Logo, company name

Description automatically generated

**Penetration Testing Report**

Ethical Hacking

Company:

**Frozen Yoghurt LTD**

**Date:** 31/03/2023

**Table of Contents:**

**Executive Summary:  3**

**Summary of Findings: 3**

**Vulnerability Findings of Windows Server:**

[CVE](https://en.wikipedia.org/wiki/CVE_(identifier))-[2017-014](https://www.cve.org/CVERecord?id=CVE-2017-0144)4 - [Server Message Block](https://en.wikipedia.org/wiki/Server_Message_Block) (SMB) protocol **4**

Attack Narrative **4**

CWE-139 - Use of Default Credentials **7**

Attack Narrative **7**

CVE-[2020-11107](https://nvd.nist.gov/vuln/detail/CVE-2020-11107) - XAMPP Local Privilege Escalation **10**

Attack Narrative  **10**

CWE-521 ‒ Use of weak passwords **14**

Attack Narrative **14**

CVE 284 - Improper Access Control allows for Privilege Escalation **16**

Attack Narrative  **16**

**Conclusion: 22**

**Recommendations: 22**

**References: 23**

**Executive Summary:**

This Penetration Test was performed on Frozen Yougert Ltd. The purview of this investigation was restricted to one local machine running the company’s software. The Intention of this Penetration Test was to Identify and exploit vulnerabilities within the target system with the aim to access sensitive information.

Each Vulnerability found and exploited was completed in three critical phases: Reconnaissance, Enumeration and Exploitation.

Reconnaissance involves the scanning of each system to recognize open ports and what services are running on each. Enumeration involves finding out more information about these open ports, including the service version of each, which can lead an investigator to known vulnerabilities. And finally, Exploitation involves multiple techniques found in the prior phases that are used to gain access to the system in order to disclose sensitive information.

**Summary of Findings:**

Within the first phase of the Penetration Test; Reconnaissance, we were able to discover many open ports on the target machine such as the very vulnerable port 445, which runs SMB, which can be exploited as demonstrated in **Figure 1.**

Diagram, schematic

Description automatically generated

**Figure 1 -** Demonstration of [CVE-201](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7494)7-0144

A series of vulnerabilities were found while inside the local machine, including passwords left in plain text on the desktop screen, default passwords being used for svices such as phpMyAdmin. Many services which were active on the target machine were running severely old versions, which were vulnerable. For example, Xampp v7.4.3 which can be exploited as shown in **Figure 2**.

A screenshot of a computer

Description automatically generated with low confidence

**Figure 2 -** Demonstration of CVE-[2020-11107](https://nvd.nist.gov/vuln/detail/CVE-2020-11107)

Shape

Description automatically generated

**Vulnerabilities Within Windows Machine**

| [**CVE-201**](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7494)**7-0144:**   [Server Message Block](https://en.wikipedia.org/wiki/Server_Message_Block) Remote Code Execution | | |
| --- | --- | --- |
| **RISK/  CVS:** | **Critical** | **9.3** |
| **TOOLS:** | Metasploit | |
| **Description:** | A vulnerability within SMB allows an attacker to send crafted packets to the target system which allows remote code execution. | |
| **Impact:** | It allows the attacker to gain admin level privileges, meaning complete integrity compromise of the system, all system files are compromised | |
| **Recommendation** | Update the Windows the version to the latest release (Windows 11) | |

**Attack Narrative:**

The reconnaissance of the Linux machine using the nmap scan ‘**nmap -sV -A [IP]’** found port 445 was open, this runs the SMB service for windows which allows file sharing between windows machines. This metasploit module exploits the vulnerability within the SMB service and how it handles specifically crafted packets. So, by sending a specifically crafted packet of the right size it can cause a buffer overflow, which allows us to gain a meterpreter shell, which allows us access to advanced features, for example downloading all user’s password hashes from the SAM (Security Accounts Manager) which we can then try and break.

