Node

Synopsis

Node focuses mainly on newer software and poor configurations. The machine starts out seemingly easy, but gets progressively harder as more access is gained. In-depth enumeration is required at several steps to be able to progress further into the machine.

Skills

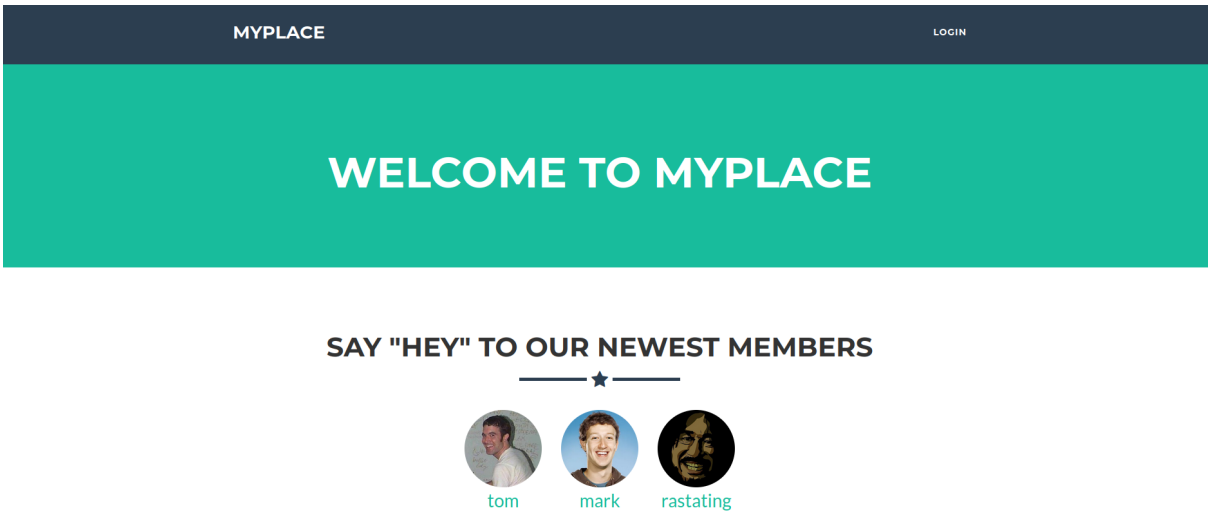
- Knowledge of Linux
- Exploiting buffer overflow
- Bypassing user-agent filtering
- Bypassing ASLR and NX

Exploitation

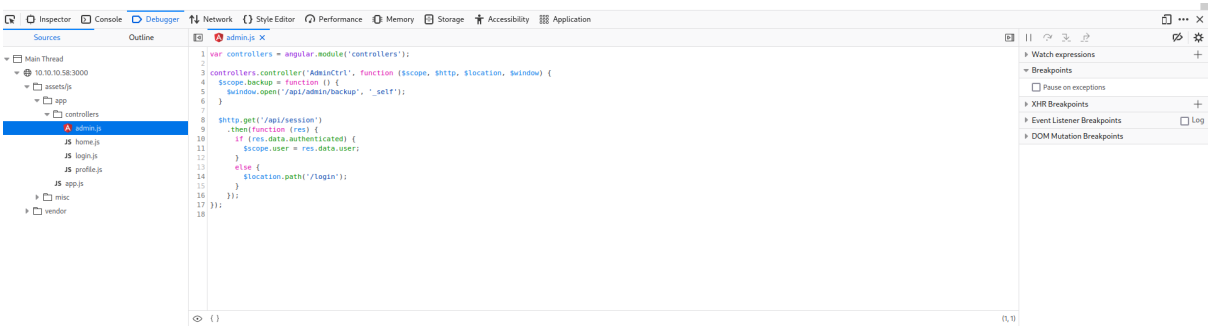
As always we start with the nmap to check what services/ports are open

