable TLS 1.0 and replace it with TLS 1.2 or higher.
4	Deprecated or weak security ciphers are supported (TLS 1.1).	Low	Disable TLS 1.1 and replace it with TLS 1.2 or higher.

## 4. Assessment Methodology

### 4.1 Information Gathering

#### 4.1.1 Host Discovery

The penetration tester conducted discovery to find out the live hosts on the network segment and was able to find out the IP address of **Safe Bank**.

```
(kali@host-1)-[~]
$ nmap -sn 10.10.10.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-29 14:13 BST
Nmap scan report for 10.10.10.1
Host is up (0.00058s latency).
Nmap scan report for 10.10.10.10
Host is up (0.0082s latency).
Nmap scan report for 10.10.10.200
Host is up (0.0050s latency).
```

```
(kali@host-1)-[~]
$ sudo arp-scan -I eth0 10.10.10.0/24
Interface: eth0, type: EN10MB, MAC: 00:50:56:08:27:39, IPv4: 10.10.10.1
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.10.10.10    00:50:56:11:7d:d9    VMware, Inc.
10.10.10.200  00:50:56:27:24:8e    VMware, Inc.
```

```
(kali@host-1)-[~]
$ nmap -sn 192.168.1.1/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-30 05:56 BST
Nmap scan report for host-3.test.net (192.168.1.3)
Host is up (0.0032s latency).
```

## 4.2 Enumeration

The penetration tester used reconnaissance and enumeration techniques to find out as much information as possible related to the target host. The below sections describe the various techniques used for it.

### 4.2.1 Service Enumeration

The following open ports and services were discovered during the network enumeration phase.

```
(kali@host-1)-[~/Downloads]
$ sudo nmap 10.0.0.3 -p- -sV -sS
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-30 03:13 BST
Illegal character(s) in hostname -- replacing with '*'
Illegal character(s) in hostname -- replacing with '*'
Nmap scan report for http:**www.safebank.local (10.0.0.3)
Host is up (0.00036s latency).
Not shown: 65520 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.53 ((Win64) OpenSSL/1.1.1n PHP/8.1.6)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/http     Apache httpd 2.4.53 ((Win64) OpenSSL/1.1.1n PHP/8.1.6)
445/tcp   open  microsoft-ds?
3306/tcp  open  mysql        MariaDB (unauthorized)
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
49674/tcp open  msrpc        Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-30 04:59 BST
Nmap scan report for safebank.local (192.168.1.3)
Host is up (0.00034s latency).
rDNS record for 192.168.1.3: host-3.test.net
Not shown: 986 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Simple DNS Plus
80/tcp    open  http             Microsoft IIS httpd 10.0
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2024-06-30 03:59:36Z)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
389/tcp   open  ldap             Microsoft Windows Active Directory LDAP (Domain: SAFE BANK.LOCAL0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap         Microsoft Windows Active Directory LDAP (Domain: SAFE BANK.LOCAL0., Site: Default-First-Site-Name)
2179/tcp  open  vmrpd?
3268/tcp  open  ldap             Microsoft Windows Active Directory LDAP (Domain: SAFE BANK.LOCAL0., Site: Default-First-Site-Name)
3269/tcp  open  ssl/ldap         Microsoft Windows Active Directory LDAP (Domain: SAFE BANK.LOCAL0., Site: Default-First-Site-Name)
3389/tcp  open  ms-wbt-server    Microsoft Terminal Services
Service Info: Host: DC-01; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.29 seconds