**Text

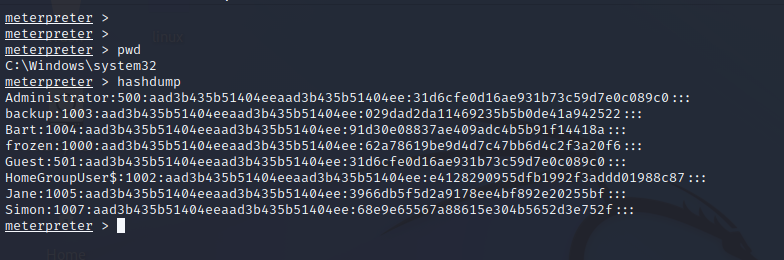
Description automatically generated**

**Figure 1 -** An Nmap scan showed that a number of ports are open, including the important 44

**Text

Description automatically generated**

**Figure 2 -** Meterpreter shell access after completing the exploit.

****

**Figure 3 -** Downloading the user password hashes from the meterpreter shell

| [**C**](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7494)**WE-1392:** Use of Default Credentials | | |
| --- | --- | --- |
| **RISK/  CVS:** | **Critical** | **9.1** |
| **TOOLS:** | Nikto v2.1.6 | |
| **Description:** | The phpMyAdmin login page, specifically user ‘root’ has default credentials | |
| **Impact:** | An attacker can have full access to all tables, meaning all sensitive information within them is accessible and or changeable. An attacker will be able to create new accounts or access already existing ones, and possibly gain access to other parts of the system. | |
| **Recommendation:** | Make sure any user accounts on this service change their passwords to meet the requirements of Digital Identity Guidelines (NIST SP 800-63B). | |

**Attack Narrative:**

Doing some reconnaissance with Nikto has found numerous directories under the IP address of the windows target machine, including a directory called ‘/phpMyAdmin/’. This is an open-source web tool that handles MySQL databases. But this tool has not been configured properly, or at all, as by simply researching for xampp default passwords we found the right pair ‘root & no password’, this allows us to have full access to all SQL databases, with the ability to change the data. With further investigation this set of passwords was also kept in a text file for which any user on the system could access.

**Text

Description automatically generated**

**Figure 1 -** Nikto scam on windows target machine on port 80 showing numerous directories.

**Graphical user interface

Description automatically generated**

**Figure 2 -** The phpMyAdmin login page

Graphical user interface, text, application, email

Description automatically generated

**Figure 3 -** Access to all User accounts within MySQl and all Databases

| **CVE-**[**2020-11107**](https://nvd.nist.gov/vuln/detail/CVE-2020-11107)**:** XAMPP 7.4.3 Privilege Escalation | | |
| --- | --- | --- |
| **RISK/  CVS:** | **High** | **8.8** |
| **TOOLS:** | Windows Powershell, Xampp v7.4.3 | |
| **Description:** | A vulnerability within SMB allows an attacker to send crafted packets to the target system which allows remote code execution. | |
| **Impact:** | It allows the attacker to gain admin level privileges, meaning complete integrity compromise of the system, all system files are compromised | |
| **Recommendation:** | Update the Windows Operating System to the latest version (Windows 11) or disable the NetBIOS service running on port 445 | |

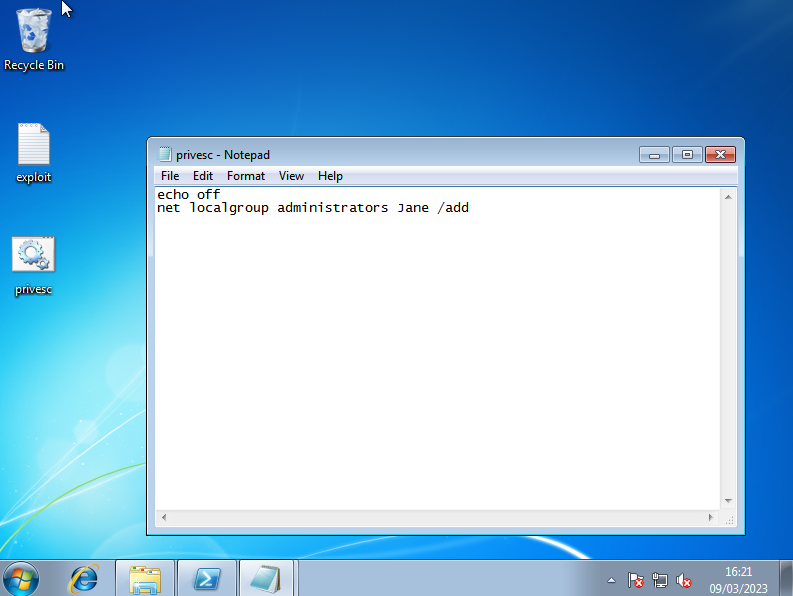
**Attack Narrative:**

The xampp files are able to be looked at by any user. Within this exploit we make a BAT file (Windows Batch file; Contains windows commands), see **Figure 2,** within powershell we type 4 commands, these replace a line inside the config file which replaces the original editor (Notepad.exe) for xampp with our batch file (**Figure 3)**. So, when an xampp user tries to access the log files; which it needs a text editor for, it runs our file instead, which in turn adds Jane to the Administrator local group, elevating her privileges.