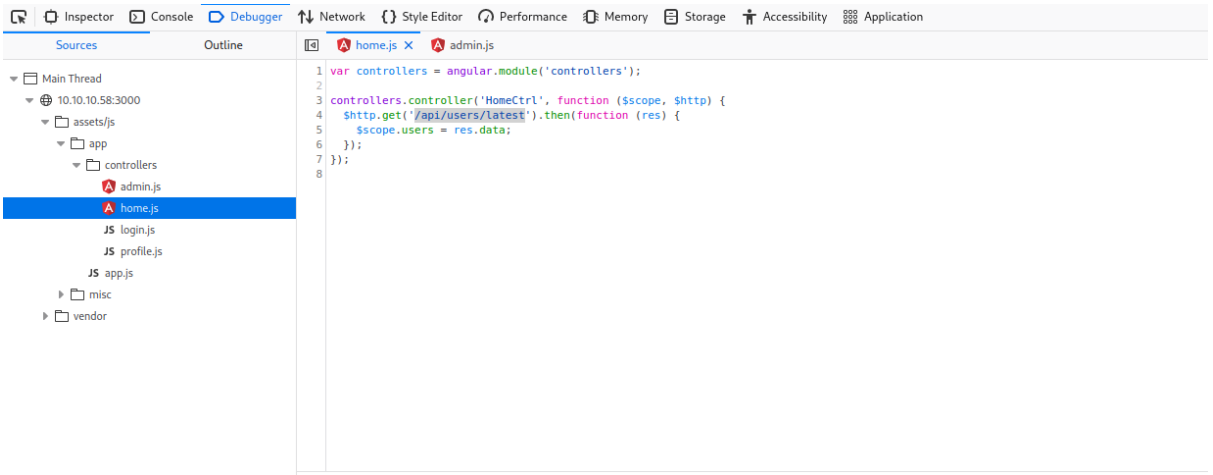
```
└─# nmap -A 10.10.10.58
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-17 09:58 EDT
Nmap scan report for 10.10.10.58 (10.10.10.58)
Host is up (0.095s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE            VERSION
22/tcp   open  ssh                OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dc5e34a625db43eceb40f4967b8ed1da (RSA)
|   256 6c8e5e5f4fd5417d1895d1dc2e3fe59c (ECDSA)
|_  256 d878b85d85ffad7be6e2b5da1e526236 (ED25519)
3000/tcp open  hadoop-tasktracker Apache Hadoop
| hadoop-datanode-info:
|_  Logs: /login
| hadoop-tasktracker-info:
|_  Logs: /login
|_http-title: MyPlace
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (92%), Linux 3.12 (92%), Linux 3.13 (92%), Linux 3.13 or 4.2 (92%), Linux 3.16 (92%), Linux 3.16 - 4.6 (92%), Linux
3.2 - 4.9 (92%), Linux 3.8 - 3.11 (92%), Linux 4.2 (92%), Linux 4.4 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   103.98 ms 10.10.14.1 (10.10.14.1)
2   103.96 ms 10.10.10.58 (10.10.10.58)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.90 seconds
```