```

## 4.2.2 Directory Enumeration

Directory enumeration was conducted to find out the hidden folder/directories available on the web application. Directory enumeration is crucial in cyber security, revealing system structures and hidden directories. It aids in vulnerability identification, risk assessment, and penetration testing, contributing to robust security measures by assessing and fortifying potential weaknesses.

```

Floppy Disk
GENERATED WORDS: 4612

--- Scanning URL: https://www.safebank.local/ ---
+ https://www.safebank.local/.svn (CODE:403|SIZE:0)
+ https://www.safebank.local/0 (CODE:301|SIZE:0)
+ https://www.safebank.local/admin (CODE:302|SIZE:0)
+ https://www.safebank.local/admin.cgi (CODE:403|SIZE:199)
+ https://www.safebank.local/akeeba.backend.log (CODE:403|SIZE:0)
+ https://www.safebank.local/AT-admin.cgi (CODE:403|SIZE:199)
+ https://www.safebank.local/atom (CODE:301|SIZE:0)
+ https://www.safebank.local/aux (CODE:403|SIZE:308)
+ https://www.safebank.local/c (CODE:301|SIZE:0)
+ https://www.safebank.local/C (CODE:301|SIZE:0)
+ https://www.safebank.local/cachemgr.cgi (CODE:403|SIZE:199)
+ https://www.safebank.local/co (CODE:301|SIZE:0)
+ https://www.safebank.local/com1 (CODE:403|SIZE:308)
+ https://www.safebank.local/com2 (CODE:403|SIZE:308)
+ https://www.safebank.local/com3 (CODE:403|SIZE:308)
+ https://www.safebank.local/comment-page-1 (CODE:301|SIZE:0)
+ https://www.safebank.local/con (CODE:403|SIZE:308)
+ https://www.safebank.local/cont (CODE:301|SIZE:0)
=> DIRECTORY: https://www.safebank.local/contact/
=> DIRECTORY: https://www.safebank.local/Contact/
+ https://www.safebank.local/dashboard (CODE:302|SIZE:0)
+ https://www.safebank.local/development.log (CODE:403|SIZE:0)
+ https://www.safebank.local/embed (CODE:301|SIZE:0)
+ https://www.safebank.local/examples (CODE:503|SIZE:408)
+ https://www.safebank.local/favicon.ico (CODE:302|SIZE:0)
=> DIRECTORY: https://www.safebank.local/feed/
+ https://www.safebank.local/h (CODE:301|SIZE:0)
+ https://www.safebank.local/H (CODE:301|SIZE:0)
+ https://www.safebank.local/hello (CODE:301|SIZE:0)
+ https://www.safebank.local/home (CODE:301|SIZE:0)
+ https://www.safebank.local/Home (CODE:301|SIZE:0)
+ https://www.safebank.local/index.php (CODE:301|SIZE:0)
-> Testing: https://www.safebank.local/jbossas

```

### 4.3 Vulnerability Assessment

The purpose of vulnerability assessment is to identify and evaluate potential security weaknesses in a system, network, or application, enabling proactive mitigation measures to enhance overall cyber security and reduce the risk of exploitation. The CyberZee used enterprise and professional vulnerability management tools to detect system vulnerabilities as well as web application vulnerabilities.

### 4.4 Exploitation

The purpose of the exploitation phase in penetration testing is to simulate real-world cyber attacks, attempting to exploit identified vulnerabilities to assess the system's resilience and identify potential security weaknesses.

## 5. Detailed Security Findings

### 5.1 10.0.0.3

#### 5.1.1 Inadequate path management

<b>No:</b>	1				
<b>Severity:</b>	<b>Critical</b>	<b>Protocol:</b>	TCP	<b>Port:</b>	80
<b>Description:</b>					
During the penetration testing process that was identified, a remote server contained many deprecated or vulnerable services that may contain severe vulnerabilities. Apache/2.4.53 (Win64) penSSL/1.1.1n PHP/8.1.6					
<b>Impact:</b>					
An attacker could exploit the relevant vulnerabilities and get unauthorized access to the server or other malicious indent using those deprecated services. Also, an attacker could leverage this information to conduct various attack using the known vulnerabilities of the version and retrieved data from the web application and its server.					
<b>Verification:</b>					

```
| Interesting Entries:
| - Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
| - X-Powered-By: PHP/8.1.6
| Found By: Headers (Passive Detection)
| Confidence: 100%
```

**Remediation:**

- Ensure the relevant services are up to date and upgrade to the latest versions that are supported.