**Graphical user interface

Description automatically generated**

**Figure 1** - Image showing user Janes Privileges before exploit.

****

**Figure 2 -** A BAT file including the windows command to add a user to Admin group.

**Text

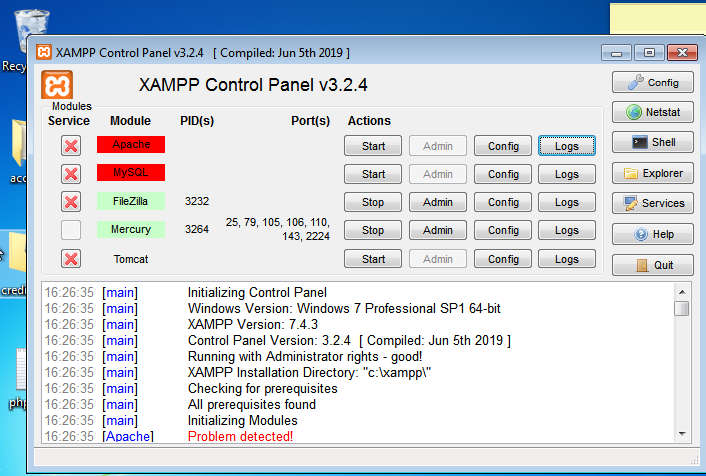
Description automatically generated**

**Figure 3 -** Image showing 4 commands entered into powershell.

**Graphical user interface, text, application

Description automatically generated**

**Figure 4 -** Xampp Config control file now shows our privesc.bat file as its editor.

****

**Figure 4 -** Xampp logs have been pressed to initiate BAT file

**A computer screen capture

Description automatically generated with medium confidence**

**Figure 6 -** User Jane now has Administrator local group Privileges.

| **CWE-521** ‒ Use of weak passwords | | |
| --- | --- | --- |
| **RISK/  CVS:** | **Medium** | **5.5** |
| **TOOLS:** | Hashcat v6.2.6 | |
| **Description:** | Users of the policy (NIST SP 800-63B) are not required to use secure passwords, which makes it simpler for attackers to access user accounts. | |
| **Impact:** | The acquired hashes are able to be cracked through a dictionary attack, 3 out of 8 passwords were cracked in under 2 seconds. 1 of which has Administrator Privileges, meaning all system integrity is lost. | |
| **Recommendation:** | Make sure all users on the machine change their passwords to meet Digital Identity Guidelines (NIST SP 800-63B) | |

**Attack Narrative:**

These hashes were retrieved from the Eternal Blue exploit in Vulnerability 1. The format of these hashes is NTLM (Microsoft's Default hash type). Again, similar to linux these hashes are susceptible to a Dictionary attack, using the same wordlist as before we were able to crack 3 of these hashes (**Figure 2**) which include, Jane, Frozen and Guest User. The rest of the hashes were not cracked due to them not being in the wordlist I used.