Opening the browser give us the following web page

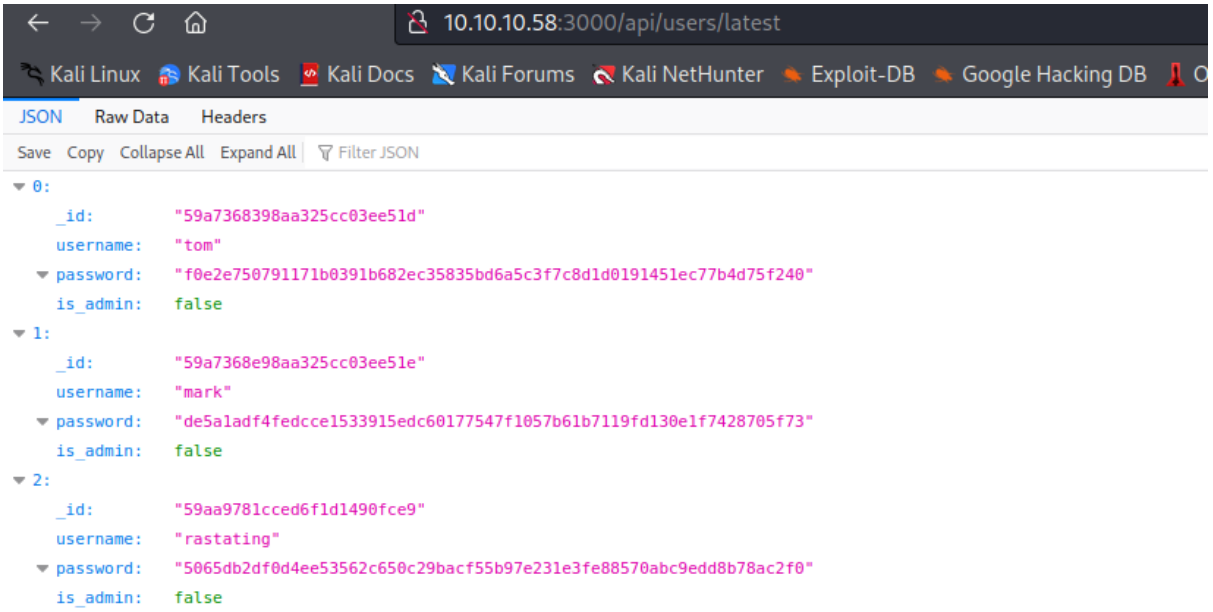


Let’s check the web console and examine a soruce code of javascript files



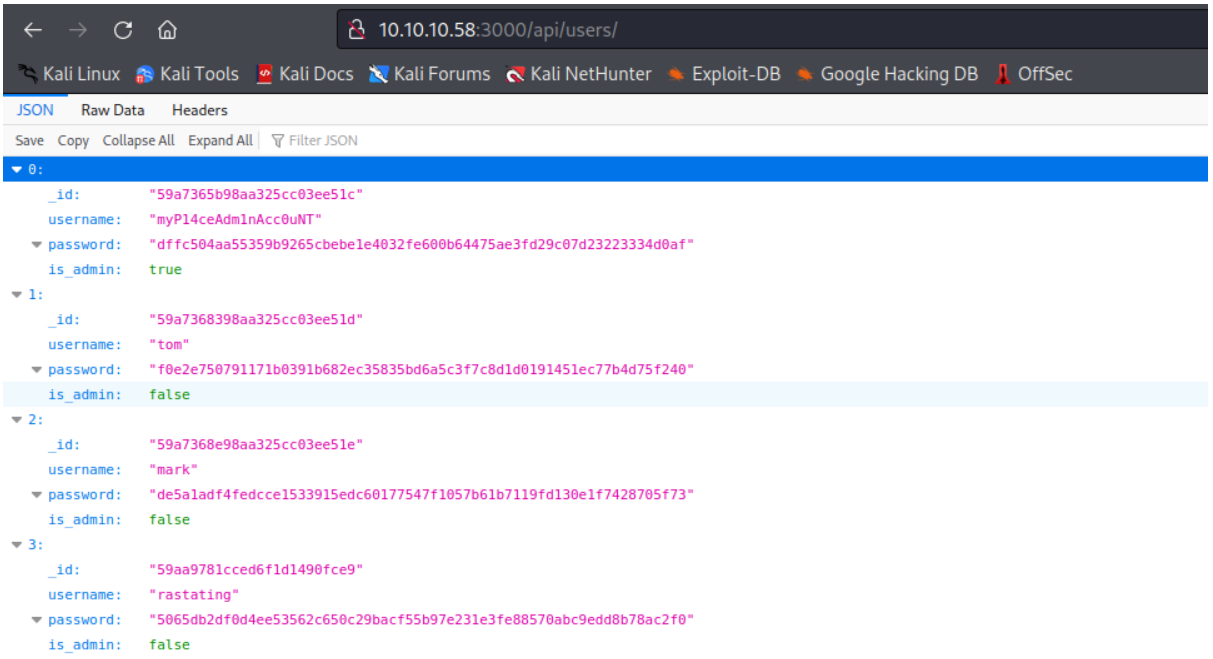


Review of the publcily available source code reviewed a few interesting urls, let’s then check their content