### 5.1.2 Deprecated or weak security ciphers are supported (TLS 1.0)

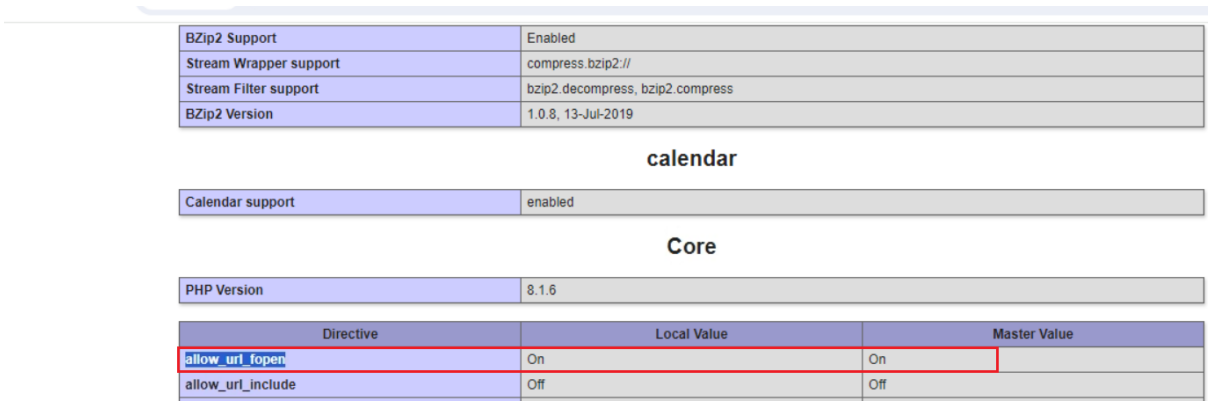
<b>No:</b>	2				
<b>Severity:</b>	Medium	<b>Protocol:</b>	TCP	<b>Port:</b>	80, 443
<b>Description:</b>					
The web server supports encryption through TLS 1.0. TLS 1.0 is not considered to be "strong cryptography" as defined and required by the PCI Data Security Standard 3.2(.1) when used to protect sensitive information transferred to or from web sites. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.					
<b>Impact:</b>					
This file may expose sensitive information that may help an malicious user to prepare more advanced attacks.					
<b>Verification:</b>					
<pre>SSL/TLS Protocols: SSLv2      disabled SSLv3      disabled TLSv1.0    enabled TLSv1.1    enabled TLSv1.2    enabled TLSv1.3    enabled</pre>					
<b>Remediation:</b>					

- It is recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher.

**References:**

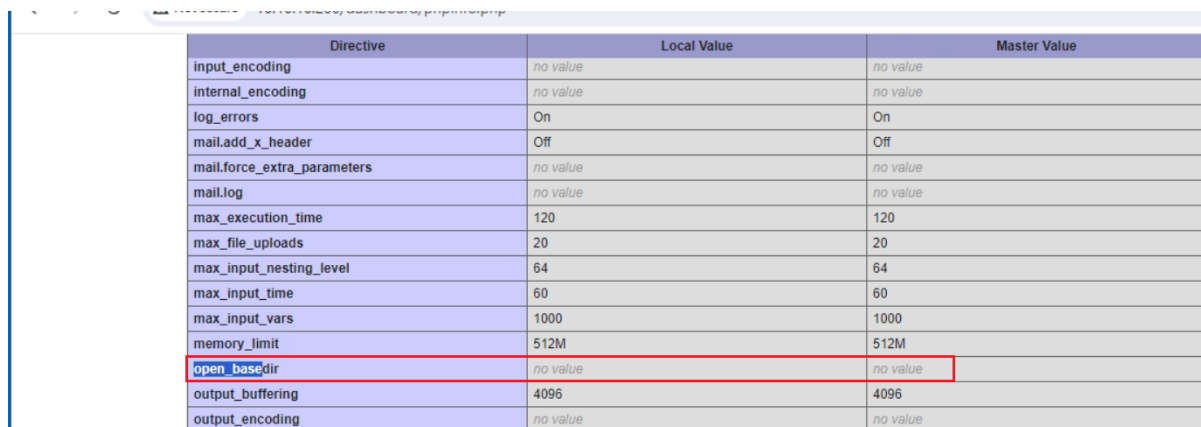
- <https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls>
- <https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2>