**Text

Description automatically generated**

**Figure 1 -** All User accounts NTLM hashes

**Text

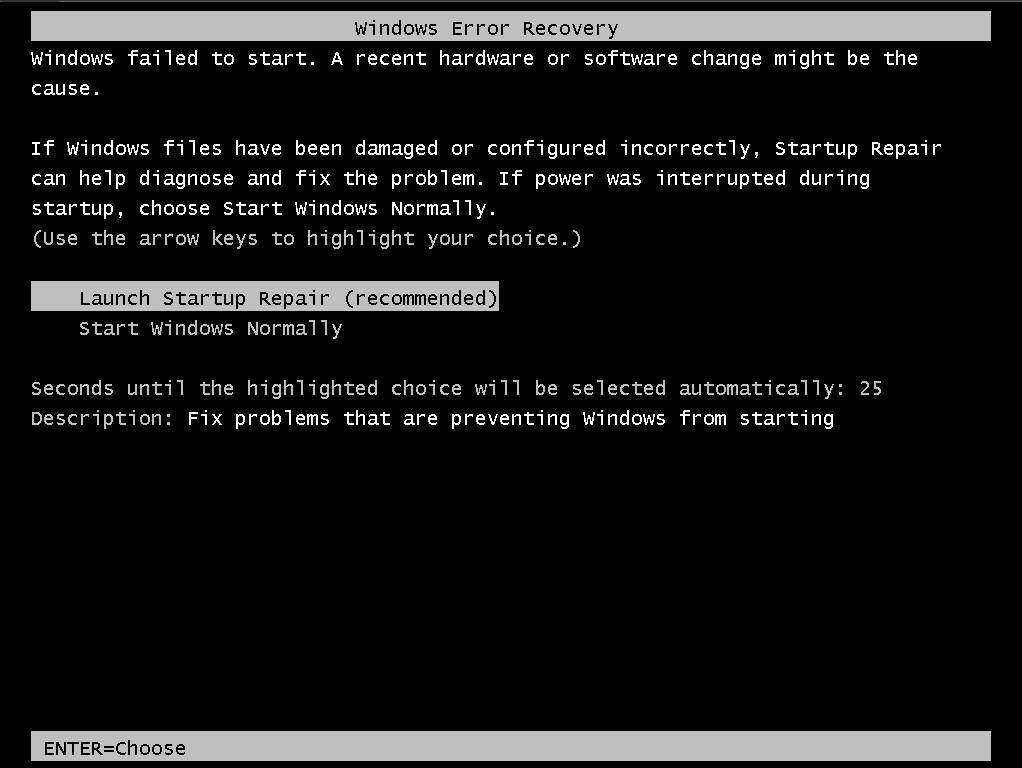
Description automatically generated**

**Figure 2 -** The output of Hashcat program after cracking the windows hashes.

| **CWE-284** - Improper Access Control | | |
| --- | --- | --- |
| **RISK/  CVS:** | **High** | **7.8** |
| **TOOLS:** | Windows Startup Repair Tool, Windows Command Prompt | |
| **Description:** | The Windows Startup Repair Tools allow a user to gain access to an Administrator shell by changing the name of a sticky key’s application. | |
| **Impact:** | The impact is very high, a user with no privileges can gain full access to the entirety of the system, meaning all files can be accessed. | |
| **Recommendation:** | Disable the sticky key’s function, Disable Windows Startup Repair Tool and or Upgrade to the newest version of Windows (11) | |

**Attack Narrative:**

This exploit starts by entering the Windows Startup Repair Tool (WSRT), done by shutting down windows while restarting the VM. After the WSRT has finished a pop-up menu will appear, in which a text file, present in **Figure 2**, will be displayed. This gives us access to the whole machine's files system, from here a file called ‘sethc’ which is the Application for the sticky keys service. When the shift bar is run 5 times, this application is run, so by changing the name of the Windows Command Prompt to ‘sethc’ (See **Figure 4)** we can launch an Administrator Shell just by clicking the shift key 5 times. (**Figure 5)**. From gaining the Administrator shell really anything is possible, but I decided to create a new user account with the name ‘pentester’ and add it to the local group ‘Administrators’ (**Figures 6 & 7)**. I did this to show what is the possible impact of this vulnerability.