By accessing /api/users/latest (whcih we got from source code examination) we got a few hashed credentials for users

But, let's remove /latest from the url to check if there are more users



By doing so we got one more user, which looks like is an admin user

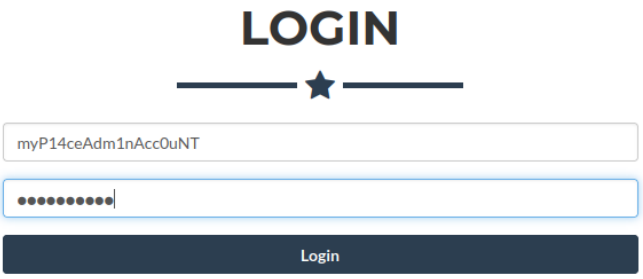
Now with those hashed passwords we can launch hashcat ot crack them and get plain text credentials

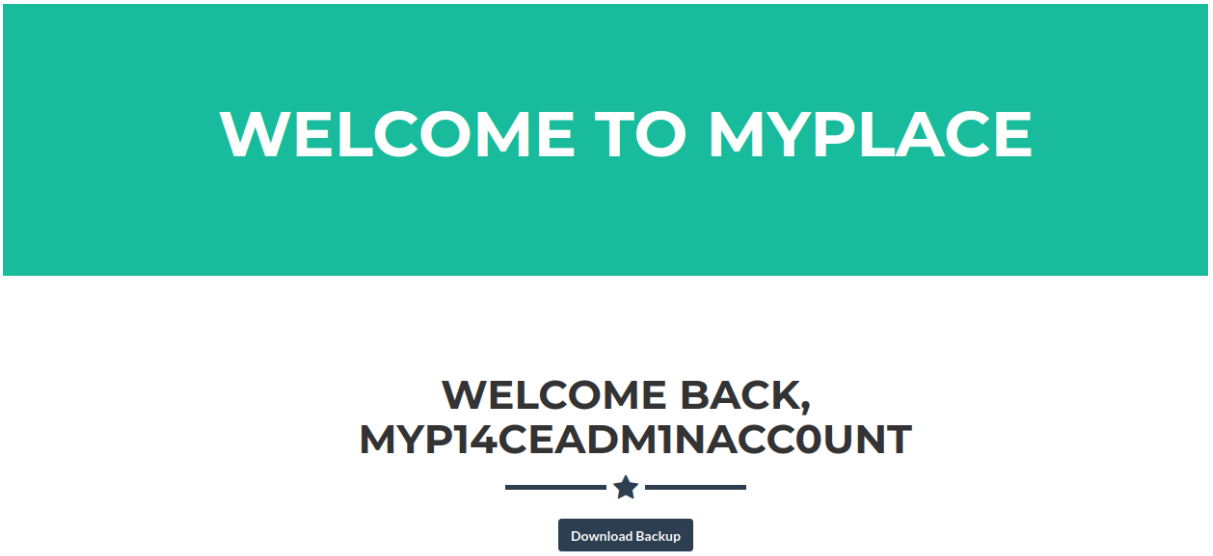
```
Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: /usr/share/dirb/wordlists/common.txt
* Passwords.: 4702
* Bytes.....: 36964
* Keyspace..: 4702
* Runtime...: 0 secs

de5a1adf4fedcce1533915edc60177547f1057b61b7119fd130e1f7428705f73:snowflake
Approaching final keyspace - workload adjusted.
```

```
Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/dirb/wordlists/common.txt
* Passwords.: 4702
* Bytes.....: 36964
* Keyspace..: 4702

dffc504aa55359b9265cbebe1e4032fe600b64475ae3fd29c07d23223334d0af:manchester
Approaching final keyspace - workload adjusted.
```