### 5.1.3 PHP allow\_url\_fopen enabled

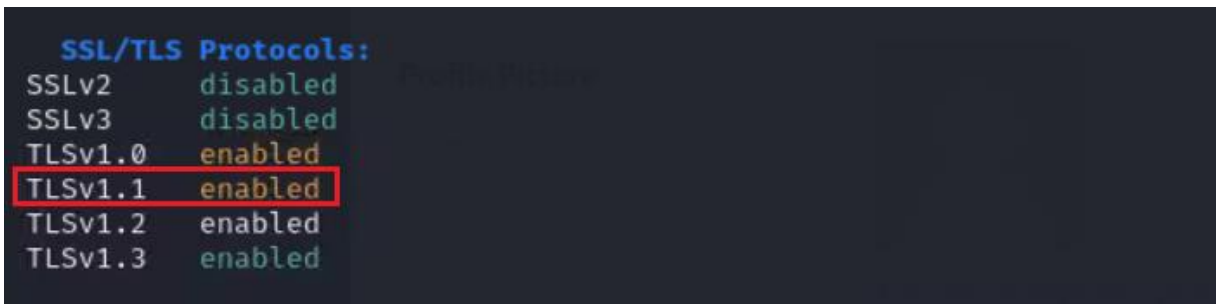
<b>No:</b>	3				
<b>Severity:</b>	Medium	<b>Protocol:</b>	TCP	<b>Port:</b>	80, 443
<b>Description:</b>					
<p>The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering.</p> <p>allow_url_fopen is enabled by default.</p>					
<b>Impact:</b>					
Application dependant - possible remote file inclusion.					
<b>Verification:</b>					
 <p>The screenshot displays various PHP configuration settings. At the top, BZip2 Support is 'Enabled', Stream Wrapper support is 'compress.bzip2://', Stream Filter support is 'bzip2.decompress, bzip2.compress', and BZip2 Version is '1.0.8, 13-Jul-2019'. Below this, the 'calendar' section shows 'Calendar support' as 'enabled'. The 'Core' section shows 'PHP Version' as '8.1.6'. At the bottom, a table lists directives: 'allow_url_fopen' is 'On' (Local Value) and 'On' (Master Value), while 'allow_url_include' is 'Off' (Local Value) and 'Off' (Master Value). The 'allow_url_fopen' row is highlighted with a red border.</p>					
<b>Remediation:</b>					
<ul style="list-style-type: none"> <li>Disable allow_url_fopen from either php.ini (for PHP versions newer than 4.3.4) or .htaccess (for PHP versions up to 4.3.4).</li> <li>php.ini (allow_url_fopen = 'off')</li> <li>.htaccess (php_flag allow_url_fopen off)</li> </ul>					
<b>References:</b>					
<ul style="list-style-type: none"> <li><a href="https://www.php.net/manual/en/filesystem.configuration.php">https://www.php.net/manual/en/filesystem.configuration.php</a></li> </ul>					



### 5.1.4 PHP open\_basedir is not set

No:	4				
Severity:	Medium	Protocol:	TCP	Port:	80, 443
Description:					
<p>The open_basedir configuration directive will limit the files that can be opened by PHP to the specified directory-tree. When a script tries to open a file with, for example, fopen() or gzopen(), the location of the file is checked. When the file is outside the specified directory-tree, PHP will refuse to open it. open_basedir is a good protection against remote file inclusion vulnerabilities. For a remote attacker it is not possible to break out of the open_basedir restrictions if he is only able to inject the name of a file to be included. Therefore the number of files he will be able to include with such a local file include vulnerability is limited.</p> <p>This vulnerability was detected using the information from phpinfo() page.</p> <p>open_basedir: no value</p>					
Impact:					
Application dependant - possible remote code inclusion.					
Verification:					
					
Remediation:					
<ul style="list-style-type: none"><li>Set open_basedir from php.ini</li><li>php.ini (open_basedir = your_application_directory)</li></ul>					

### 5.1.5 Deprecated or weak security ciphers are supported (TLS 1.1)

<b>No:</b>	5				
<b>Severity:</b>	Low	<b>Protocol:</b>	TCP	<b>Port:</b>	80, 443
<b>Description:</b>					
The web server supports encryption through TLS 1.1. When aiming for Payment Card Industry (PCI) Data Security Standard (DSS) compliance, it is recommended (although at the time of writing not required) to use TLS 1.2 or higher instead. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.					
<b>Impact:</b>					
An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.					
<b>Verification:</b>					
 <pre> SSL/TLS Protocols: SSLv2      disabled SSLv3      disabled TLSv1.0    enabled TLSv1.1    enabled TLSv1.2    enabled TLSv1.3    enabled </pre>					
<b>Remediation:</b>					
<ul style="list-style-type: none"> <li>It is recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher.</li> </ul>					
<b>References:</b>					
<ul style="list-style-type: none"> <li><a href="https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls">https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls</a></li> <li><a href="https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2">https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2</a></li> </ul>					