****

**Figure 1 -** Windows Startup Repair tool in BIOS startup

**Graphical user interface, application

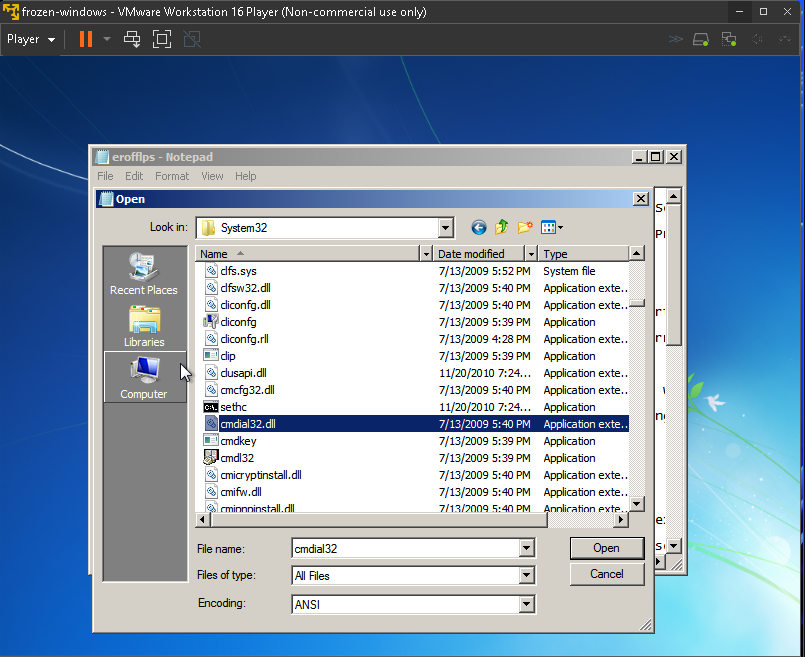
Description automatically generated**

**Figure 2 -** Startup Repair giving a link to a txt file.

**Graphical user interface, application

Description automatically generated**

**Figure 3 -** Renaming the ‘sethc’ sticky keys application to ‘sethc.OLD’

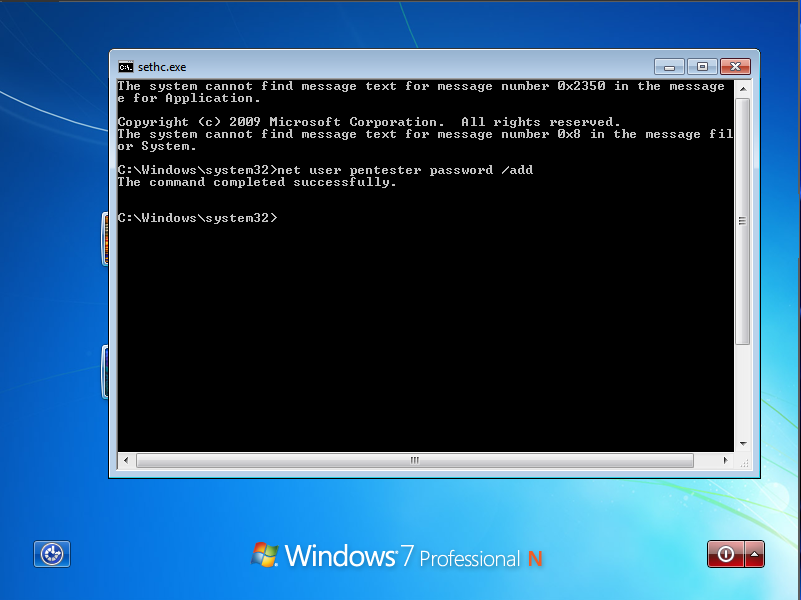
****

**Figure 4 -** Renaming the Windows Command Prompt Application to ‘sethc’

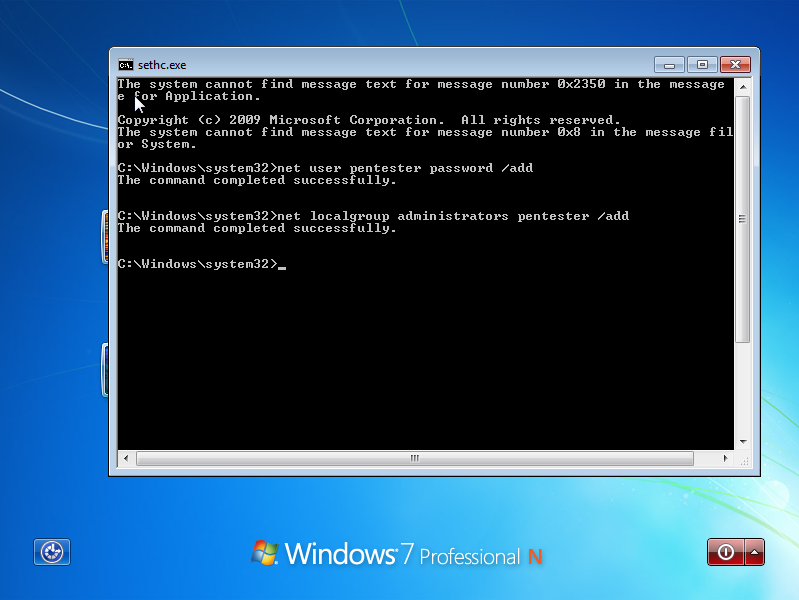
**Graphical user interface, website

Description automatically generated**

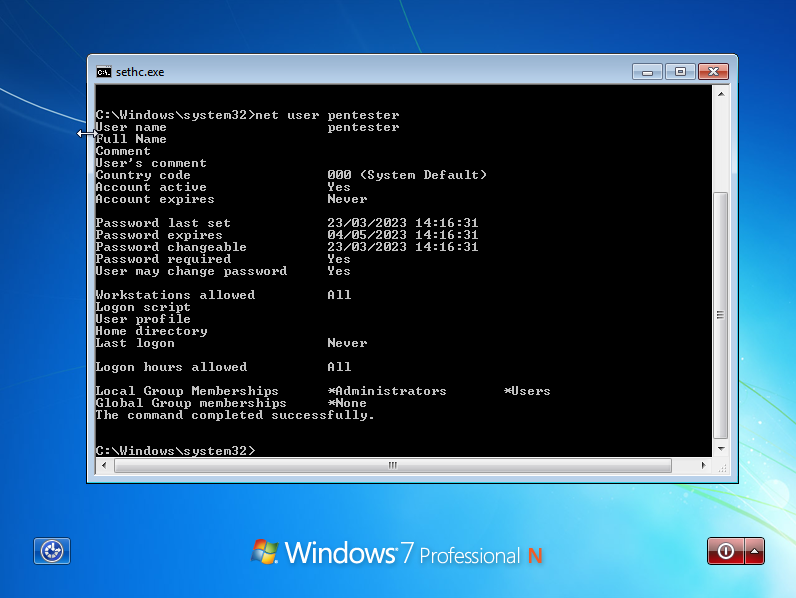
**Figure 5 -** Showing instance of command prompt with admin rights running on login screen.

****

**Figure 6 -** Adding the user ‘pentester’ to the windows machine.

****

**Figure 7 -** Adding the user ‘pentester’ to the local group administrators.

****

**Figure 8 -** Showing user ‘pentester’ privileges

**Graphical user interface, website

Description automatically generated**

**Figure 9 -** showing user ‘pentester’ on the login page.

**Conclusion**

This Penetration test on the Frozen Yougert Windows Machine found numerous dangerous vulnerabilities that endanger the company’s security and data, these include vulnerabilities but are not limited to keeping passwords in clear text on the machines home screen, default credentials for running software and using vulnerable versions of software.

I highly recommend using the following recommendations otherwise a bad actor may exploit these vulnerabilities and have access to your employee and customer data.

Hopefully by taking these important measures Frozen Yougert can have a solid security barrier around its data, meaning all sensitive information within the company cannot be accessed.

**Recommendations**

* Make sure the Digital Identity Guidelines (NIST SP 800-63B) format is compulsory for all new users and change all passwords of current users to meet this requirement. Also change all services running which use a password to fulfill this requirement.