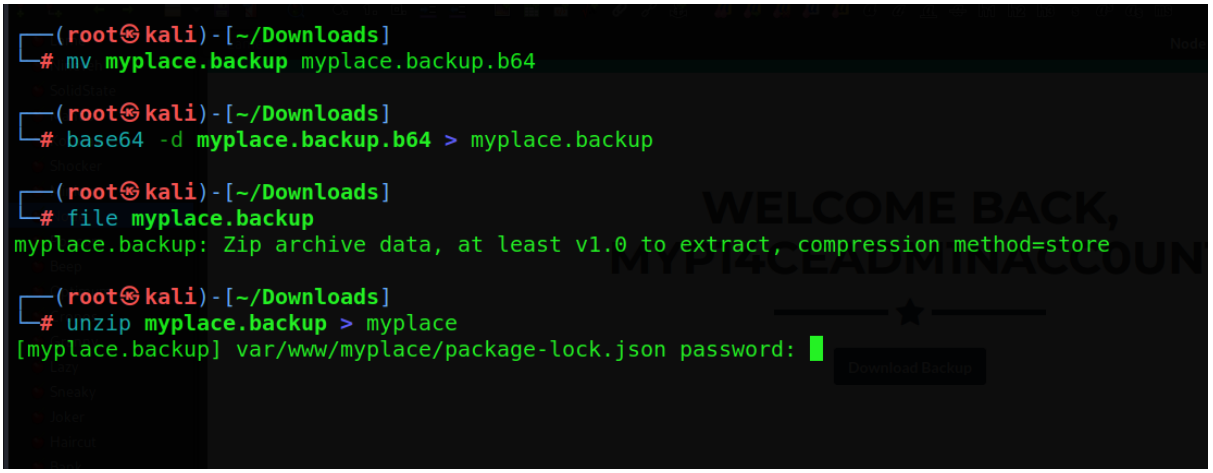
And we cracked two hases, among which one belongs to the admin user

Let’s use those credentials to login as an administrator to the application

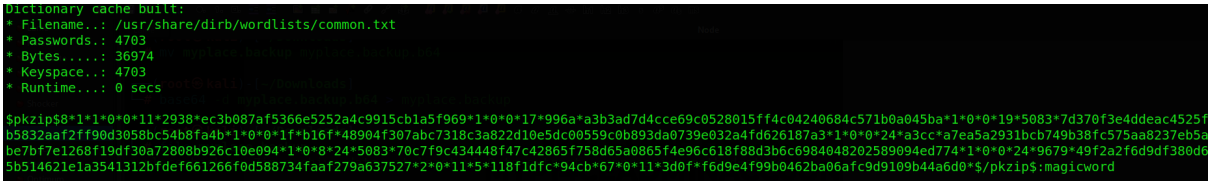




As an administrator we can download a backup of the entire application

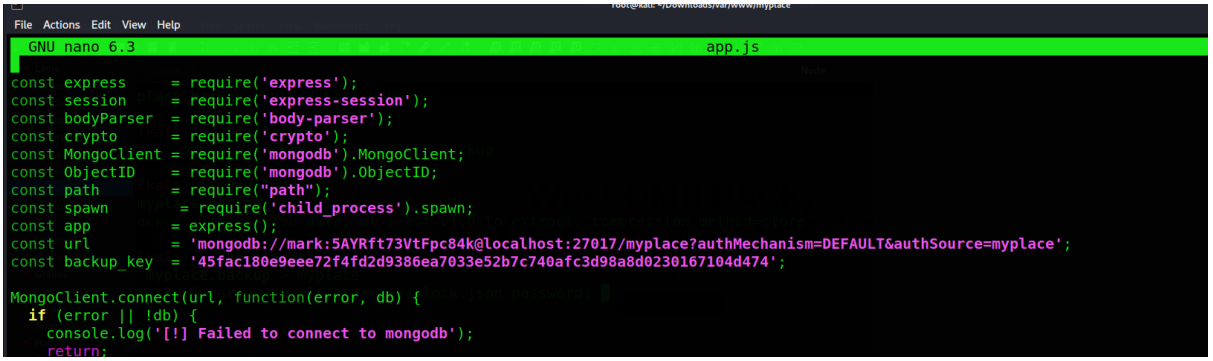


But the backup file is password protected, in order to crack it, we need to use zip2john (to convert into hashcar friendly format) and then launch hashcat

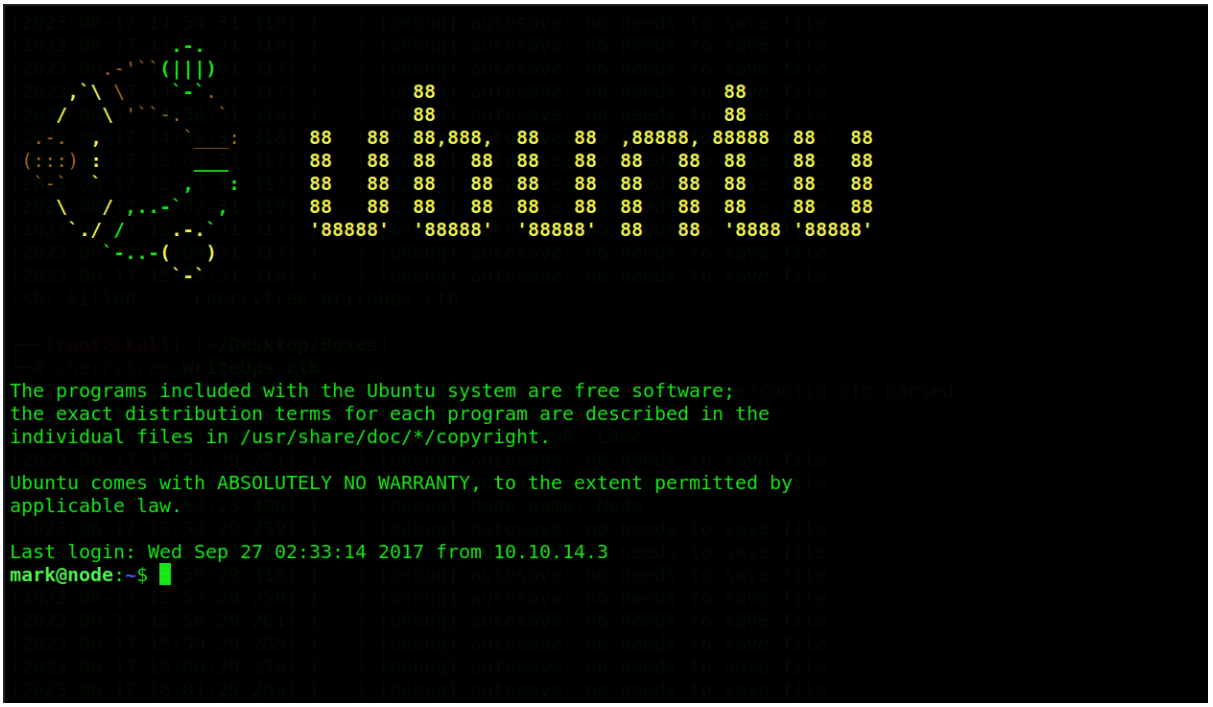


And we cracked the hash and got password needed to unzip application backup

Examination of the application’s source code provided us with credentials for user mark



Let’s check if those credentials will allow us to ssh to the machine



And we successfully got an access as a user mark by using credentials found in the applicat