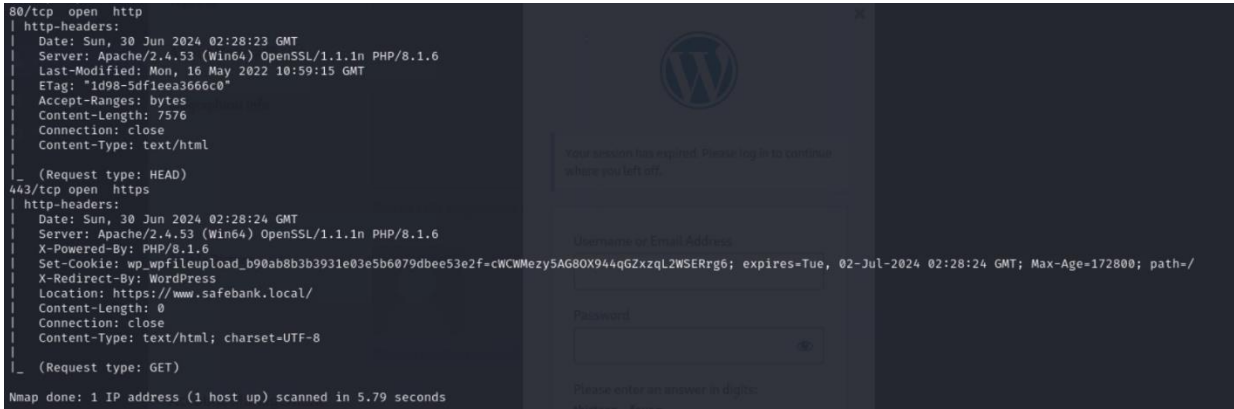
### 5.1.6 PHP info page

No:	6																																						
Severity:	Low	Protocol:	TCP	Port:	80, 443																																		
Description:																																							
PHPinfo page has been found in this directory. The PHPinfo page outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.																																							
Impact:																																							
This file may expose sensitive information that may help an malicious user to prepare more advanced attacks.																																							
Verification:																																							
<div><div><div>10.0.0.3/dashboard/phpinfo.php</div><div>Import bookmarks... Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Target</div></div><div><div>PHP Version 8.1.6</div><div><table><tr><td>System</td><td>Windows NT HTTP-01 10.0 build 20348 (Windows Server 2022) AMD64</td></tr><tr><td>Build Date</td><td>May 11 2022 08:52:54</td></tr><tr><td>Build System</td><td>Microsoft Windows Server 2019 Datacenter [10.0.17763]</td></tr><tr><td>Compiler</td><td>Visual C++ 2019</td></tr><tr><td>Architecture</td><td>x64</td></tr><tr><td>Configure Command</td><td>cscript /nologo /e:javascript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=.\..\..\..\instantclient\sdk\shared" "--with-oci8-19=.\..\..\..\instantclient\sdk\shared" "--enable-object-out-dir=.\obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"</td></tr><tr><td>Server API</td><td>Apache 2.0 Handler</td></tr><tr><td>Virtual Directory Support</td><td>enabled</td></tr><tr><td>Configuration File (php.ini) Path</td><td>no value</td></tr><tr><td>Loaded Configuration File</td><td>C:\xampp1\php\php.ini</td></tr><tr><td>Scan this dir for additional .ini files</td><td>(none)</td></tr><tr><td>Additional .ini files parsed</td><td>(none)</td></tr><tr><td>PHP API</td><td>20210902</td></tr><tr><td>PHP Extension</td><td>20210902</td></tr><tr><td>Zend Extension</td><td>420210902</td></tr><tr><td>Zend Extension Build</td><td>API420210902.TS.VS16</td></tr><tr><td>PHP Extension Build</td><td>API20210902.TS.VS16</td></tr></table></div></div></div>						System	Windows NT HTTP-01 10.0 build 20348 (Windows Server 2022) AMD64	Build Date	May 11 2022 08:52:54	Build System	Microsoft Windows Server 2019 Datacenter [10.0.17763]	Compiler	Visual C++ 2019	Architecture	x64	Configure Command	cscript /nologo /e:javascript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=.\..\..\..\instantclient\sdk\shared" "--with-oci8-19=.\..\..\..\instantclient\sdk\shared" "--enable-object-out-dir=.\obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"	Server API	Apache 2.0 Handler	Virtual Directory Support	enabled	Configuration File (php.ini) Path	no value	Loaded Configuration File	C:\xampp1\php\php.ini	Scan this dir for additional .ini files	(none)	Additional .ini files parsed	(none)	PHP API	20210902	PHP Extension	20210902	Zend Extension	420210902	Zend Extension Build	API420210902.TS.VS16	PHP Extension Build	API20210902.TS.VS16
System	Windows NT HTTP-01 10.0 build 20348 (Windows Server 2022) AMD64																																						
Build Date	May 11 2022 08:52:54																																						
Build System	Microsoft Windows Server 2019 Datacenter [10.0.17763]																																						
Compiler	Visual C++ 2019																																						
Architecture	x64																																						
Configure Command	cscript /nologo /e:javascript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=.\..\..\..\instantclient\sdk\shared" "--with-oci8-19=.\..\..\..\instantclient\sdk\shared" "--enable-object-out-dir=.\obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"																																						
Server API	Apache 2.0 Handler																																						
Virtual Directory Support	enabled																																						
Configuration File (php.ini) Path	no value																																						
Loaded Configuration File	C:\xampp1\php\php.ini																																						
Scan this dir for additional .ini files	(none)																																						
Additional .ini files parsed	(none)																																						
PHP API	20210902																																						
PHP Extension	20210902																																						
Zend Extension	420210902																																						
Zend Extension Build	API420210902.TS.VS16																																						
PHP Extension Build	API20210902.TS.VS16																																						
Remediation:																																							
Remove the file from production systems.																																							
References:																																							
https://www.php.net/manual/en/function.phpinfo.php																																							

### 5.1.7 HTTP strict transport security (HSTS) not implemented

<b>No:</b>	7				
<b>Severity:</b>	Low	<b>Protocol:</b>	TCP	<b>Port:</b>	80, 443
<b>Description:</b>					
HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessible using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response.					
<b>Impact:</b>					
HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks.					
<b>Verification:</b>					
					
<b>Remediation:</b>					
<ul style="list-style-type: none"><li>It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information.</li></ul>					
<b>References:</b>					
<ul style="list-style-type: none"><li><a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security</a></li><li><a href="https://hstspreload.org/">https://hstspreload.org/</a></li></ul>					

### 5.1.8 X-Frame-Options header missing

<b>No:</b>	8				
<b>Severity:</b>	Low	<b>Protocol:</b>	TCP	<b>Port:</b>	80
<b>Description:</b>					
<p>Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.</p> <p>The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.</p>					
<b>Impact:</b>					
The impact depends on the affected web application.					
<b>Verification:</b>					
 <pre> 80/tcp open  http  _ http-headers:     Date: Sun, 30 Jun 2024 02:28:23 GMT     Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6     Last-Modified: Mon, 16 May 2022 10:59:15 GMT     ETag: "1d98-5dfilea3666c0"     Accept-Ranges: bytes     Content-Length: 7576     Connection: close     Content-Type: text/html  _  _ (Request type: HEAD) 443/tcp open  https  _ http-headers:     Date: Sun, 30 Jun 2024 02:28:24 GMT     Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6     X-Powered-By: PHP/8.1.6     Set-Cookie: wp_wpfileupload_b90ab8b3b3931e03e5b6079dbec53e2f-cWCMMezy5AG80X944qGZxqL2WSErRg6; expires=Tue, 02-Jul-2024 02:28:24 GMT; Max-Age=172800; path=/     X-Redirect-By: WordPress     Location: https://www.safebank.local/     Content-Length: 0     Connection: close     Content-Type: text/html; charset=UTF-8  _  _ (Request type: GET) Nmap done: 1 IP address (1 host up) scanned in 5.79 seconds </pre>					
<b>Remediation:</b>					
<ul style="list-style-type: none"> <li>Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.</li> </ul>					
<b>References:</b>					
<ul style="list-style-type: none"> <li><a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options</a></li> <li><a href="https://en.wikipedia.org/wiki/Clickjacking">https://en.wikipedia.org/wiki/Clickjacking</a></li> </ul>					

- [https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking\\_Defense\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html)

### 5.1.9 Content Security Policy (CSP) not implemented

<b>No:</b>	9				
<b>Severity:</b>	Low	<b>Protocol:</b>	TCP	<b>Port:</b>	80
<b>Description:</b>					
<p>Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.</p> <p>Content Security Policy (CSP) can be implemented by adding a Content-Security-Policy header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:</p> <p><i>Content-Security-Policy:</i></p> <pre>default-src 'self'; script-src 'self' https://code.jquery.com;</pre> <p>It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.</p>					
<b>Impact:</b>					
<p>CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.</p>					
<b>Verification:</b>					

<pre>80/tcp open  http   http-headers:     Date: Sun, 30 Jun 2024 02:28:23 GMT     Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6     Last-Modified: Mon, 16 May 2022 10:59:15 GMT     ETag: "1d98-5df1eea3666c0"     Accept-Ranges: bytes     Content-Length: 7576     Connection: close     Content-Type: text/html    _ (Request type: HEAD) 443/tcp open  https   http-headers:     Date: Sun, 30 Jun 2024 02:28:24 GMT     Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6     X-Powered-By: PHP/8.1.6     Set-Cookie: wp_wplfileupload_b90ab8b3b3931e03e5b6079dbee53e2f-cWCWMezy5AG80X944qGZxzqL2WSErrg6; expires=Tue, 02-Jul-2024 02:28:24 GMT; Max-Age=172800; path=/     X-Redirect-By: WordPress     Location: https://www.safebank.local/     Content-Length: 0     Connection: close     Content-Type: text/html; charset=UTF-8    _ (Request type: GET) Nmap done: 1 IP address (1 host up) scanned in 5.79 seconds</pre>	
<b>Remediation:</b>	
<ul style="list-style-type: none"><li>It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.</li></ul>	
<b>References:</b>	
<ul style="list-style-type: none"><li><a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP">https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP</a></li><li><a href="https://hacks.mozilla.org/2016/02/implementing-content-security-policy/">https://hacks.mozilla.org/2016/02/implementing-content-security-policy/</a></li></ul>	





### 5.2.2 Insufficient password policy implementation

[illegible]

**Remediation:**

- Utilize unique local admin passwords. Limit local admin users via least privilege. Consider implementing a PAM solution. For full mitigation and detection guidance, please reference the MITRE guidance [here](#).

**5.3 192.168.1.3****5.3.1 DNS Server Spoofed Request Amplification DDoS**

<b>No:</b>	1				
<b>Severity:</b>	<b>High</b>	<b>Protocol:</b>	UDP	<b>Port:</b>	53
<b>Description:</b>					
The remote DNS server answers to any request. It is possible to query the name servers (NS) of the root zone ('.') and get an answer that is bigger than the original request. By spoofing the source IP address, a remote attacker can leverage this 'amplification' to launch a denial of service attack against a third-party host using the remote DNS server.					
<b>Impact:</b>					
This vulnerability allows attackers to amplify DNS requests, flooding targets with excessive traffic. It leads to network congestion, service outages, and potential financial losses, necessitating robust security measures to mitigate such DDoS attacks effectively.					
<b>Verification:</b>					
<pre>The DNS query was 17 bytes long, the answer is 241 bytes long.</pre>					
<b>Remediation:</b>					
<ul style="list-style-type: none"> <li>▪ Restrict access to your DNS server from public network or reconfigure it to reject such queries.</li> </ul>					

### 5.3.2 SSL 64-bit Block Size Cipher Suites Supported (SWEET32)

<b>No:</b>	2				
<b>Severity:</b>	<b>High</b>	<b>Protocol:</b>	TCP	<b>Port:</b>	636/ldap, 3269/ldap, 3389/msrdp, 3269/ldap, 3389/msrdp
<b>Description:</b>					
<p>The remote host supports the use of a block cipher with 64-bit blocks in one or more cipher suites. It is, therefore, affected by a vulnerability, known as SWEET32, due to the use of weak 64-bit block ciphers. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.</p> <p>Proof-of-concepts have shown that attackers can recover authentication cookies from an HTTPS session in as little as 30 hours.</p> <p>Note that the ability to send a large number of requests over the same TLS connection between the client and server is an important requirement for carrying out this attack. If the number of requests allowed for a single connection were limited, this would mitigate the vulnerability. This plugin requires report paranoia as Nessus has not checked for such a mitigation.</p>					
<b>Impact:</b>					
<p>The SSL 64-bit Block Size Cipher Suites Supported (SWEET32) vulnerability allows attackers to decrypt encrypted data due to weak 64-bit block ciphers. This compromises data confidentiality, potentially exposing sensitive information transmitted over affected SSL/TLS connections.</p>					
<b>Verification:</b>					

List of 64-bit block cipher suites supported by the remote server :

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name Code KEX Auth Encryption MAC

-----  
DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1

The fields above are :

{Tenable ciphername}

{Cipher ID code}

Kex={key exchange}

Auth={authentication}

Encrypt={symmetric encryption method}

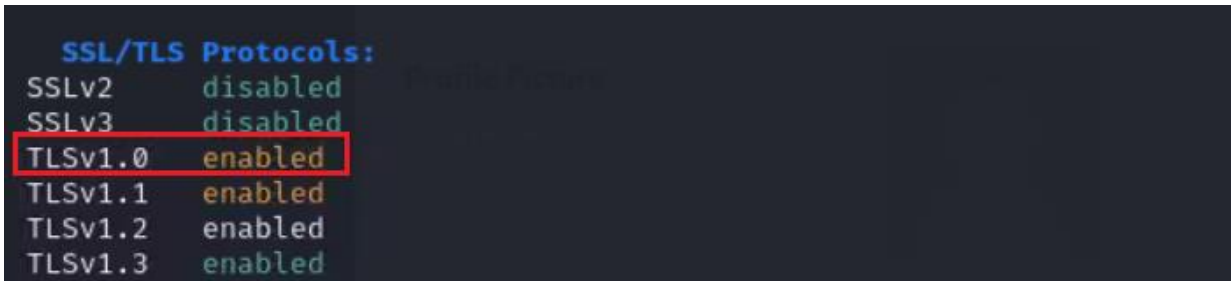
MAC={message authentication code}

{export flag}

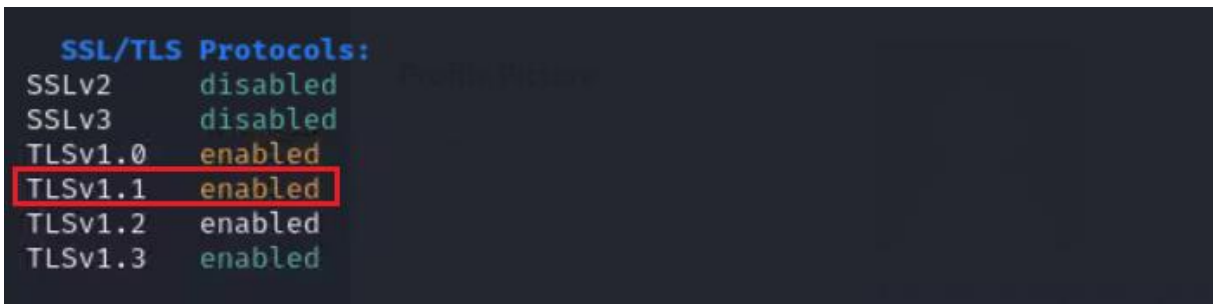
### Remediation:

- Reconfigure the affected application, if possible, to avoid use of all 64-bit block ciphers. Alternatively, place limitations on the number of requests that are allowed to be processed over the same TLS connection to mitigate this vulnerability.

### 5.3.3 Deprecated or weak security ciphers are supported (TLS 1.0)

<b>No:</b>	3				
<b>Severity:</b>	Medium	<b>Protocol:</b>	TCP	<b>Port:</b>	80, 443
<b>Description:</b>					
The web server supports encryption through TLS 1.0. TLS 1.0 is not considered to be "strong cryptography" as defined and required by the PCI Data Security Standard 3.2(.1) when used to protect sensitive information transferred to or from web sites. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.					
<b>Impact:</b>					
This file may expose sensitive information that may help an malicious user to prepare more advanced attacks.					
<b>Verification:</b>					
 <pre> SSL/TLS Protocols: SSLv2      disabled SSLv3      disabled TLSv1.0    enabled TLSv1.1    enabled TLSv1.2    enabled TLSv1.3    enabled </pre>					
<b>Remediation:</b>					
<ul style="list-style-type: none"> <li>It is recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher.</li> </ul>					
<b>References:</b>					
<ul style="list-style-type: none"> <li><a href="https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls">https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls</a></li> <li><a href="https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2">https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2</a></li> </ul>					

### 5.3.4 Deprecated or weak security ciphers are supported (TLS 1.1)

<b>No:</b>	4				
<b>Severity:</b>	Low	<b>Protocol:</b>	TCP	<b>Port:</b>	80, 443
<b>Description:</b>					
The web server supports encryption through TLS 1.1. When aiming for Payment Card Industry (PCI) Data Security Standard (DSS) compliance, it is recommended (although at the time of writing not required) to use TLS 1.2 or higher instead. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.					
<b>Impact:</b>					
An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.					
<b>Verification:</b>					
 <pre> SSL/TLS Protocols: SSLv2      disabled SSLv3      disabled TLSv1.0    enabled TLSv1.1    enabled TLSv1.2    enabled TLSv1.3    enabled </pre>					
<b>Remediation:</b>					
<ul style="list-style-type: none"> <li>It is recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher.</li> </ul>					
<b>References:</b>					
<ul style="list-style-type: none"> <li><a href="https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls">https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls</a></li> <li><a href="https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2">https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2</a></li> </ul>					