* Make sure passwords are not stored in plaintext on the home screen of a machine or visible to any outsider.
* Update this machine to its newest operating system version: Windows 11
* Follow the NIST Special Publication 800-53 guidelines to ensure privilege management is obeyed.
* Update all running versions of software to the latest available.

**References:**

*CVE-2017-0144 : The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows*. (2017). Cvedetails.com. <https://www.cvedetails.com/cve/CVE-2017-0144/>

*CVE-2020-11107 : An issue was discovered in XAMPP before 7.2.29, 7.3.x before 7.3.16 , and 7.4.x before 7.4.4 on Windows. An unprivileged*. (n.d.). Www.cvedetails.com. Retrieved March 24, 2023, from https://www.cvedetails.com/cve/CVE-2020-11107/

*CWE - CWE-284: Improper Access Control (4.2)*. (n.d.). Cwe.mitre.org. https://cwe.mitre.org/data/definitions/284.html

*CWE - CWE-312: Cleartext Storage of Sensitive Information (4.4)*. (n.d.). Cwe.mitre.org. <https://cwe.mitre.org/data/definitions/312.html>

*CWE - CWE-521: Weak Password Requirements (4.1)*. (n.d.). Cwe.mitre.org. <https://cwe.mitre.org/data/definitions/521.html>

*CWE - CWE-1392: Use of Default Credentials (4.10)*. (n.d.). Cwe.mitre.org. Retrieved March 24, 2023, from https://cwe.mitre.org/data/definitions/1392.html

*Microsoft CVE-2017-0144: Windows SMB Remote Code Execution Vulnerability*. (n.d.). Rapid7. https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-0144/#:~:text=Description

NIST. (2019). *NIST Special Publication 800-63B*. Nist.gov. <https://pages.nist.gov/800-63-3/sp800-63b.html>

NIST. (2020, September 23). *Security and Privacy Controls for Information Systems and Organizations*. Csrc.nist.gov. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

*PHPMyAdmin Default login password*. (n.d.). Stack Overflow. <https://stackoverflow.com/questions/5818358/phpmyadmin-default-login-password>

National Institute of Standards and Technology. (n.d.-b). *NVD - CVSS v3 Calculator*. Nvd.nist.gov. https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator